
Revisiting differentially private linear regression: optimal and adaptive prediction & estimation in unbounded domain

Yu-Xiang Wang *

University of California, Santa Barbara, CA
Amazon AWS AI, Palo Alto, CA

Abstract

We revisit the problem of linear regression under a differential privacy constraint. By consolidating existing pieces in the literature, we clarify the correct dependence of the feature, label and coefficient domains in the optimization error and estimation error, hence revealing the delicate price of differential privacy in statistical estimation and statistical learning. Moreover, we propose simple modifications of two existing DP algorithms: (a) posterior sampling, (b) sufficient statistics perturbation, and show that they can be *upgraded* into adaptive algorithms that are able to exploit data-dependent quantities and behave nearly optimally *for every instance*. Extensive experiments are conducted on both simulated data and real data, which conclude that both ADAOPS and ADASSP outperform the existing techniques on nearly all 36 data sets that we test on.

1 INTRODUCTION

Linear regression is one of the oldest tools for data analysis (Galton, 1886) and it remains one of the most commonly-used as of today (Draper & Smith, 2014), especially in social sciences (Agresti & Finlay, 1997), econometrics (Greene, 2003) and medical research (Armitage et al., 2008). Moreover, many nonlinear models are either intrinsically linear in certain function spaces, e.g., kernels methods, dynamical systems, or can be reduced to solving a sequence of linear regressions, e.g., iterative reweighted least square for generalized Linear models, gradient boosting for additive models and so on (see Friedman et al., 2001, for a detailed review).

In order to apply linear regression to sensitive data such as those in social sciences and medical studies, it is of-

ten needed to do so such that the privacy of individuals in the data set is protected. Differential privacy (Dwork et al., 2006b) is a commonly-accepted criterion that provides provable protection against identification and is resilient to arbitrary auxiliary information that might be available to attackers. In this paper, we focus on linear regression with (ϵ, δ) -differentially privacy (Dwork et al., 2006a).

Isn't it a solved problem? It might be a bit surprising why this is still a problem, since several general frameworks of differential privacy have been proposed that cover linear regression. Specifically, in the agnostic setting (without a data model), linear regression is a special case of differentially private empirical risk minimization (ERM), and its theoretical properties have been quite well-understood in a sense that the minimax lower bounds are known (Bassily et al., 2014) and a number of algorithms (Chaudhuri et al., 2011; Kifer et al., 2012) have been shown to match the lower bounds under various assumptions. In the statistical estimation setting where we assume the data is generated from a linear Gaussian model, linear regression is covered by the sufficient statistics perturbation approach for exponential family models (Dwork & Smith, 2010; Foulds et al., 2016), propose-test-release framework (Dwork & Lei, 2009) as well as the the subsample-and-aggregate framework (Smith, 2008), with all three approaches achieving the asymptotic efficiency in the fixed dimension ($d = O(1)$), large sample ($n \rightarrow \infty$) regime.

Despite these theoretical advances, very few empirical evaluations of these algorithms were conducted and we are not aware of a commonly-accepted best practice. Practitioners are often left puzzled about which algorithm to use for the specific data set they have. The nature of differential privacy often requires them to set parameters of the algorithm (e.g., how much noise to add) according to the diameter of the parameter domain, as well as properties of a hypothetical worst-case data set, which often leads to

Corresponding email: yuxiangw@cs.ucsb.edu

an inefficient use of their valuable data.

The main contribution of this paper is threefold:

1. We consolidated many bits and pieces from the literature and clarified the price of differential privacy in statistical estimation and statistical learning.
2. We carefully analyzed One Posterior Sample (OPS) and Sufficient Statistics Perturbation (SSP) for linear regression and proposed simple modifications of them into adaptive versions: ADAOPS and ADASSP. Both work near optimally for every problem instance without any hyperparameter tuning.
3. We conducted extensive real data experiments to benchmark existing techniques and concluded that the proposed techniques give rise to the more favorable privacy-utility tradeoff relative to existing methods.

Outline of this paper. In Section 2 we will describe the problem setup and explain differential privacy. In Section 3, we will survey the literature and discuss existing algorithms. Then we will propose and analyze our new method ADASSP and ADAOPS in Section 4 and conclude the paper with experiments in Section 5.

2 NOTATIONS AND SETUP

Throughout the paper we will use $X \in \mathbb{R}^{n \times d}$ and $\mathbf{y} \in \mathbb{R}^n$ to denote the design matrix and response vector. These are collections of data points $(x_1, y_1), \dots, (x_n, y_n) \in \mathcal{X} \times \mathcal{Y}$. We use $\|\cdot\|$ to denote Euclidean norm for vector inputs, ℓ_2 -operator norm for matrix inputs. In addition, for set inputs, $\|\cdot\|$ denotes the radius of the smallest Euclidean ball that contains the set. For example, $\|\mathcal{Y}\| = \sup_{y \in \mathcal{Y}} |y|$ and $\|\mathcal{X}\| = \sup_{x \in \mathcal{X}} \|x\|$. Let Θ be the domain of coefficients. Our results do not require Θ to be compact but existing approaches often depend on $\|\Theta\|$. \lesssim and \gtrsim denote greater than or smaller than up to a universal multiplicative constant, which is the same as the big $O(\cdot)$ and the big $\Omega(\cdot)$. $\tilde{O}(\cdot)$ hides at most a logarithmic term. \prec and \succ denote the standard semidefinite ordering of positive semi-definite (psd) matrices. $\cdot \vee \cdot$ and $\cdot \wedge \cdot$ denote the bigger or smaller of the two inputs.

