Journal of Privacy and Confidentiality (2016) **7**, Number 2, 3–22

Between Pure and Approximate Differential Privacy

Thomas Steinke[*] and Jonathan Ullman[†]

We show a new lower bound on the sample complexity of (ε, δ)-differentially private algorithms that accurately answer statistical queries on high-dimensional databases. The novelty of our bound is that it depends optimally on the parameter δ, which loosely corresponds to the probability that the algorithm fails to be private, and is the first to smoothly interpolate between approximate differential privacy ($\delta > 0$) and pure differential privacy ($\delta = 0$).

Specifically, we consider a database $D \in \{\pm 1\}^{n \times d}$ and its *one-way marginals*, which are the d queries of the form "What fraction of individual records have the i-th bit set to $+1$?" We show that in order to answer all of these queries to within error $\pm\alpha$ (on average) while satisfying (ε, δ)-differential privacy for some function δ such that $\delta \geq 2^{-o(n)}$ and $\delta \leq 1/n^{1+\Omega(1)}$, it is necessary that

$$n \geq \Omega\left(\frac{\sqrt{d \log(1/\delta)}}{\alpha\varepsilon}\right).$$

This bound is optimal up to constant factors. This lower bound implies similar new bounds for problems like private empirical risk minimization and private PCA. To prove our lower bound, we build on the connection between *fingerprinting codes* and lower bounds in differential privacy (Bun, Ullman, and Vadhan, STOC'14).

In addition to our lower bound, we give new purely and approximately differentially private algorithms for answering arbitrary statistical queries that improve on the sample complexity of the standard Laplace and Gaussian mechanisms for achieving worst-case accuracy guarantees by a logarithmic factor.

1 Introduction

The goal of privacy-preserving data analysis is to enable rich statistical analysis of a database while protecting the privacy of individuals whose data is in the database. A formal privacy guarantee is given by (ε, δ)-*differential privacy* (Dwork et al., 2006b;a), which ensures that no individual's data has a significant influence on the information released about the database. The two parameters ε and δ control the level of privacy. Very roughly, ε is an upper bound on the amount of influence an individual's record has

[*] Harvard University School of Engineering and Applied Sciences. Supported by NSF grants CCF-1116616, CCF-1420938, and CNS-1237235. mailto:tsteinke@seas.harvard.edu

[†] Northeastern University College of Computer and Information Science. Most of this work was done while the author was a postdoctoral fellow in the Department of Computer Science at Columbia University. Supported by a junior fellowship from the Simons Society of Fellows. mailto:jullman@cs.columbia.edu

© 2016 by the authors http://repository.cmu.edu/jpc

on the information released and δ is the probability that this bound fails to hold[1], so the definition becomes more stringent as $\varepsilon, \delta \to 0$.

A natural way to measure the tradeoff between privacy and utility is *sample complexity*—the minimum number of records n that is sufficient in order to publicly release a given set of statistics about the database, while achieving both differential privacy and statistical accuracy. Intuitively, it's easier to achieve these two goals when n is large, as each individual's data will have only a small influence on the aggregate statistics of interest. Conversely, the sample complexity n should increase as ε and δ decrease (which strengthens the privacy guarantee).

The strongest version of differential privacy, in which $\delta = 0$, is known as *pure differential privacy*. The sample complexity of achieving pure differential privacy is well known for many settings (e.g. Hardt and Talwar (2010)). The more general case where $\delta > 0$ is known as *approximate differential privacy*, and is less well understood. Recently, Bun, Ullman, and Vadhan (Bun et al., 2014) showed how to prove strong lower bounds for approximate differential privacy that are essentially optimal for $\delta \approx 1/n$, which is essentially the weakest privacy guarantee that is still meaningful.[2]

Since δ bounds the probability of a complete privacy breach, we would like δ to be very small. Thus we would like to quantify the cost (in terms of sample complexity) as $\delta \to 0$. In this work we give lower bounds for approximately differentially private algorithms that are nearly optimal for every choice of δ, and smoothly interpolate between pure and approximate differential privacy.

Specifically, we consider algorithms that compute the *one-way marginals of the database*—an extremely simple and fundamental family of queries. For a database $D \in \{\pm 1\}^{n \times d}$, the d one-way marginals are simply the mean of the bits in each of the d columns. Formally, we define

$$\overline{D} := \frac{1}{n} \sum_{i=1}^{n} D_i \in [\pm 1]^d$$

where $D_i \in \{\pm 1\}^d$ is the i-th row of D. A mechanism M is said to be *accurate* if, on input D, its output is "close to" $\overline{D}$. Accuracy may be measured in a *worst-case* sense—i.e. $\left|\left|M(D) - \overline{D}\right|\right|_\infty \le \alpha$, meaning every one-way marginal is answered with accuracy α—or in an *average-case* sense—i.e. $\left|\left|M(D) - \overline{D}\right|\right|_1 \le \alpha d$, meaning the marginals are answered with average accuracy α.

Some of the earliest results in differential privacy (Dinur and Nissim, 2003; Dwork and Nissim, 2004; Blum et al., 2005; Dwork et al., 2006b) give a simple (ε, δ)-differentially private algorithm—the *Laplace mechanism*—that computes the one-way marginals of

[1] This intuition is actually imprecise, but it is suitable for this informal discussion. See Kasiviswanathan and Smith (Kasiviswanathan and Smith, 2008) for a formal justification of this interpretation of (ε, δ)-differential privacy.

[2] When $\delta \ge 1/n$ there are algorithms that are intuitively not private, yet satisfy $(0, \delta)$-differential privacy.

$D \in \{\pm 1\}^{n \times d}$ with average error α as long as

$$n \geq O\left(\min\left\{\frac{\sqrt{d\log(1/\delta)}}{\varepsilon\alpha}, \frac{d}{\varepsilon\alpha}\right\}\right). \tag{1}$$

The previous best lower bounds are $n \geq \Omega(d/\varepsilon\alpha)$ (Hardt and Talwar, 2010) for pure differential privacy and $n \geq \tilde{\Omega}(\sqrt{d}/\varepsilon\alpha)$ for approximate differential privacy with $\delta = o(1/n)$ (Bun et al., 2014). Our main result is an optimal lower bound that combines the previous lower bounds.

Theorem 1.1 (Main Theorem)**.** *For every $\varepsilon \in (0,1)$, every function $\delta = \delta(n)$ with $\delta \geq 2^{-o(n)}$ and $\delta \leq 1/n^{1+\Omega(1)}$, and every $\alpha \leq 1/10$, if $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ is (ε, δ)-differentially private and $\mathop{\mathbb{E}}_{M}\left[\|M(D) - \overline{D}\|_1\right] \leq \alpha d$ for all $D \in \{\pm 1\}^{n \times d}$, then*

$$n \geq \Omega\left(\frac{\sqrt{d\log(1/\delta)}}{\varepsilon\alpha}\right).$$

Although there has been a long line of work developing methods to prove lower bounds in differential privacy (see Dinur and Nissim (2003); Dwork et al. (2007); Dwork and Yekhanin (2008); Kasiviswanathan et al. (2010); Hardt and Talwar (2010); Nikolov et al. (2013); Bun et al. (2014) for a representative, but not exhaustive, sample), our result is the first to show that the sample complexity must grow by a multiplicative factor of $\sqrt{\log(1/\delta)}$ for answering any family of queries, as opposed to an additive dependence on δ. We also remark that the assumption on the range of δ is necessary: The Laplace mechanism gives accuracy α and satisfies $(\varepsilon, 0)$-differential privacy when $n \geq O(d/\varepsilon\alpha)$. On the other hand, randomly sampling $O(1/\alpha^2)$ rows from the database and outputting the average of those rows gives accuracy α and satisfies $(0, \delta)$-differential privacy when $n \geq O(1/\alpha^2\delta)$.

Lower bounds for answering one-way marginals have been shown to imply lower bounds for fundamental problems such as private convex empirical risk minimization (Bassily et al., 2014) and private principle component analysis (Dwork et al., 2014). Our new lower bound for one-way marginals thus implies similar new lower bounds for these problems. We describe these lower bounds in Section 5.