We now define a few data dependent quantities. We use $\lambda_{\min}(X^T X)$ (abbrv. λ_{\min}) to denote the smallest eigenvalue of $X^T X$, and to make the implicit dependence in d and n clear from this quantity, we define $\alpha := \lambda_{\min} \frac{d}{n \|\mathcal{X}\|^2}$. One can think of α as a normalized smallest eigenvalue of $X^T X$ such that $0 \leq \alpha \leq 1$. Also, $1/\alpha$ is closely related to the condition number of $X^T X$.

Define the least square solution $\theta^* = (X^T X)^\dagger X^T \mathbf{y}$. It is the optimal solution to $\min_{\theta} \frac{1}{2} \|\mathbf{y} - X\theta\|^2 =: F(\theta)$. Similarly, we use $\theta_\lambda^* = (X^T X + \lambda I)^{-1} X^T \mathbf{y}$ denotes the optimal solution to the ridge regression objective $F_\lambda(\theta) = F(\theta) + \lambda \|\theta\|^2$.

In addition, we denote the global Lipschitz constant of F as $L^* := \|\mathcal{X}\|^2 \|\Theta\| + \|\mathcal{X}\| \|\mathcal{Y}\|$ and data-dependent local Lipschitz constant at θ^* as $L := \|\mathcal{X}\|^2 \|\theta^*\| + \|\mathcal{X}\| \|\mathcal{Y}\|$. Note that when $\Theta = \mathbb{R}^d$, $L^* = \infty$, but L will remain finite for every given data set.

Metric of success. We measure the performance of an estimator $\hat{\theta}$ in two ways.

First, we consider the optimization error $F(\hat{\theta}) - F(\theta^*)$ in expectation or with probability $1 - \rho$. This is related to the prediction accuracy in the distribution-free statistical learning setting.

Second, we consider how well the coefficients can be estimated under the linear Gaussian model:

$$\mathbf{y} = X\theta_0 + \mathcal{N}(0, \sigma^2 I_n)$$

in terms of $\mathbb{E}[\|\hat{\theta} - \theta_0\|^2]$ or in some cases $\mathbb{E}[\|\hat{\theta} - \theta_0\|^2 | E]$ where E is a high probability event.

The optimal error in either case will depend on the specific design matrix X , optimal solution θ^* , the data domain \mathcal{X}, \mathcal{Y} , the parameter domain Θ as well as θ_0, σ^2 in the statistical estimation setting.

Differential privacy. We will focus on estimators that are differential private, as defined below.

Definition 1 (Differential privacy (Dwork et al., 2006b)). *We say a randomized algorithm \mathcal{A} satisfies (ϵ, δ) -DP if for all fixed data set (X, \mathbf{y}) and data set (X', \mathbf{y}') that can be constructed by adding or removing one row (x, y) from (X, \mathbf{y}) , and for any measurable set \mathcal{S} over the probability of the algorithm*

$$\mathbb{P}(\mathcal{A}((X, \mathbf{y})) \in \mathcal{S}) \leq e^\epsilon \mathbb{P}(\mathcal{A}((X', \mathbf{y}')) \in \mathcal{S}) + \delta,$$

Parameter ϵ represents the amount of privacy loss from running the algorithm and δ denotes a small probability of failure. These are user-specified targets to achieve and the differential privacy guarantee is considered meaningful if $\epsilon \leq 1$ and $\delta \ll 1/n$ (see, e.g., Section 2.3.3 of Dwork et al., 2014a, for a comprehensive review).

The pursuit for adaptive estimators. Another important design feature that we will mention repeatedly in this paper is *adaptivity*. We call an estimator $\hat{\theta}$ *adaptive* if it behaves optimally simultaneously for a wide range of parameter choices. Being adaptive is of great practical

relevance because we do not need to specify the class of problems or worry about whether our specification is wrong (see examples of adaptive estimators in e.g., [Donoho, 1995](#); [Birgé & Massart, 2001](#)). *Adaptivity* is particularly important for differentially private data analysis because often we need to decide the amount of noise to add by the size of the domain. For example, an adaptive algorithm will not rely on conservative upper bounds of θ_0 , or a worst case λ_{\min} (which would be 0 on any \mathcal{X}), and it can take advantage of favorable properties when they exist in the data set. We want to design an estimator that does not take these parameters as inputs and behave nearly optimally for every fixed data set $X \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}$ under a variety of configuration of $\|\mathcal{X}\|, \|\mathcal{Y}\|, \|\Theta\|$.

3 A SURVEY OF PRIOR WORK

In this section, we summarize existing theoretical results in linear regression with and without differential privacy constraints. We will start with lower bounds.

3.1 Information-theoretic lower bounds

Lower bounds under linear Gaussian model. Under the statistical assumption of linear Gaussian model $\mathbf{y} = X\theta_0 + \mathcal{N}(0, \sigma^2)$, the minimax risk for both estimation and prediction are crisply characterized for each fixed design matrix X :

$$\inf_{\hat{\theta}} \sup_{\theta_0 \in \mathbb{R}^d} \mathbb{E}[F(\hat{\theta}) - F(\theta_0)|X] = \frac{d\sigma^2}{2}, \quad (1)$$

and if we further assume that $n \geq d$ and $X^T X$ is invertible (for identifiability), then

$$\inf_{\hat{\theta}} \sup_{\theta_0 \in \mathbb{R}^d} \mathbb{E}[\|\hat{\theta} - \theta_0\|_2^2|X] = \sigma^2 \text{tr}[(X^T X)^{-1}]. \quad (2)$$

In the above setup, $\hat{\theta}$ is any measurable function of $\hat{\mathbf{y}}$ (note that X is fixed). These are classic results that can be found in standard statistical decision theory textbooks (See, e.g., [Wasserman, 2013](#), Chapter 13).

Under the same assumptions, the Cramer-Rao lower bound mandates that the covariance matrix of any unbiased estimator $\hat{\theta}$ of θ_0 to obey that

$$\text{Cov}(\hat{\theta}) \succ \sigma^2 (X^T X)^{-1}. \quad (3)$$

This bound applies to every problem instance separately and also implies a sharp lower bound on the prediction variance on every data point x . More precisely, $\text{Var}(\hat{\theta}^T x) \geq \sigma^2 x^T (X^T X)^{-1} x$ for any x .

Minimax risk (1), (2) and the Cramer-Rao lower bound (3) are simultaneously attained by θ^* .

Statistical learning lower bounds. Perhaps much less well-known, linear regression is also thoroughly studied in the distribution-free statistical learning setting, where the only assumption is that the data are drawn iid from some unknown distribution \mathcal{P} defined on some compact domain $\mathcal{X} \times \mathcal{Y}$. Specifically, let the risk ($\mathbb{E}[\text{loss}]$) be

$$R(\theta) = \mathbb{E}_{(x,y) \sim \mathcal{P}} \left[\frac{1}{2} (x^T \theta - y)^2 \right] = \frac{1}{n} \mathbb{E}_{(X,\mathbf{y}) \sim \mathcal{P}^n} [F(\theta)].$$

[Shamir \(2015\)](#) showed that when Θ, \mathcal{X} are \mathcal{Y} are Euclidean balls,

$$\inf_{\hat{\theta}} \sup_{\mathcal{P}} \left[\mathbb{E}[n \cdot R(\hat{\theta})] - \inf_{\theta \in \Theta} [n \cdot R(\theta)] \right] \gtrsim \min\{n\|\mathcal{Y}\|^2, \|\Theta\|^2\|\mathcal{X}\|^2 + d\|\mathcal{Y}\|^2, \sqrt{n}\|\Theta\|\|\mathcal{X}\|\|\mathcal{Y}\|\}. \quad (4)$$

where $\hat{\theta}$ be any measurable function of the data set X, \mathbf{y} to Θ and the expectation is taken over the data generating distribution $X, \mathbf{y} \sim \mathcal{P}^n$. Note that to be compatible to other bounds that appear in this paper, we multiplied the $R(\cdot)$ by a factor of n . Informally, one can think of $\|\mathcal{Y}\|$ as σ in (1) so both terms depend on $d\sigma^2$ (or $d\|\mathcal{Y}\|^2$), but the dependence on $\|\Theta\|\|\mathcal{X}\|$ is new for the distribution-free setting.

[Koren & Levy \(2015\)](#) later showed that this lower bound is matched up to a constant by Ridge Regression with $\lambda = 1$ and both [Koren & Levy \(2015\)](#) and [Shamir \(2015\)](#) conjecture that ERM without additional regularization should attain the lower bound (4). If the conjecture is true, then the unconstrained OLS is simultaneously optimal for all distributions supported on the smallest ball that contains all data points in X, \mathbf{y} for any Θ being an ℓ_2 ball with radius larger than $\|\theta^*\|$.

Lower bounds with (ϵ, δ) -privacy constraints. Suppose that we further require $\hat{\theta}$ to be (ϵ, δ) -differentially private, then there is an additional price to pay in terms of how accurately we can approximate the ERM solution. Specifically, the lower bounds for the *empirical* excess risk for differentially private ERM problem in ([Bassily et al., 2014](#)) implies that for $\delta < 1/n$ and sufficiently large n :

1. There exists a triplet of $(\mathcal{X}, \mathcal{Y}, \Theta) \subset \mathbb{R}^d \times \mathbb{R} \times \mathbb{R}^d$, such that

$$\inf_{\hat{\theta} \text{ is } (\epsilon, \delta)\text{-DP}} \sup_{X \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}^n} \left[F(\hat{\theta}) - \inf_{\theta \in \Theta} F(\theta) \right] \gtrsim \min\left\{n\|\mathcal{Y}\|^2, \frac{\sqrt{d}(\|\mathcal{X}\|^2\|\Theta\|^2 + \|\mathcal{X}\|\|\Theta\|\|\mathcal{Y}\|)}{\epsilon}\right\}. \quad (5)$$

2. Consider the class of data set \mathcal{S} where all data sets $X \in \mathcal{S} \subset \mathcal{X}^n$ obeys that the inverse condition number $\alpha \geq \alpha^* \geq \frac{d^{1.5}(\|\mathcal{X}\|\|\Theta\| + \|\mathcal{Y}\|)}{n\|\mathcal{X}\|\|\Theta\|\epsilon}$. There exists a

¹This requires $\lambda_{\min} \geq \sqrt{dL}/\epsilon$ for all data sets X .

triplet of $(\mathcal{X}, \mathcal{Y}, \Theta) \subset \mathbb{R}^d \times \mathbb{R} \times \mathbb{R}^d$ such that

$$\hat{\theta} \text{ is } (\epsilon, \delta)\text{-DP } X \in \mathcal{S}, \mathbf{y} \in \mathcal{Y}^n \left[F(\hat{\theta}) - \inf_{\theta \in \Theta} F(\theta) \right] \quad (6)$$

$$\gtrsim \min \left\{ n \|\mathcal{Y}\|^2, \frac{d^2 (\|\mathcal{X}\| \|\Theta\| + \|\mathcal{Y}\|)^2}{n \alpha^* \epsilon^2} \right\}.$$

These bounds are attained by a number of algorithms, which we will go over in Section 3.2.