Finally, our techniques yield a simple alternative proof that $n \geq \Omega(d/\varepsilon\alpha)$ is necessary to achieve pure differential privacy while satisfying the accuracy condition in Theorem 1.1. We present this proof in Appendix 5.2.

1.1 New Algorithms for Maximum Error

Our lower bound holds for mechanisms that bound the average error over the queries (we denote this as L_1 error). Thus, it also holds for algorithms that bound the maximum error over the queries (we denote this as L_∞ error). The Laplace mechanism gives a matching upper bound for average error. In many cases bounds on the maximum error are preferable. For maximum error, the sample complexity of the best previous mechanisms degrades by an additional polylog(d) factor compared to (1).

Surprisingly, this degradation is not necessary. We present algorithms that answer every one-way marginal with α accuracy and improve on the sample complexity of the Laplace mechanism by roughly a $\log d$ factor. These algorithms demonstrate that the widely used technique of adding independent noise to each query is suboptimal when the goal is to achieve worst-case error guarantees.

Our algorithm for pure differential privacy satisfies the following.

Theorem 1.2. *For every $\varepsilon, \alpha > 0$, $d \geq 1$, and $n \geq 4d/\varepsilon\alpha$, there exists an efficient mechanism $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ that is $(\varepsilon, 0)$-differentially private and*

$$\forall D \in \{\pm 1\}^{n \times d} \qquad \underset{M}{\mathbb{P}}\left[\left|\left|M(D) - \overline{D}\right|\right|_\infty \geq \alpha\right] \leq (2e)^{-d}.$$

In fact, the algorithm promised by Theorem 1.2 is oblivious, perturbing the answers with noise from a fixed distribution[3] and only depends on the dimension d and the scale εn. In particular, the mechanism does not depend on α.

And our algorithm for approximate differential privacy is as follows.

Theorem 1.3. *For every $\varepsilon, \delta, \alpha > 0$, $d \geq 1$, and*

$$n \geq O\left(\frac{\sqrt{d \cdot \log(1/\delta) \cdot \log\log d}}{\varepsilon\alpha}\right),$$

there exists an efficient mechanism $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ that is (ε, δ)-differentially private and

$$\forall D \in \{\pm 1\}^{n \times d} \qquad \underset{M}{\mathbb{P}}\left[\left|\left|M(D) - \overline{D}\right|\right|_\infty \geq \alpha\right] \leq \frac{1}{d^{\omega(1)}}.$$

The algorithm stipulated by Theorem 1.3 is also oblivious, although in this case the distribution depends on α in addition to d and εn.

These algorithms improve over the sample complexity of the best known mechanisms for each privacy and accuracy guarantee by a factor of $(\log d)^{\Omega(1)}$. Namely, the Laplace mechanism requires $n \geq O(d \cdot \log d/\varepsilon\alpha)$ samples for pure differential privacy and the Gaussian mechanism requires $n \geq O(\sqrt{d \cdot \log(1/\delta) \cdot \log d}/\varepsilon\alpha)$ samples for approximate differential privacy.

We remark that the algorithms in Theorems 1.2 and 1.3 are not specific to one-way marginals. They can be use to answer any set of d sensitivity-$2/n$ queries. We also conjecture that the Algorithm in Theorem 1.3 can be improved to match our lower bound — that is, we believe that the $\sqrt{\log\log d}$ factor is unnecessary.

[3] That is, $M(D)$ is simply $\overline{D} + Y$ (truncated to $[\pm 1]^d$), where Y is a single distribution and does not depend on D.

Privacy	Accuracy	Type	Previous bound	This work
(ε, δ)	L_1 or L_∞	Lower	$n = \tilde{\Omega}\left(\frac{\sqrt{d}}{\alpha\varepsilon}\right)$ Bun et al. (2014)	$n = \Omega\left(\frac{\sqrt{d \log(1/\delta)}}{\alpha\varepsilon}\right)$
(ε, δ)	L_1	Upper	$n = O\left(\frac{\sqrt{d \cdot \log(1/\delta)}}{\alpha\varepsilon}\right)$ Gaussian	
(ε, δ)	L_∞	Upper	$n = O\left(\frac{\sqrt{d \cdot \log(1/\delta) \cdot \log d}}{\alpha\varepsilon}\right)$ Gaussian	$n = O\left(\frac{\sqrt{d \cdot \log(1/\delta) \cdot \log\log d}}{\varepsilon\alpha}\right)$
$(\varepsilon, 0)$	L_1 or L_∞	Lower	$n = \Omega\left(\frac{d}{\alpha\varepsilon}\right)$ Hardt and Talwar (2010)	
$(\varepsilon, 0)$	L_1	Upper	$n = O\left(\frac{d}{\alpha\varepsilon}\right)$ Laplace	
$(\varepsilon, 0)$	L_∞	Upper	$n = O\left(\frac{d \cdot \log d}{\alpha\varepsilon}\right)$ Laplace	$n = O\left(\frac{d}{\alpha\varepsilon}\right)$

Figure 1: Summary of sample complexity upper and lower bounds for privately answering d one-way marginals with L_1 error αd or L_∞ error α.

1.2 Techniques

Lower Bounds: Our lower bound relies on a combinatorial objected called a *fingerprinting code* (Boneh and Shaw, 1998). Fingerprinting codes were originally used in cryptography for watermarking digital content, but several recent works have shown they are intimately connected to lower bounds for differential privacy and related learning problems (Ullman, 2013; Bun et al., 2014; Hardt and Ullman, 2014; Steinke and Ullman, 2014). In particular, Bun et al. (Bun et al., 2014) showed that fingerprinting codes can be used to construct an attack demonstrating that any mechanism that accurately answers one-way marginals is not differentially private.

A fingerprinting code gives a distribution on individuals' data and a corresponding *tracing* algorithm. The tracing algorithm guarantees that if the database is constructed from some subset of the individuals, and the tracing algorithm is given approximate answers to the one-way marginals of the database, then the tracing algorithm will identify one of the n individuals, and with overwhelming probability this individual will be in the subset that was used to form the database. This tracing property is guaranteed as long as the dimension of the database d is sufficiently large relative to n. Such a tracing algorithm rules out differential privacy because there must be at least one individual in the database that is output by the tracer with significant probability, but if we were to remove that individual's data from the database, then that individual cannot be output by the tracer except with tiny probability, violating the differential privacy constraints.

To obtain the strongest lower bound for differential privacy, we want to have fingerprinting codes where d can be as small as possible relative to n. Tardos (Tardos, 2008) gave a beautiful construction of fingerprinting codes with $d = \tilde{O}(n^2)$. Bun, Ullman, and Vadhan (Bun et al., 2014) used Tardos' construction to show that any mechanism that satisfies $(1, o(1/n))$-differential privacy requires $n \geq \tilde{\Omega}(\sqrt{d})$ samples to compute one-way marginals with constant accuracy.

Our proof uses a new, more general reduction from breaking fingerprinting codes to differentially private data release. Specifically, our reduction uses *group differential privacy*. This property states that if an algorithm is (ε, δ)-differentially private with respect to the change of one individual's data, then for any k, it is roughly $(k\varepsilon, e^{k\varepsilon}\delta)$-differentially private with respect to the change of k individuals' data. Thus an (ε, δ)-differentially private algorithm provides a meaningful privacy guarantee for groups of size $k \approx \log(1/\delta)/\varepsilon$.

To use this in our reduction, we start with a mechanism M that takes a database of n rows and is (ε, δ)-differentially private. We design a mechanism M_k that takes a database of n/k rows, copies each of its rows k times, and uses the result as input to M. Using the property of group differential privacy above, the resulting mechanism M_k is roughly $(k\varepsilon, e^{k\varepsilon}\delta)$-differentially private. For our choice of k, these parameters will be small enough to apply the attack of Bun et al. (2014) to obtain a lower bound on the number of samples used by M_k, which is n/k. Thus, for larger values of k (equivalently, smaller values of δ), we obtain a stronger lower bound. The remainder of the proof is to quantify the parameters precisely.