Comparing to the non-private minimax rates on prediction accuracy, the bounds look different in several aspects. First, neither rate for prediction error in (1) or (4) depends on whether the design matrix X is well-conditioned or not, while α^* appears explicitly in (6). Secondly, the dependence on $\|\Theta\|, \|\mathcal{X}\|, \|\mathcal{Y}\|, d, n$ are different, which makes it hard to tell whether the optimization error lower bound due to privacy requirement is limiting. One may ask the following question:

When is privacy *for free* in statistical learning?

Specifically, what is the smallest ϵ such that an (ϵ, δ) -DP algorithm matches the minimax rate in (4)? The answer really depends on the relative scale of $\|\mathcal{X}\| \|\Theta\|$ and $\|\mathcal{Y}\|$ and that of n, d . When $\|\mathcal{X}\| \|\Theta\| \asymp \|\mathcal{Y}\|$, (5) says that (ϵ, δ) -DP algorithms can achieve the nonconvex minimax rate provided that $\epsilon \gtrsim \min \left\{ \frac{1}{\sqrt{d}} \sqrt{\frac{d}{n}}, \sqrt{\frac{d^2}{n^{1.5} \alpha^*}} \sqrt{\frac{d}{n \alpha^*}} \right\}$. On the other hand, if $\|\mathcal{X}\| \|\Theta\| \asymp \sqrt{d} \|\mathcal{Y}\|^2$ and $n > d$, then we need $\epsilon \gtrsim \min \left\{ \sqrt{d} \sqrt{\frac{d^{3/2}}{n}}, \frac{d}{\sqrt{n \alpha^*}} \sqrt{\frac{d^{3/2}}{n \alpha^*}} \right\}$.

The regions are illustrated graphically in Figure 1. In the first case, there is a large region upon $n \gtrsim d$, where meaningful differential privacy (with $\epsilon \leq 1$ and $\delta = o(1/n)$) can be achieved without incurring a significant toll relative to (4). In the second case, we need at least $n \gtrsim d^2$ to achieve ‘‘privacy-for-free’’ in the most favorable case where $\alpha^* = 1$. In the case when X could be rank-deficient, then it is infeasible to achieve ‘‘privacy for free’’ no matter how large n is.

It might be tempting to conclude that one should always prefer Case 1 over Case 2. This is unfortunately not true because the artificial restriction of the model class via a bounded $\|\Theta\|$ also weakens our non-private baseline. In other word, the best solution within a small Θ might be significantly worse than the best solution in \mathbb{R}^d .

In practice, it is hard to find a Θ with a small radius that fits all purposes³ and it is unreasonable to assume $\alpha^* > 0$.

²This is arguably the more relevant setting. Note that if $x \sim \mathcal{N}(0, I_d)$ and θ is fixed, then $x^T \theta = O_P(d^{-1/2} \|x\| \|\theta\|)$.

³If $\|\Theta\| \gg \|\theta^*\|$ then the constraint becomes limiting. If $\|\theta^*\| \ll \|\Theta\|$ instead, then calibrating the noise according to $\|\Theta\|$ will inject more noise than necessary.

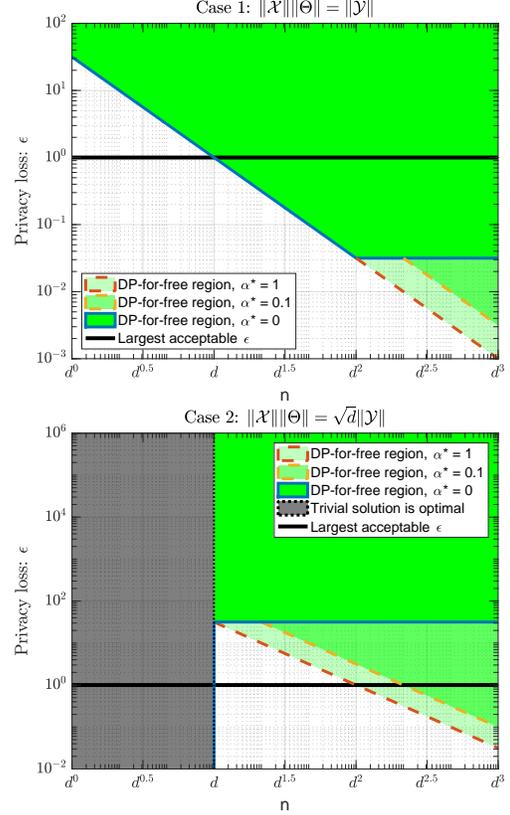


Figure 1: Illustration of the region of ϵ where DP can be obtained without losing minimax rate (4). [Zoom to see!]

This motivates us to go beyond the worst-case and come up with *adaptive* algorithms that work without knowing $\|\theta^*\|$ and α while achieving the minimax rate for the class with $\|\Theta\| = \|\theta^*\|$ and $\alpha^* = \alpha$ (in hindsight).

In Appendix B, we provide an alternative illustration of the lower bounds and highlight the price of differential privacy for different configuration of n, d, α, ϵ .

3.2 Existing algorithms and our contribution

We now survey the following list of five popular algorithms in differentially private learning and highlight the novelty in our proposals⁴.

1. Sufficient statistics perturbation (SSP) (Vu & Slavkovic, 2009; Foulds et al., 2016): Release $X^T X$ and $X \mathbf{y}$ differentially privately and then output $\hat{\theta} = (\widehat{X^T X})^{-1} \widehat{X \mathbf{y}}$.
2. Objective perturbation (OBJPERT) (Kifer et al.,

⁴While we try to be as comprehensive as possible, the literature has grown massively and the choice of this list is limited by our knowledge and opinions.