Upper Bounds: Our algorithm for pure differential privacy and worst-case error is an instantiation of the exponential mechanism (McSherry and Talwar, 2007) using the L_∞ norm. That is, the mechanism samples $y \in \mathbb{R}^d$ with probability proportional to $\exp(-\eta \left|\left|y\right|\right|_\infty)$ and outputs $M(D) = \overline{D} + y$. In contrast, adding independent Laplace noise corresponds to using the exponential mechanism with the L_1 norm and adding independent Gaussian noise corresponds to using the exponential mechanism with the L_2 norm squared. Using this distribution turns out to give better tail bounds than adding independent noise.

For approximate differential privacy, we use a completely different algorithm. We start by adding independent Gaussian noise to each marginal. However, rather than using a union bound to show that each Gaussian error is small with high probability, we argue that "most" errors are small. Namely, with the sample complexity that we allow M, we can ensure that all but a $1/\text{polylog}(d)$ fraction of the errors are small with high probability. Now we "fix" the $d/\text{polylog}(d)$ marginals that are bad. We repeatedly use the exponential mechanism (McSherry and Talwar, 2007) to find one bad error and the correct it by sampling fresh Gaussian noise. The key is that we only need to run this procedure $d/\text{polylog}(d)$ times, which means we can afford the necessary sample complexity.

2 Preliminaries

We define a *database* $D \in \{\pm 1\}^{n \times d}$ to be a matrix of n rows, where each row corresponds to an individual, and each row has *dimension* d (consists of d binary attributes). We say that two databases $D, D' \in \{\pm 1\}^{n \times d}$ are *adjacent* if they differ only by a single row, and we denote this by $D \sim D'$. In particular, we can replace the ith row of a database D with some fixed element of $\{\pm 1\}^d$ to obtain another database $D_{-i} \sim D$.

Definition 2.1 (Differential Privacy (Dwork et al., 2006b))**.** Let $M : \{\pm 1\}^{n \times d} \to \mathcal{R}$ be a randomized mechanism. We say that M is (ε, δ)*-differentially private* if for every two adjacent databases $D \sim D'$ and every subset $S \subseteq \mathcal{R}$,

$$\mathbb{P}\left[M(D) \in S\right] \leq e^{\varepsilon} \cdot \mathbb{P}\left[M(D') \in S\right] + \delta.$$

A well known fact about differential privacy is that it generalizes smoothly to databases that differ on more than a single row. We say that two databases $D, D' \in \{\pm 1\}^{n \times d}$ are *k-adjacent* if they differ by at most k rows, and we denote this by $D \sim_k D'$. The following statement is essentially folklore, and we refer the reader to Dwork and Roth (2014) for a textbook proof.

Fact 2.2 (Group Differential Privacy)**.** *For every $k \geq 1$, if $M : \{\pm 1\}^{n \times d} \to \mathcal{R}$ is (ε, δ)-differentially private, then for every two k-adjacent databases $D \sim_k D'$, and every subset $S \subseteq \mathcal{R}$,*

$$\mathbb{P}\left[M(D) \in S\right] \leq e^{k\varepsilon} \cdot \mathbb{P}\left[M(D') \in S\right] + \frac{e^{k\varepsilon} - 1}{e^{\varepsilon} - 1} \cdot \delta.$$

All of the upper and lower bounds for one-way marginals have a multiplicative $1/\alpha\varepsilon$ dependence on the accuracy α and the privacy loss ε. This is no coincidence, and follows from the following general statement, which is folklore.

Fact 2.3 (Dependence on α and ε)**.** *Let $\alpha, \delta \in [0, 1/10]$, and $\varepsilon \in (0, 1/10]$. Fix some norm $||\cdot||$.*

Suppose there exists a (ε, δ)-differentially private mechanism $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ such that for every database $D \in \{\pm 1\}^{n \times d}$,

$$\mathop{\mathbb{E}}_{M}\left[\|M(D) - \overline{D}\|\right] \leq \alpha \left|\left|\vec{1}\right|\right|.$$

Then there exists a $(1, \delta/\varepsilon)$-differentially private mechanism $M' : \{\pm 1\}^{n' \times d} \to [\pm 1]^d$ for $n' = \Theta(\alpha\varepsilon n)$ such that for every database $D' \in \{\pm 1\}^{n' \times d}$,

$$\mathop{\mathbb{E}}_{M'}\left[\|M'(D') - \overline{D'}\|\right] \leq \frac{1}{10} \left|\left|\vec{1}\right|\right|.$$

This fact allows us to suppress the accuracy parameter α and the privacy loss ε when proving our lower bounds. Namely, if we prove a lower bound of $n' \geq n^*$ for all $(1, \delta)$-differentially private mechanisms $M' : \{\pm 1\}^{n' \times d} \to [\pm 1]^d$ with $\mathop{\mathbb{E}}_{M'}\left[\|M'(D') - \overline{D'}\|_p\right] \leq d^{1/p}/10$, then we obtain a lower bound of $n \geq \Omega(n^*/\alpha\varepsilon)$ for all $(\varepsilon, \varepsilon\delta)$-differentially private mechanisms $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ with $\mathop{\mathbb{E}}_{M}\left[\|M(D) - \overline{D}\|_p\right] \leq \alpha d^{1/p}$. So we will simply fix the parameters $\alpha = 1/10$ and $\varepsilon = 1$ in our lower bounds.

Proof. Let $k = \lfloor \log(2)/\varepsilon \rfloor$. Given $D' \in \{\pm 1\}^{n' \times d}$, define $D \in \{\pm 1\}^{n \times d}$ to be k copies of D' followed by $n - kn'$ rows of all 1 entries. Then

$$n\overline{D} = n'\overline{D'} \cdot k + (n - kn')\vec{1} \quad \text{and} \quad \overline{D'} = \frac{n}{kn'}\overline{D} - \frac{n - kn'}{kn'}\vec{1}.$$

Define M' by

$$M'(D') = \frac{n}{kn'}M(D) - \frac{n - kn'}{kn'}\vec{1}.$$

Then

$$\mathop{\mathbb{E}}_{M'}\left[\left|\left|M'(D') - \overline{D'}\right|\right|\right] = \frac{n}{kn'}\mathop{\mathbb{E}}_{M}\left[\left|\left|M(D) - \overline{D}\right|\right|\right] \leq \frac{\alpha n}{kn'}\left|\left|\vec{1}\right|\right|.$$

Thus, if $n' \geq 20\alpha\varepsilon n \geq 10\alpha n/k$, we have $\mathop{\mathbb{E}}_{M'}\left[\left|\left|M'(D') - \overline{D'}\right|\right|\right] \leq \frac{1}{10}\left|\left|\vec{1}\right|\right|$, as required. By Fact 2.2, M' is $\left(k\varepsilon, \frac{e^{k\varepsilon}-1}{e^{\varepsilon}-1} \cdot \delta\right)$-differentially private. By our choice of k, we have $k\varepsilon \leq \log 2 \leq 1$ and $\frac{e^{k\varepsilon}-1}{e^{\varepsilon}-1}\delta \leq \frac{e^{\log 2}-1}{\varepsilon}\delta$, as required. □

3 Lower Bounds for Approximate Differential Privacy

Our main theorem can be stated as follows.

Theorem 3.1 (Main Theorem)**.** *Let $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ be a $(1, \delta)$-differentially private mechanism that answers one-way marginals such that*

$$\forall D \in \{\pm 1\}^{n \times d} \quad \mathop{\mathbb{E}}_{M}\left[\left|\left|M(D) - \overline{D}\right|\right|_1\right] \leq \frac{d}{10},$$

where $\overline{D}$ is the true answer vector. If $\delta \geq e^{-n/200}$ and $\delta \leq 1/n^{1+\gamma}$ for some $\gamma \in (0, 1)$, and n is sufficiently large, then

$$d \leq O\left(\frac{n^2}{\gamma^2 \log(1/\delta)}\right).$$

Theorem 1.1 in the introduction follows by rearranging terms, and applying Fact 2.3.