2012): $\hat{\theta} = \operatorname{argmin} F(\theta) + 0.5\lambda\|\theta\|^2 + Z^T\theta$ with an appropriate λ and Z is an appropriately chosen iid Gaussian random vector.

3. Subsample and Aggregate (Sub-Agg) (Smith, 2008; Dwork & Smith, 2010): Subsample many times, apply debiased MLE to each subset and then randomize the way we aggregate the results.
4. Posterior sampling (OPS) (Mir, 2013; Dimitrakakis et al., 2014; Wang et al., 2015; Minami et al., 2016): Output $\hat{\theta} \sim P(\theta) \propto e^{-\gamma(F(\theta)+0.5\lambda\|\theta\|^2)}$ with parameters γ, λ .
5. NOISYSGD (Bassily et al., 2014): Run SGD for a fixed number of iterations with additional Gaussian noise added to the stochastic gradient evaluated on one randomly-chosen data point.

We omit detailed operational aspects of these algorithms and focus our discussion on their theoretical guarantees. Interested readers are encouraged to check out each paper separately. These algorithms are proven under different scalings and assumptions. To ensure fair comparison, we make sure that all results are converted to our setting under a subset of the following assumptions.

A.1 $\|\mathcal{X}\|$ is bounded, $\|\mathcal{Y}\|$ is bounded.

A.2 $\|\Theta\|$ is bounded.

A.3 All possible data sets X obey that the smallest eigenvalue $\lambda_{\min}(X^T X)$ is greater than $\frac{n\|\mathcal{X}\|^2}{d}\alpha^*$.

Note that A.3 is a restriction on the domain of the data set, rather than the domain of individual data points in the data set of size n . While it is a little unconventional, it is valid to define differential privacy within such a restricted space of data sets. It is the same assumption that we needed to assume for the lower bound in (6) to be meaningful. As in Koren & Levy (2015), we simplify the expressions of the bound by assuming $\|\mathcal{Y}\| \leq \|\mathcal{X}\|\|\Theta\|$, and in addition, we assume that $\|\mathcal{Y}\| \lesssim \|\mathcal{X}\|\|\theta^*\|$.

Table 1 summarizes the upper bounds of optimization error the aforementioned algorithms in comparison to our two proposals: ADAOPS and ADASSP. Comparing the rates to the lower bounds in the previous section, it is clear that NoisySGD, OBJPERT both achieve the minimax rate in optimization error but their hyperparameter choice depends on the unknown $\|\Theta\|$ and α^* . SSP is adaptive to α and $\|\theta^*\|$ but has a completely different type of issue — it can fail arbitrarily badly for regime covered under (5), and even for well-conditioned problems, its theoretical guarantees only kick in as n gets very large. Our proposed algorithms ADAOPS and ADASSP are able to simultaneously switch between the two regimes and get the best of both worlds.

Table 2 summarizes the upper bounds for estimation. The second row compares the approximation of θ^* in MSE and the third column summarizes the statistical efficiency of the DP estimators relative to the MLE: θ^* under the linear Gaussian model. All algorithms except OPS are asymptotically efficient. For the interest of (ϵ, δ) -DP, SSP has the fastest convergence rate and does not explicitly depend on the smallest eigenvalue, but again it behaves differently when n is small, while ADAOPS and ADASSP work optimally (up to a constant) for all n .

3.3 Other related work

The problem of adaptive estimation is closely related to model selection (see, e.g., Birgé & Massart, 2001) and an approach using Bayesian Information Criteria was carefully studied in the differential private setting for the problem of ℓ_1 constrained ridge regression by Lei et al. (2017). Their focus is different to ours in that they care about inferring the correct model, while we take the distribution-free view. Linear regression is also studied in many more specialized setups, e.g., high dimensional linear regression (Kifer et al., 2012; Talwar et al., 2014, 2015), statistical inference (Sheffet, 2017) and so on. For the interest of this paper, we focus on the standard regime of linear regression where $d < n$ and do not use sparsity or ℓ_1 constraint set to achieve the $\log(d)$ dependence. That said, we acknowledge that Sheffet (2017) analyzed SSP under the linear Gaussian model (the third row in Table 2 and their techniques of adaptively adding regularization have inspired ADASSP.

4 MAIN RESULTS

In this section, we present and analyze ADAOPS and ADASSP that achieve the aforementioned adaptive rate. The pseudo-code of these two algorithms are given in Algorithm 1 and Algorithm 2.

The idea of both algorithms is to release key data-dependent quantities differentially privately and then use a high probability confidence interval of these quantities to calibrate the noise to privacy budget as well as to choose the ridge regression’s hyperparameter λ for achieving the smallest prediction error. Specifically, ADAOPS requires us to release both the smallest eigenvalue λ_{\min} of $X^T X$ and the local Lipschitz constant $L := \|\mathcal{X}\|(\|\mathcal{X}\|\|\theta_x^*\| + \|\mathcal{Y}\|)$, while ADASSP only needs the smallest eigenvalue λ_{\min} .

In both ADASSP and ADAOPS, we choose λ by minimizing an upper bound of $F(\hat{\theta}) - F(\theta^*)$ in the form of “variance” and “bias”

$$\tilde{O}\left(\frac{d\|\mathcal{X}\|^4\|\theta^*\|^2}{\lambda + \lambda_{\min}}\right) + \lambda\|\theta^*\|^2.$$

Table 1: Summary of optimization error bounds. This table compares the (expected or high probability) additive suboptimality of different differentially private linear regression procedures relative to the (non-private) empirical risk minimizer θ^* . In particular, the results for NoisySGD holds in expectation and everything else with probability $1 - \rho$ (hiding at most a logarithmic factor in $\sqrt{1/\rho}$). Constant factors are dropped for readability.

	$F(\hat{\theta}) - F(\theta^*)$	Assumptions	Remarks
NoisySGD	$\frac{\sqrt{d \log(\frac{n}{\delta})} \ \mathcal{X}\ ^2 \ \Theta\ ^2}{\epsilon}$	A.1, A.2	Theorem 2.4 (Part 1) of (Bassily et al., 2014).
	$\frac{d^2 \log(\frac{n}{\delta}) \ \Theta\ ^2}{\alpha^* n \epsilon^2}$	A.1, A.2, A.3	Theorem 2.4 (Part 2) of (Bassily et al., 2014)
OBJPERT	$\frac{\sqrt{d \log(\frac{1}{\delta})} \ \mathcal{X}\ ^2 \ \Theta\ \ \theta^*\ }{\epsilon}$	A.1, A.2	Theorem 4 (Part 2) of (Kifer et al., 2012).
	$\frac{d^2 \log(\frac{1}{\delta}) \ \Theta\ ^2}{\alpha^* n \epsilon^2}$	A.1, A.2, A.3	Theorem 5 & Appendix E.2 of (Kifer et al., 2012).
OPS	$\frac{d \ \mathcal{X}\ ^2 \ \Theta\ ^2}{\epsilon}$	A.1, A.2	Results for ϵ -DP (Wang et al., 2015)
SSP	$\frac{d^2 \log(\frac{1}{\delta}) \ \mathcal{X}\ ^2 \ \theta^*\ ^2}{\alpha n \epsilon^2}$	A.1	Adaptive to $\ \theta^*\ , X, \alpha$, but requires $n = \Omega(\frac{d^{1.5} \log(4/\delta)}{\alpha \epsilon})^5$.
ADAOPS & ADASSP	$\frac{\sqrt{d \log(\frac{1}{\delta})} \ \mathcal{X}\ ^2 \ \theta^*\ ^2}{\epsilon} \wedge \frac{d^2 \log(\frac{1}{\delta}) \ \theta^*\ ^2}{\alpha n \epsilon^2}$	A.1	Adaptive in $\ \theta^*\ , X, \alpha$.

Table 2: Summary of estimation error bounds under the linear Gaussian model. On the second column we compare the approximation of MLE θ^* in mean square error up to a universal constant. On the third column, we compare the relative efficiency. The relative efficiency bounds are simplified with the assumption of $\alpha = \Omega(1)$, which implies that $\text{tr}[(X^T X)^{-1}] = O(d^2 n^{-1} \|\mathcal{X}\|^{-2})$ and $\text{tr}[(X^T X)^{-2}] = O(d n^{-1} \|\mathcal{X}\|^{-2} \text{tr}[(X^T X)^{-1}])$. $\tilde{O}(\cdot)$ hides $\text{polylog}(1/\delta)$ terms.

	Approx. MLE: $\mathbb{E} \ \hat{\theta} - \theta^*\ ^2$	Rel. efficiency: $\frac{\mathbb{E} \ \hat{\theta} - \theta_0\ ^2}{\mathbb{E} \ \theta^* - \theta_0\ ^2}$	Remarks
Sub-Agg	$O\left(\frac{\text{poly}(d, \ \Theta\ , \ \mathcal{X}\ , \alpha^{-1})}{\epsilon^{6/5} n^{6/5}}\right)$	$1 + \tilde{O}\left(\frac{\text{poly}(d, \ \Theta\ , \ \mathcal{X}\)}{n^{1/5} \epsilon^{6/5}}\right)$	ϵ -DP, suboptimal in n , possibly also in d (Dwork & Smith, 2010).
OPS	$O\left(\frac{\ \mathcal{X}\ ^2 \ \Theta\ ^2}{\epsilon} \text{tr}[(X^T X)^{-1}]\right)$	$\tilde{O}\left(\frac{\ \mathcal{X}\ ^2 \ \Theta\ ^2}{\epsilon \sigma^2}\right)$	ϵ -DP, adaptive in X , but not asymptotically efficient (Wang et al., 2015).
SSP	$O\left(\frac{\log(\frac{1}{\delta}) \ \mathcal{X}\ ^4 \ \theta^*\ ^2}{\epsilon^2} \text{tr}[(X^T X)^{-2}]\right)$	$1 + \tilde{O}\left(\frac{d \ \mathcal{X}\ ^2 \ \theta_0\ ^2}{n \epsilon^2 \sigma^2} + \frac{d^3}{n^2 \epsilon^2}\right)$	Adaptive in $\ \theta^*\ , X$, no explicit dependence on α , but requires large n . (Sheffet, 2017, Theorem 5.1)
ADAOPS & ADASSP	$O\left(\frac{d \log(\frac{1}{\delta}) \ \mathcal{X}\ ^2 \ \theta^*\ ^2}{\alpha n \epsilon^2} \text{tr}[(X^T X)^{-1}]\right)$	$1 + \tilde{O}\left(\frac{d \ \mathcal{X}\ ^2 \ \theta_0\ ^2}{n \epsilon^2 \sigma^2} + \frac{d^3}{n^2 \epsilon^2}\right)$	Adaptive in $\ \theta^*\ , X, \alpha$.