First we must introduce fingerprinting codes. The following definition is tailored to the application to privacy. Fingerprinting codes were originally defined by Boneh and Shaw (Boneh and Shaw, 1998) with a worst-case accuracy guarantee. Subsequent works (Bun et al., 2014; Steinke and Ullman, 2014) have altered the accuracy guarantee to an average-case one, which we use here.

Definition 3.2 (L_1 Fingerprinting Code)**.** A *ε-complete δ-sound α-robust L_1 fingerprinting code for n users with length d* is a pair of random variables $D \in \{\pm 1\}^{n \times d}$ and *Trace* : $[\pm 1]^d \to 2^{[n]}$ such that the following hold.

Completeness: For any fixed $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$,

$$\mathbb{P}\left[\left(\left|\left|M(D) - \overline{D}\right|\right|_1 \leq \alpha d\right) \wedge \left(\mathit{Trace}(M(D)) = \emptyset\right)\right] \leq \varepsilon.$$

Soundness: For any $i \in [n]$ and fixed $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$,

$$\mathbb{P}\left[i \in \mathit{Trace}(M(D_{-i}))\right] \leq \delta,$$

where D_{-i} denotes D with the i^{th} row replaced by some fixed element of $\{\pm 1\}^d$.

We remark that δ in the above definition is not the same quantity as δ in the definition of (ε, δ)-differential privacy. However, we chose to reuse the notation, since in our proof, we will apply both definitions with the same choice of δ.

Fingerprinting codes with optimal length were first constructed by Tardos (Tardos, 2008) (for worst-case error) and subsequent works (Bun et al., 2014; Steinke and Ullman, 2014) have adapted Tardos' construction to work for average-case error guarantees, which yields the following theorem.

Theorem 3.3 ((Steinke and Ullman, 2014, Theorem 2.21))**.** *For every $n \geq 1$, $\delta > 0$, and $d \geq d_{n,\delta} = O(n^2 \log(1/\delta))$, there exists a $1/100$-complete δ-sound $1/8$-robust L_1 fingerprinting code for n users with length d.*

We now show how the existence of fingerprinting codes implies our lower bound.

Proof of Theorem 3.1 from Theorem 3.3. Let $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ be a $(1, \delta)$-differentially private mechanism such that

$$\forall D \in \{\pm 1\}^{n \times d} \quad \mathop{\mathbb{E}}_{M}\left[\left|\left|M(D) - \overline{D}\right|\right|_1\right] \leq \frac{d}{10}.$$

Then, by Markov's inequality,

$$\forall D \in \{\pm 1\}^{n \times d} \quad \mathop{\mathbb{P}}_{M}\left[\left|\left|M(D) - \overline{D}\right|\right|_1 > \frac{d}{9}\right] \leq \frac{9}{10}. \tag{2}$$

Let k be an integer parameter to be chosen later. Let $n_k = \lfloor n/k \rfloor$. Let $M_k : \{\pm 1\}^{n_k \times d} \to [\pm 1]^d$ be the following mechanism. On input $D^* \in \{\pm 1\}^{n_k \times d}$, M_k creates $D \in \{\pm 1\}^{n \times d}$ by taking k copies of D^* and filling the remaining entries with 1s. Then M_k runs M on D and outputs $M(D)$.

By group privacy (Fact 2.2), M_k is a $\left(\varepsilon_k = k, \delta_k = \frac{e^k - 1}{e - 1}\delta\right)$-differentially private mechanism. By the triangle inequality,

$$\left|\left|M_k(D^*) - \overline{D^*}\right|\right|_1 \leq \left|\left|M(D) - \overline{D}\right|\right|_1 + \left|\left|\overline{D} - \overline{D^*}\right|\right|_1. \tag{3}$$

Now

$$\overline{D}_j = \frac{k \cdot n_k}{n}\overline{D^*_j} + \frac{n - k \cdot n_k}{n} 1.$$

Thus

$$\left|\overline{D}_j - \overline{D^*_j}\right| = \left|\left(\frac{k \cdot n_k}{n} - 1\right)\overline{D^*_j} + \frac{n - k \cdot n_k}{n}\right| = \frac{n - k \cdot n_k}{n}\left|1 - \overline{D^*_j}\right| \leq 2\frac{n - k \cdot n_k}{n}.$$

We have
$$\frac{n - k \cdot n_k}{n} = \frac{n - k\lfloor n/k \rfloor}{n} \leq \frac{n - k(n/k - 1)}{n} = \frac{k}{n}.$$
Thus $\left|\left|\overline{D} - \overline{D^*}\right|\right|_1 \leq 2dk/n$. Assume $k \leq n/200$. Thus $\left|\left|\overline{D} - \overline{D^*}\right|\right|_1 \leq d/100$ and, by (2) and (3),
$$\underset{M_k}{\mathbb{P}}\left[\left|\left|M_k(D^*) - \overline{D^*}\right|\right|_1 > \frac{d}{8}\right] \leq \underset{M}{\mathbb{P}}\left[\left|\left|M(D) - \overline{D}\right|\right|_1 > \frac{d}{9}\right] \leq \frac{9}{10}. \tag{4}$$

Assume $d \geq d_{n_k,\delta}$, where $d_{n_k,\delta} = O(n_k^2 \log(1/\delta))$ is as in Theorem 3.3. We will show by contradiction that this cannot be – that is $d \leq O(n_k^2 \log(1/\delta))$. Let $D^* \in \{\pm 1\}^{n_k \times d}$ and $\mathit{Trace} : [\pm 1]^d \to 2^{[n_k]}$ be a $1/100$-complete δ-sound $1/8$-robust L_1 fingerprinting code for n_k users of length d.

By the completeness of the fingerprinting code,
$$\mathbb{P}\left[\left|\left|M_k(D^*) - \overline{D^*}\right|\right|_1 \leq \frac{d}{8} \wedge \mathit{Trace}(M(D)) = \emptyset\right] \leq \frac{1}{100}. \tag{5}$$
Combinging (4) and (5), gives
$$\mathbb{P}\left[\mathit{Trace}(M_k(D^*)) \neq \emptyset\right] \geq \frac{9}{100} > \frac{1}{12}.$$
In particular, there exists $i^* \in [n_k]$ such that
$$\mathbb{P}\left[i^* \in \mathit{Trace}(M_k(D^*))\right] > \frac{1}{12 n_k}. \tag{6}$$

We have that $\mathit{Trace}(M_k(D^*))$ is a $(\varepsilon_k, \delta_k)$-differentially private function of D^*, as it is only postprocessing $M_k(D^*)$. Thus
$$\mathbb{P}\left[i^* \in \mathit{Trace}(M_k(D^*))\right] \leq e^{\varepsilon_k} \mathbb{P}\left[i^* \in \mathit{Trace}(M_k(D^*_{-i^*}))\right] + \delta_k \leq e^{\varepsilon_k}\delta + \delta_k, \tag{7}$$
where the second inequality follows from the soundness of the fingerprinting code.

Combining (6) and (7) gives
$$\frac{1}{12 n_k} \leq e^{\varepsilon_k}\delta + \delta_k = e^k \delta + \frac{e^k - 1}{e - 1}\delta = \frac{e^{k+1} - 1}{e - 1}\delta < e^{k+1}\delta. \tag{8}$$
If $k \leq \log(1/12 n_k \delta) - 1$, then (8) gives a contradiction. Let $k = \lfloor \log(1/12 n \delta) - 1 \rfloor$, since larger values of k give stronger lower bounds. Assuming $\delta \geq e^{-n/200}$ ensures $k \leq n/200$, as required. Assuming $\delta \leq 1/n^{1+\gamma}$ implies $k \geq \log(1/\delta)/(1 + 1/\gamma) - 5 \geq \Omega(\gamma \log(1/\delta))$. This setting of k gives a contradiction, which implies that
$$d < d_{n_k,\delta} = O(n_k^2 \log(1/\delta)) = O\left(\frac{n^2}{k^2}\log(1/\delta)\right) = O\left(\frac{n^2}{\gamma^2 \log(1/\delta)}\right),$$
as required.