Algorithm 1 ADAOPS: One-Posterior Sample estimator with adaptive regularization

input Data X, \mathbf{y} . Privacy budget: ϵ, δ , Bounds: $\|\mathcal{X}\|, \|\mathcal{Y}\|$.

1. Calculate the minimum eigenvalue $\lambda_{\min}(X^T X)$.
2. Sample $Z \sim \mathcal{N}(0, 1)$ and privately release

$$\tilde{\lambda}_{\min} = \max \left\{ \lambda_{\min} + \frac{\sqrt{\log(6/\delta)}}{\epsilon/4} Z - \frac{\log(6/\delta)}{\epsilon/4}, 0 \right\}.$$

3. Set $\bar{\epsilon}$ as the positive solution of the quadratic equation

$$\bar{\epsilon}^2 / (2 \log(6/\delta)) + \bar{\epsilon} - \epsilon/4 = 0.$$

4. Set $\varrho = 0.05$, $C_1 = (d/2 + \sqrt{d \log(1/\varrho)} + \log(1/\varrho)) \log(6/\delta) / \bar{\epsilon}^2$, $C_2 = \log(6/\delta) / (\epsilon/4)$, $t_{\min} = \max \left\{ \frac{\|\mathcal{X}\|^2 (1 + \log(6/\delta))}{2\epsilon} - \tilde{\lambda}_{\min}, 0 \right\}$ and solve

$$\lambda = \underset{t \geq t_{\min}}{\operatorname{argmin}} \frac{\|\mathcal{X}\|^4 C_1 [1 + \|\mathcal{X}\|^2 / (t + \tilde{\lambda}_{\min})]^{2C_2}}{t + \tilde{\lambda}_{\min}} + t. \quad (7)$$

which has a unique solution.

5. Calculate $\hat{\theta} = (X^T X + \lambda I)^{-1} X^T \mathbf{y}$.

6. Sample $Z \sim \mathcal{N}(0, 1)$ and privately release

$$\Delta = \log(\|\mathcal{Y}\| + \|\mathcal{X}\| \|\hat{\theta}\|) + \frac{\log(1 + \|\mathcal{X}\|^2 / (\lambda + \tilde{\lambda}_{\min}))}{\epsilon / (4 \sqrt{\log(6/\delta)})} Z +$$

$$\frac{\log(1 + \|\mathcal{X}\|^2 / (\lambda + \tilde{\lambda}_{\min}))}{\epsilon / (4 \log(6/\delta))}. \text{ Set } \tilde{L} := \|\mathcal{X}\| e^{\Delta}.$$

7. Calibrate noise by choosing $\tilde{\epsilon}$ as the positive solution of the quadratic equation

$$\frac{\tilde{\epsilon}^2}{2} \left[\frac{1}{\log(6/\delta)} \frac{1 + \log(6/\delta)}{\log(6/\delta)} \right] + \tilde{\epsilon} - \epsilon/2 = 0. \quad (8)$$

and then set $\gamma = \frac{(\tilde{\lambda}_{\min} + \lambda) \tilde{\epsilon}^2}{\log(6/\delta) \tilde{L}^2}$.

output $\tilde{\theta} \sim p(\theta | X, \mathbf{y}) \propto e^{-\frac{\gamma}{2} (\|\mathbf{y} - X\theta\|^2 + \lambda \|\theta\|^2)}$.

Note that while $\|\theta^*\|^2$ cannot be privately released in general due to unbounded sensitivity, it appears in both terms and do not enter the decision process of finding the optimal λ that minimizes the bound. This convenient feature follows from our assumption that $\|\mathcal{Y}\| \lesssim \|\mathcal{X}\| \|\theta^*\|$. Dealing with the general case involving an arbitrary $\|\mathcal{Y}\|$ is an intriguing open problem.

A tricky situation for ADAOPS is that the choice of γ depends on λ through \tilde{L} , which is the local Lipschitz constant at the ridge regression solution θ_λ^* . But the choice of λ also depends on γ since the ‘‘variance’’ term above is inversely proportional to γ . Our solution is to express \tilde{L} (hence γ) as a function of λ and solve the nonlinear univariate optimization problem (7).

We are now ready to state the main results.

Theorem 2. *Algorithm 1 outputs $\tilde{\theta}$ which obeys that*

- (i) *It satisfies (ϵ, δ) -DP.*

Algorithm 2 ADASSP: Sufficient statistics perturbation with adaptive damping

input Data X, \mathbf{y} . Privacy budget: ϵ, δ , Bounds: $\|\mathcal{X}\|, \|\mathcal{Y}\|$.

1. Calculate the minimum eigenvalue $\lambda_{\min}(X^T X)$.

2. Privately release $\tilde{\lambda}_{\min} = \max \left\{ \lambda_{\min} + \frac{\sqrt{\log(6/\delta)}}{\epsilon/3} \|\mathcal{X}\|^2 Z - \frac{\log(6/\delta)}{\epsilon/3} \|\mathcal{X}\|^2, 0 \right\}$,

where $Z \sim \mathcal{N}(0, 1)$.

3. Set $\lambda = \max \left\{ 0, \frac{\sqrt{d \log(6/\delta) \log(2d^2/\rho)} \|\mathcal{X}\|^2}{\epsilon/3} - \tilde{\lambda}_{\min} \right\}$

4. Privately release $\widehat{X^T X} = X^T X + \frac{\sqrt{\log(6/\delta)} \|\mathcal{X}\|^2}{\epsilon/3} Z$ for $Z \in \mathbb{R}^{d \times d}$ is a symmetric matrix and every element from the upper triangular matrix is sampled from $\mathcal{N}(0, 1)$.