□

4 New Mechanisms for L_∞ Error

Adding independent noise seems very natural for one-way marginals, but it is suboptimal if one is interested in worst-case (i.e. L_∞) error bounds, rather than average-case (i.e. L_1) error bounds.

4.1 Pure Differential Privacy

Theorem 1.2 follows from Theorem 4.1. In particular, the mechanism $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ in Theorem 1.2 is given by $M(D) = \overline{D} + Y$, where $Y \sim \mathcal{D}$ and $\mathcal{D}$ is the distribution from Theorem 4.1 with $\Delta = 2/n$.[4]

Theorem 4.1. *For all $\varepsilon > 0$, $d \geq 1$, and $\Delta > 0$, there exists a continuous distribution $\mathcal{D}$ on $\mathbb{R}^d$ with the following properties.*

- ***Privacy:*** *If $x, x' \in \mathbb{R}^d$ with $\|x - x'\|_\infty \leq \Delta$, then*
$$\underset{Y \sim \mathcal{D}}{\mathbb{P}}[x + Y \in S] \leq e^\varepsilon \underset{Y \sim \mathcal{D}}{\mathbb{P}}[x' + Y \in S]$$
for all measurable $S \subseteq \mathbb{R}^d$.
- ***Accuracy:*** *For all $\alpha > 0$,*
$$\underset{Y \sim \mathcal{D}}{\mathbb{P}}[\|Y\|_\infty \geq \alpha] \leq \left(\frac{\Delta d}{\varepsilon \alpha}\right)^d e^{d - \alpha\varepsilon/\Delta}.$$
In particular, if $d \leq \varepsilon\alpha/2\Delta$, then $\underset{Y \sim \mathcal{D}}{\mathbb{P}}[\|Y\|_\infty \geq \alpha] \leq (2e)^{-d}$.
- ***Efficiency:*** *$\mathcal{D}$ can be efficiently sampled.*

Proof. The distribution $\mathcal{D}$ is simply an instantiation of the exponential mechanism (McSherry and Talwar, 2007). In particular, the probability density function is given by
$$\mathrm{pdf}_{\mathcal{D}}(y) \propto \exp\left(-\frac{\varepsilon}{\Delta}\|y\|_\infty\right).$$

Formally, for every measurable $S \subseteq \mathbb{R}^d$,
$$\underset{Y \sim \mathcal{D}}{\mathbb{P}}[Y \in S] = \frac{\int_S \exp\left(-\frac{\varepsilon}{\Delta}\|y\|_\infty\right) \mathrm{d}y}{\int_{\mathbb{R}^d} \exp\left(-\frac{\varepsilon}{\Delta}\|y\|_\infty\right) \mathrm{d}y}.$$

Firstly, this is clearly a well-defined distribution as long as $\varepsilon/\Delta > 0$.

Privacy is easy to verify: It suffices to bound the ratio of the probability densities for the shifted distributions. For $x, x' \in \mathbb{R}^d$ with $\|x' - x\|_\infty \leq \Delta$, by the triangle inequality,
$$\frac{\mathrm{pdf}_{\mathcal{D}}(x + y)}{\mathrm{pdf}_{\mathcal{D}}(x' + y)} = \frac{\exp\left(-\frac{\varepsilon}{\Delta}\|x + y\|_\infty\right)}{\exp\left(-\frac{\varepsilon}{\Delta}\|x' + y\|_\infty\right)} = \exp\left(\frac{\varepsilon}{\Delta}\left(\|x' + y\|_\infty - \|x + y\|_\infty\right)\right) \leq \exp\left(\frac{\varepsilon}{\Delta}\|x' - x\|_\infty\right) \leq e^\varepsilon.$$

[4] Note that we must truncate the output of M to ensure that $M(D)$ is always in $[\pm 1]^d$.

Define a distribution $\mathcal{D}^*$ on $[0,\infty)$ to by $Z \sim \mathcal{D}^*$ meaning $Z = ||Y||_\infty$ for $Y \sim \mathcal{D}$. To prove accuracy, we must give a tail bound on $\mathcal{D}^*$. The probability density function of $\mathcal{D}^*$ is given by

$$\mathrm{pdf}_{\mathcal{D}^*}(z) \propto z^{d-1} \cdot \exp\left(-\frac{\varepsilon}{\Delta} z\right),$$

which is obtained by integrating the probability density function of $\mathcal{D}$ over the infinity-ball of radius z, which has surface area $d2^d z^{d-1} \propto z^{d-1}$. Thus $\mathcal{D}^*$ is precisely the gamma distribution with shape d and mean $d\Delta/\varepsilon$. The moment generating function is therefore

$$\mathop{\mathbb{E}}_{Z\sim\mathcal{D}^*}\left[e^{tZ}\right] = \left(1 - \frac{\Delta}{\varepsilon} t\right)^{-d}$$

for all $t < \varepsilon/\Delta$. By Markov's inequality

$$\mathop{\mathbb{P}}_{Z\sim\mathcal{D}^*}\left[Z \geq \alpha\right] \leq \frac{\mathop{\mathbb{E}}_{Z\sim\mathcal{D}^*}\left[e^{tZ}\right]}{e^{t\alpha}} = \left(1 - \frac{\Delta}{\varepsilon} t\right)^{-d} e^{-t\alpha}.$$

Setting $t = \varepsilon/\Delta - d/\alpha$ gives the required bound.

It is easy to verify that $Y \sim \mathcal{D}$ can be sampled by first sampling a radius R from a gamma distribution with shape $d+1$ and mean $(d+1)\Delta/\varepsilon$ and then sampling $Y \in [\pm R]^d$ uniformly at random. To sample R we can set $R = \frac{\Delta}{\varepsilon}\sum_{i=0}^{d} \log U_i$, where each $U_i \in (0,1]$ is uniform and independent. This gives an algorithm (in the form of an explicit circuit) to sample $\mathcal{D}$ that uses only $O(d)$ real arithmetic operations, $d+1$ logarithms, and $2d+1$ independent uniform samples from $[0,1]$. □

We remark that the noise distribution in Theorem 4.1 is better than the Laplace mechanism *even for L_1 error* by a constant factor. In particular, the expected L_1 norm of the noise distribution in Theorem 4.1 is smaller than that of the Laplace mechanism with the same privacy level by a factor of $(2 - o_d(1))$. Moreover, the L_1 noise of the noise distribution in Theorem 4.1 stochastically dominates that of the Laplace mechanism:

Remark 4.2. *Fix $\varepsilon > 0$, $d \geq 1$, and $\Delta > 0$. Let $\mathcal{D}$ be the distribution on $\mathbb{R}^d$ from Theorem 4.1. Let $\mathcal{D}'$ be the distribution on $\mathbb{R}^d$ consisting of d independent samples from the Laplace distribution with scale $2d/\varepsilon n$. Both distributions provide ε-differential privacy when used to answer d one-way marginals. However*

$$\mathop{\mathbb{E}}_{Y\sim\mathcal{D}}\left[||Y||_1\right] = \frac{2}{1+1/d} \cdot \mathop{\mathbb{E}}_{Y'\sim\mathcal{D}'}\left[||Y'||_1\right]$$

and

$$\mathop{\mathbb{P}}_{Y\sim\mathcal{D}}\left[||Y||_1 > \alpha d\right] \leq \mathop{\mathbb{P}}_{Y'\sim\mathcal{D}'}\left[||Y'||_1 > \alpha d\right]$$

for all α.

```
Parameters: $\alpha \in (0,1)$.
Input: $D \in \{\pm 1\}^{n \times d}$.
Let
    $T = \left\lceil \frac{2d}{\log^4 d} \right\rceil, \qquad \sigma_0^2 = \frac{\alpha^2}{32 \log\log d}, \qquad \sigma_1^2 = \frac{\alpha^2}{8 \log^2 d}, \qquad \eta = \frac{2}{\alpha} \log^2 d.$
For $j \in [d]$, sample $a_j^0$ from $\mathcal{N}(\overline{D}_j, \sigma_0^2)$.
For $t \in [T]$ do:
  Sample $k_t \in [d]$ with
      $\mathbb{P}[k_t = k] = \frac{\exp(\eta |a_k^{t-1} - \overline{D}_k|)}{\sum_{j \in [d]} \exp(\eta |a_j^{t-1} - \overline{D}_j|)}.$
  Sample $a_{k_t}^t$ from $\mathcal{N}(\overline{D}_j, \sigma_1^2)$.
  For $j \in [d] \setminus \{k_t\}$, $a_j^t = a_j^{t-1}$.
Output $a_1^T, \cdots, a_d^T$.
```

Figure 2: Approximately DP Mechanism $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$

4.2 Approximate Differential Privacy

We now describe our approximately differentially private mechanism in Figure 2.

Proof of Theorem 1.3. Firstly, we consider the privacy of M: The data is used in d applications of the Gaussian mechanism with variance σ_0^2 and sensitivity $2/n$, T applications of the Gaussian mechanism with variance σ_1^2, and T applications of the exponential mechanism. By the composition and postprocessing properties of differential privacy (Dwork et al., 2010; Dwork and Roth, 2014), this implies that M satisfies $(4\tau + \sqrt{4\tau \log(1/\delta)}, \delta)$-differential privacy for all $\delta > 0$, where

$$\begin{aligned}
\tau =& \frac{2d}{\sigma_0^2 n^2} + \frac{2T}{\sigma_1^2 n^2} + \frac{8\eta^2 T}{n^2} \\
=& \frac{64d}{\alpha^2 n^2} \log\log d + \frac{T}{\alpha^2 n^2} \left(16 \log^2 d + 128 \log^4 d\right) \\
\leq& \frac{64d}{\alpha^2 n^2} \log\log d + \frac{1}{\alpha^2 n^2} \left(\frac{2d}{\log^4 d} + 1\right) \left(16 \log^2 d + 128 \log^4 d\right) \\
\leq& \frac{d}{\alpha^2 n^2} \left(64 \log\log d + 288 + \frac{144 \log^4 d}{d}\right) \\
\leq& \frac{d}{\alpha^2 n^2} \left(64 \log\log d + O(1)\right).
\end{aligned}$$

In particular, if $\varepsilon \le 1$ and $\delta \le e^{-8}$, it is sufficient that $\tau \le \varepsilon^2/5\log(1/\delta)$. Thus M is (ε,δ)-differentially private if

$$n \ge \sqrt{\frac{5d\log(1/\delta)}{\alpha^2\varepsilon^2}\left(64\log\log d + 288 + \frac{144\log^4 d}{d}\right)} \le \frac{(18+o(1))\sqrt{d\cdot\log\log d\cdot\log(1/\delta)}}{\alpha\varepsilon}.$$

Now we turn our attention to the accuracy of M: For $j \in [d]$, $t \in \{0,1,\cdots,T\}$, and $\hat{\alpha} > 0$, let $X_j^t(\hat{\alpha}) \in \{0,1\}$ be indicator of the event that $|a_j^T - \overline{D}_j| > \hat{\alpha}$ and let $X^t(\hat{\alpha}) = \sum_{j\in[d]} X_j^t(\hat{\alpha})$. The final answers are α-accurate if and only if $X^T(\alpha) = 0$. Thus we must show that $\mathbb{P}\left[X^T(\alpha) > 0\right] \le \beta$, where

$$\beta = e^{-2d/\log^8 d} + \frac{d(d+1)}{d^{\log d}} = \frac{1}{d^{\omega(1)}}.$$

This follows from the following three claims:

(i) All but T of the initial answers are $\frac{\alpha}{2}$-accurate. i.e. $\mathbb{P}\left[X^0(\alpha/2) > T\right] \le e^{-2d/\log^8 d}$.

(ii) In each of the T "fixing rounds," the exponential mechanism finds a bad answer. i.e. $\mathbb{P}\left[X_{k_t}^{t-1}(\alpha/2) = 0 \mid X^{t-1}(\alpha) > 0\right] \le \frac{1}{d^{\log d - 1}}$.

(iii) Each of the T resampled answers is accurate. i.e. $\mathbb{P}\left[X_{k_t}^t(\alpha/2) = 1\right] \le \frac{1}{d^{\log d}}$.

Claim (i) says that, with high probability, $X^0(\alpha/2) \le T$. Claims (ii) and (iii) imply that, with high probability, $X^t(\alpha/2)$ strictly decreases in each round, as long as $X^t(\alpha) > 0$. Thus either $X^t(\alpha) = 0$ for some $t \in [T]$ or $X^T(\alpha/2) = 0$. Claim (iii) implies that if $X^t(\alpha/2) = 0$ at some point, then it remains 0 for the rest of the execution and $X^t(\alpha/2) = 0$ with high probability. So, as long as all the good events in claims (i-iii) happen, the final answers are α-accurate. A union bound shows that this happens with probability $1-\beta$.

(i) Firstly, the random variables $X_1^0(\alpha/2), X_2^0(\alpha/2), \cdots, X_d^0(\alpha/2)$ are independent. For each $j \in [d]$,

$$\mathbb{E}\left[X_j^0(\alpha/2)\right] = \underset{G\sim\mathcal{N}(0,\sigma_0^2)}{\mathbb{P}}\left[|G| > \alpha/2\right] \le e^{-\alpha^2/8\sigma_0^2} \le \frac{1}{\log^4 d}.$$

Thus $\mathbb{E}\left[X^0(\alpha/2)\right] \le d/\log^4 d$. By Hoeffding's inequality,

$$\mathbb{P}\left[X_0(\alpha/2) > \mathbb{E}\left[X_0(\alpha/2)\right] + \lambda\right] \le e^{-2\lambda^2/d}$$

for all $\lambda > 0$. Setting $\lambda = d/\log^4 d$ verifies the first claim.

(ii) Now we must verify that, in each round, the exponential mechanism finds a bad query with high probability. We have

$$\mathbb{P}\left[X_{k_t}^{t-1}(\alpha/2) = 0\right] = \frac{\sum_{k\in[d]}\exp(\eta|a_k^{t-1} - \overline{D}_k|)\cdot\mathbb{I}(|a_k^{t-1} - \overline{D}_k| \le \alpha/2)}{\sum_{j\in[d]}\exp(\eta|a_j^{t-1} - \overline{D}_j|)} \le \frac{\exp(\eta\alpha/2)\cdot d}{\exp(\eta\alpha)\cdot X^{t-1}(\alpha)} \le d^{1-\log d},$$

assuming $X^{t-1}(\alpha) > 0$.

(iii) Finally, we have

$$\mathbb{P}\left[X^t_{k_t}(\alpha/2) = 1\right] = \underset{G\sim\mathcal{N}(0,\sigma_1^2)}{\mathbb{P}}\left[|G| > \alpha/2\right] \le e^{-\alpha^2/8\sigma_1^2} \le d^{-\log d}.$$

□

5 Applications of our Lower Bound

5.1 Private Empirical Risk Minimization

In the most well studied variant of the private empirical risk minimization problem, we are given a dataset $D = (x_1, \ldots, x_n) \in X^n$ where X is a some finite data universe, and each element of the data universe is associated with a 1-Lipschitz convex *risk function* (also known as a loss or penalty function) $\ell_x : B_2^d \to \mathbb{R}$. Here, B_2^d is the set $\left\{\theta \in \mathbb{R}^d \mid \|\theta\|_2 = 1\right\}$ of d-dimensional unit-vectors.[5]

The goal is to find the *empirical risk minimizer*

$$\theta^* = \underset{\theta\in B_2^d}{\arg\min}\, \frac{1}{n}\sum_{i=1}^n \ell_{x_i}(\theta).$$

Since the empirical risk minimizer θ^* may reveal sensitive information about the dataset D, when adding differential privacy as a constraint, we will settle for an *α-approximate empirical risk minimizer* $\hat{\theta}$ such that

$$\frac{1}{n}\sum_{i=1}^n \ell_{x_i}(\hat{\theta}) \le \frac{1}{n}\sum_{i=1}^n \ell_{x_i}(\theta^*) + \alpha.$$

Using the lower bounds for one-way marginals in Bun et al. (Bun et al., 2014), Bassily et al. (Bassily et al., 2014) showed that in order to find an α-approximate empirical risk minimizer for a d-dimensional empirical risk minimization problem while satisfying $(\varepsilon, o(1/n))$-differential privacy, it is necessary that $n \ge \tilde{\Omega}(\sqrt{d}/\varepsilon\alpha)$. Further, they showed that $n \ge \tilde{\Omega}(\sqrt{d}/\varepsilon\sqrt{\alpha})$ samples are necessary even when the risk functions are 1-strongly convex.[6] Using our improved lower bounds for one-way marginals, we can prove a more precise lower bound for both of these cases. As in Bassily et al., our lower bound applies for a very simple instance of convex empirical risk minimization.

[5] The assumptions that ℓ_x is 1-Lipschitz and that $\|\theta\|_2 = 1$ should be viewed as normalizations, and many other normalizations for the problem are possible and have been studied.

[6] A differentiable function $f : \mathbb{R}^d \to \mathbb{R}$ is 1-strongly convex if for every $x, x' \in \mathbb{R}^d$,

$$f(x') \ge f(x) + \nabla f(x)^\top (x' - x) + \tfrac{1}{2}\|x' - x\|_2^2.$$

Theorem 5.1 (Lower Bound for Private Convex ERM)**.** *For every $\varepsilon \in (0,1)$, every function $\delta = \delta(n)$ with $\delta \geq 2^{-o(n)}$ and $\delta \leq 1/n^{1+\Omega(1)}$ and every $\alpha \leq 1/10$, if $M : (B_2^d)^n \to B_2^d$ is (ε, δ)-differentially private and when given $(x_1, \cdots, x_n) \in (B_2^d)^n$ as input, outputs an α-approximate empirical risk minimizer $\hat{\theta} \in B_2^d$ satisfying*

$$\mathop{\mathbb{E}}_{\hat{\theta}=M(x_1,\cdots,x_n)}\left[\frac{1}{n}\sum_{i=1}^{n}\langle\hat{\theta}, x_i\rangle\right] \leq \min_{\theta \in B_2^d} \frac{1}{n}\sum_{i=1}^{n}\langle\theta, x_i\rangle + \alpha, \tag{9}$$

then

$$n \geq \Omega\left(\frac{\sqrt{d\log(1/\delta)}}{\varepsilon\alpha}\right).$$

The proof is effectively identical to Bassily et al. (2014, Theorem 5.3), but using Theorem 1.1 in place of the results of Bun et al. (Bun et al., 2014).[7]

We also can show a similar bound for a strongly convex empirical risk minimization problem:

Theorem 5.2 (Lower Bound for Private Strongly Convex ERM)**.** *For every $\varepsilon \in (0,1)$, every function $\delta = \delta(n)$ with $\delta \geq 2^{-o(n)}$ and $\delta \leq 1/n^{1+\Omega(1)}$ and every $\alpha \leq 1/10$, if $M : (B_2^d)^n \to B_2^d$ is (ε, δ)-differentially private and when given $(x_1, \cdots, x_n) \in (B_2^d)^n$ as input, outputs an α-approximate empirical risk minimizer $\hat{\theta}$ satisfying*

$$\mathop{\mathbb{E}}_{\hat{\theta}=M(x_1,\cdots,x_n)}\left[\frac{1}{n}\sum_{i=1}^{n}\|\hat{\theta} - x_i\|_2^2\right] \leq \min_{\theta \in B_2^d} \frac{1}{n}\sum_{i=1}^{n}\|\theta - x_i\|_2^2 + \alpha, \tag{10}$$

then

$$n \geq \Omega\left(\frac{\sqrt{d\log(1/\delta)}}{\varepsilon\sqrt{\alpha}}\right).$$

Observe that for every $x \in B_2^d$, the loss function $\ell_x(\theta) = \|\theta - x\|_2^2$ is 1-strongly convex and Lipschitz, so the problem described in Theorem 5.2 is in fact a valid instance of the empirical risk minimization problem described above.

Proof. Observe that

$$\theta^* = \frac{1}{n}\sum_{i=1}^{n} x_i = \arg\min_{\theta \in B_2^d} \frac{1}{n}\sum_{i=1}^{n}\|\theta - x_i\|_2^2.$$

[7] Although Bassily et al. (2014, Theorem 5.3) is not explictly stated as such, it is effectively a reduction from answering 1-way marginals with low L_1 error to solving the instance of empirical risk minimization described in our Theorem 5.1. Thus, we can immediately apply our new lower bounds for answer 1-way marginals to prove Theorem 5.1.

Moreover

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n}\|\hat{\theta}-x_i\|_2^2 =& \frac{1}{n}\sum_{i=1}^{n}\|\hat{\theta}-\theta^*\|_2^2+\|\theta^*-x_i\|_2^2+2\langle\hat{\theta}-\theta^*,\theta^*-x_i\rangle\\ =&\|\hat{\theta}-\theta^*\|_2^2+\frac{1}{n}\sum_{i=1}^{n}\|\theta^*-x_i\|_2^2+2\langle\hat{\theta}-\theta^*,\frac{1}{n}\sum_{i=1}^{n}\theta^*-x_i\rangle\\ =&\|\hat{\theta}-\theta^*\|_2^2+\min_{\theta\in B_2^d}\frac{1}{n}\sum_{i=1}^{n}\|\theta-x_i\|_2^2.\end{aligned}$$

By (10), this implies $\underset{\hat{\theta}}{\mathbb{E}}\left[\|\hat{\theta}-\theta^*\|_2^2\right]\leq\alpha$. Cauchy-Schwartz and Jensen's inequalities then give

$$\underset{\hat{\theta}}{\mathbb{E}}\left[\|\hat{\theta}-\theta^*\|_1\right]\leq\underset{\hat{\theta}}{\mathbb{E}}\left[\sqrt{d}\|\hat{\theta}-\theta^*\|_2\right]\leq\sqrt{\alpha}d. \tag{11}$$

Now we can reduce to one-way marginals. Define $M' : \{\pm1\}^{n\times d}\to[\pm1]^d$ as follows. On input $D\in\{\pm1\}^{n\times d}$, let $x_i = D_i/\sqrt{d}\in B_2^d$, compute $\hat{\theta}=M(x_1,\cdots,x_n)$ and return $\hat{\theta}\cdot\sqrt{d}$ truncated to $[\pm1]^d$. By (11), $\mathbb{E}\left[\|M'(D)-\overline{D}\|_1\right]\leq\sqrt{\alpha}d$. The result now follows from applying Theorem 1.1 to M'. □

5.2 Private PCA

Suppose our sensitive dataset is an $n\times d$ matrix where each row has norm at most 1. That is, $D\in(B_2^d)^n$. We would like to find the eigenvector corresponding to the largest eigenvalue of D, namely $v^*=\arg\max_{v:\|v\|_2=1}\|Dv\|_2^2$. Since this vector may reveal sensitive information about D, we will settle for an α-*approximate eigenvector*, which is a unit vector $\hat{v}$ such that $\|D\hat{v}\|_2^2\geq\|Dv^*\|_2^2-\alpha n$.

Using the lower bounds for one-way marginals in Bun et al. (Bun et al., 2014), Dwork et al. (Dwork et al., 2014) showed that in order to find an α-approximate eigenvector for D while satisfying $(1,o(1/n))$-differential privacy, it is necessary that $n\geq\tilde{\Omega}(\sqrt{d}/\varepsilon\alpha)$. Using our improved lower bounds for one-way marginals, we can prove a more precise bound.

Theorem 5.3. *For every $\varepsilon\in(0,1)$, every function $\delta=\delta(n)$ with $\delta\geq2^{-o(n)}$ and $\delta\leq1/n^{1+\Omega(1)}$ and every $\alpha\leq1/10$, if $M:(B_2^d)^n\to B_2^d$ is (ε,δ)-differentially private and when given $D\in(B_2^d)^n$ as input, outputs an α-approximate eigenvector of D, then*

$$n\geq\Omega\left(\frac{\sqrt{d\log(1/\delta)}}{\varepsilon\alpha}\right).$$

References

Bassily, R., Smith, A., and Thakurta, A. (2014). "Private Empirical Risk Minimization: Efficient Algorithms and Tight Error Bounds." In *Symposium on Foundations of Computer Science FOCS*, 464–473. IEEE Computer Society.

Blum, A., Dwork, C., McSherry, F., and Nissim, K. (2005). "Practical privacy: the SuLQ framework." In *PODS*, 128–138. ACM.

Boneh, D. and Shaw, J. (1998). "Collusion-Secure Fingerprinting for Digital Data." *IEEE Transactions on Information Theory*, 44(5): 1897–1905.

Bun, M., Ullman, J., and Vadhan, S. P. (2014). "Fingerprinting codes and the price of approximate differential privacy." In *STOC*, 1–10. ACM.

Dinur, I. and Nissim, K. (2003). "Revealing information while preserving privacy." In *PODS*, 202–210. ACM.

Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., and Naor, M. (2006a). "Our Data, Ourselves: Privacy Via Distributed Noise Generation." In *EUROCRYPT*, 486–503. Springer.

Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006b). "Calibrating Noise to Sensitivity in Private Data Analysis." In *TCC*, 265–284. Springer.

Dwork, C., McSherry, F., and Talwar, K. (2007). "The price of privacy and the limits of LP decoding." In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, 85–94.

Dwork, C. and Nissim, K. (2004). "Privacy-Preserving Datamining on Vertically Partitioned Databases." In *CRYPTO*, 528–544. Springer.

Dwork, C. and Roth, A. (2014). "The Algorithmic Foundations of Differential Privacy." *Foundations and Trends in Theoretical Computer Science*, 9(3-4): 211–407.

Dwork, C., Rothblum, G. N., and Vadhan, S. (2010). "Boosting and Differential Privacy." In *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, FOCS '10, 51–60. Washington, DC, USA: IEEE Computer Society.
URL http://dx.doi.org/10.1109/FOCS.2010.12

Dwork, C., Talwar, K., Thakurta, A., and Zhang, L. (2014). "Analyze gauss: optimal bounds for privacy-preserving principal component analysis." In *Symposium on Theory of Computing STOC*, 11–20. ACM.

Dwork, C. and Yekhanin, S. (2008). "New Efficient Attacks on Statistical Disclosure Control Mechanisms." In *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, 469–480.

Hardt, M. and Talwar, K. (2010). "On the Geometry of Differential Privacy." In *Symposium on Theory of Computing (STOC)*, 705–714. ACM.

Hardt, M. and Ullman, J. (2014). "Preventing False Discovery in Interactive Data Analysis is Hard." In *FOCS*. IEEE.

Kasiviswanathan, S. P., Rudelson, M., Smith, A., and Ullman, J. (2010). "The price of privately releasing contingency tables and the spectra of random matrices with correlated rows." In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, 775–784.

Kasiviswanathan, S. P. and Smith, A. (2008). "On the "Semantics" of Differential Privacy: A Bayesian Formulation." *CoRR*, abs/0803.3946.

McSherry, F. and Talwar, K. (2007). "Mechanism Design via Differential Privacy." In *Symposium on Foundations of Computer Science (FOCS)*, 94–103. IEEE Computer Society.

Nikolov, A., Talwar, K., and Zhang, L. (2013). "The geometry of differential privacy: the sparse and approximate cases." In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, 351–360.

Steinke, T. and Ullman, J. (2014). "Interactive Fingerprinting Codes and the Hardness of Preventing False Discovery." *CoRR*, abs/1410.1228.

Tardos, G. (2008). "Optimal probabilistic fingerprint codes." *J. ACM*, 55(2).

Ullman, J. (2013). "Answering $\mathrm{n}^{2+o(1)}$ counting queries with differential privacy is hard." In *STOC*, 361–370. ACM.

A Alternative Lower Bound for Pure Differential Privacy

It is known (Hardt and Talwar, 2010) that any ε-differentially private mechanism that answers d one-way marginals requires $n \geq \Omega(d/\varepsilon)$ samples. Our techniques yield an alternative simple proof of this fact.

Theorem A-1. *Let $M : \{\pm 1\}^{n \times d} \to [\pm 1]^d$ be a ε-differentially private mechanism. Suppose*

$$\forall D \in \{\pm 1\}^{n \times d} \quad \mathop{\mathbb{E}}_{M}\left[\left|\left|M(D) - \overline{D}\right|\right|_1\right] \leq 0.9d$$

Then $n \geq \Omega(d/\varepsilon)$.

The proof uses a special case of Hoeffding's Inequality:

Lemma A-2 (Hoeffding's Inequality)**.** *Let $X \in \{\pm 1\}^n$ be uniformly random and $a \in \mathbb{R}^n$ fixed. Then*

$$\mathop{\mathbb{P}}_{X}\left[\langle a, X \rangle > \lambda \left|\left|a\right|\right|_2\right] \leq e^{-\lambda^2/2}$$

for all $\lambda \geq 0$.

Proof of Theorem A-1. Let $x, x' \in \{\pm 1\}^d$ be independent and uniform. Let $D \in \{\pm 1\}^{n \times d}$ be n copies of x and, likewise, let $D' \in \{\pm 1\}^{n \times d}$ be n copies of x'. Let $Z = \langle M(D), x \rangle$ and $Z' = \langle M(D'), x \rangle$.

Now we give conflicting tail bounds for Z and Z', which we can relate by privacy.

By our hypothesis and Markov's inequality,

$$\begin{aligned}\mathbb{P}\left[Z \leq d/20\right] =& \mathbb{P}\left[\langle M(D), x \rangle \leq 0.05d\right] \\ =& \mathbb{P}\left[\langle \overline{D}, x \rangle - \langle \overline{D} - M(D), x \rangle \leq 0.05d\right] \\ =& \mathbb{P}\left[\langle \overline{D} - M(D), x \rangle \geq 0.95d\right] \\ \leq& \mathbb{P}\left[\left|\left|\overline{D} - M(D)\right|\right|_1 \geq 0.95d\right] \\ \leq& \frac{\mathbb{E}\left[\left|\left|\overline{D} - M(D)\right|\right|_1\right]}{0.95d} \\ \leq& \frac{0.9}{0.95} < 0.95.\end{aligned}$$

Since $M(D')$ is independent from x, we have

$$\forall \lambda \geq 0 \quad \mathbb{P}\left[Z' > \lambda\sqrt{d}\right] \leq \mathbb{P}\left[\langle M(D'), x \rangle > \lambda \left|\left|M(D')\right|\right|_2\right] \leq e^{-\lambda^2/2},$$

by Lemma A-2. In particular, setting $\lambda = \sqrt{d}/20$ gives $\mathbb{P}\left[Z' > d/20\right] \leq e^{-d/800}$.

Now D and D' are databases that differ in at most n rows, so privacy implies that

$$\mathbb{P}\left[M(D) \in S\right] \leq e^{n\varepsilon}\mathbb{P}\left[M(D') \in S\right]$$

for all S. Thus

$$\frac{1}{20} < \mathbb{P}\left[Z > \frac{d}{20}\right] = \mathbb{P}\left[M(D) \in S_x\right] \leq e^{n\varepsilon}\mathbb{P}\left[M(D') \in S_x\right] = e^{n\varepsilon}\mathbb{P}\left[Z' > \frac{d}{20}\right] \leq e^{n\varepsilon}e^{-d/800},$$

where

$$S_x = \left\{y \in [\pm 1]^d : \langle y, x \rangle > \frac{d}{20}\right\}.$$

Rearranging $1/20 < e^{n\varepsilon}e^{-d/800}$, gives

$$n > \frac{d}{800\varepsilon} - \frac{\log(20)}{\varepsilon},$$

as required. □