5. Privately release $\widehat{X \mathbf{y}} = X \mathbf{y} + \frac{\sqrt{\log(6/\delta)} \|\mathcal{X}\| \|\mathcal{Y}\|}{\epsilon/3} Z$ for $Z \sim \mathcal{N}(0, I_d)$.

output $\tilde{\theta} = (\widehat{X^T X} + \lambda I)^{-1} \widehat{X \mathbf{y}}$

- (ii) *Assume $\|\mathcal{Y}\| \lesssim \|\mathcal{X}\| \|\theta^*\|$. With probability $1 - \varrho$, $F(\tilde{\theta}) - F(\theta^*) \leq$*

$$O \left(\frac{\sqrt{d + \log(\frac{1}{\varrho})} \|\mathcal{X}\|^2 \|\theta^*\|^2}{\epsilon / \sqrt{\log(\frac{1}{\varrho})}} \wedge \frac{d [d + \log(\frac{1}{\varrho})] \|\theta^*\|^2}{\alpha n \epsilon^2 / \log(\frac{1}{\varrho})} \right).$$

- (iii) *Assume that $\mathbf{y} | X$ obeys a linear Gaussian model and X is full-rank. Then there is an event E satisfying $\mathbb{P}(E) \geq 1 - \delta/3$ and $E \perp \mathbf{y} | X$, such that $\mathbb{E}[\tilde{\theta} | X, E] = \theta_0$ and*

$$\operatorname{Cov}[\tilde{\theta} | X, E] \prec \left(1 + O \left(\frac{\tilde{C} d \log(6/\delta)}{\sigma^2 \alpha n \epsilon^2} \right) \right) \sigma^2 (X^T X)^{-1}$$

where constant

$$\tilde{C} := \|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 (\|\theta_0\|^2 + \sigma^2 \operatorname{tr}[(X^T X)^{-1}]).$$

The proof, deferred to Appendix D, makes use of a fine-grained DP-analysis through the recent per instance DP techniques (Wang, 2017) and then convert the results to DP by releasing data dependent bounds of α and the magnitude of a ridge-regression output θ_λ^* with an adaptively chosen λ . Note that $\|\theta_\lambda^*\|$ does not have a bounded global sensitivity. The method to release it differentially privately (described in Lemma 12) is part of our technical contribution.

The ADASSP algorithm is simpler and enjoys slightly stronger theoretical guarantees.

Theorem 3. *Algorithm 2 outputs $\tilde{\theta}$ which obeys that*

- (i) *It satisfies (ϵ, δ) -DP.*

- (ii) *Assume $\|\mathcal{Y}\| \lesssim \|\mathcal{X}\| \|\theta^*\|$. With probability $1 - \varrho$, $F(\tilde{\theta}) - F(\theta^*) \leq$*

$$O \left(\frac{\sqrt{d \log(\frac{d^2}{\varrho})} \|\mathcal{X}\|^2 \|\theta^*\|^2}{\epsilon / \sqrt{\log(\frac{6}{\varrho})}} \wedge \frac{\|\mathcal{X}\|^4 \|\theta^*\|^2 \operatorname{tr}[(X^T X)^{-1}]}{\epsilon^2 / [\log(\frac{6}{\varrho}) \log(\frac{d^2}{\varrho})]} \right)$$

(iii) Assume that $\mathbf{y}|X$ obeys a linear Gaussian model and X has a sufficiently large α . Then there is an event E satisfying $\mathbb{P}(E) \geq 1 - \delta/3$ and $E \perp \mathbf{y}|X$, such that $\mathbb{E}[\tilde{\theta}|X, E] = \theta_0$ and

$$\begin{aligned} & \mathbb{E}[\|\tilde{\theta} - \theta_0\|^2|X, E] \\ &= \sigma^2 \text{tr}[(X^T X)^{-1}] + O\left(\frac{\tilde{C}\|\mathcal{X}\|^2 \text{tr}[(X^T X)^{-2}]}{\epsilon^2 / \log(\frac{6}{\delta})}\right), \end{aligned}$$

with the same constant \tilde{C} in Theorem 2 (iii).

The proof of Statement (1) is straightforward. Note that we release the eigenvalue $\lambda_{\min}(X^T X)$, $X\mathbf{y}$ and $X^T X$ differentially privately each with parameter $(\epsilon/3, \delta/3)$. For the first two, we use Gaussian mechanism and for $X^T X$, we use the Analyze-Gauss algorithm (Dwork et al., 2014b) with a symmetric Gaussian random matrix. The result then follows from the composition theorem of differential privacy. The proof of the second and third statements is provided in Appendix C. The main technical challenge is to prove the concentration on the spectrum and the Johnson-Lindenstrauss-like distance preserving properties for symmetric Gaussian random matrices (Lemma 6). We note that while SSP is an old algorithm the analysis of its theoretical properties is new to this paper.

Remarks. Both ADAOPS and ADASSP match the smaller of the two lower bounds (5) and (6) for each problem instance. They are slightly different in that ADAOPS preserves the shape of the intrinsic geometry while ADASSP’s bounds are slightly stronger as they do not explicitly depend on the smallest eigenvalue.

5 EXPERIMENTS

In this section, we conduct synthetic and real data experiments to benchmark the performance of ADAOPS and ADASSP relative to existing algorithms we discussed in Section 3. NOISYSGD and Sub-Agg are excluded because they are dominated by OBJPERT and an (ϵ, δ) -DP version of OPS (see Appendix F for details)⁶.

Prediction accuracy in UCI data sets experiments.

The first set of experiments is on training linear regression on a number of UCI regression data sets. Standard z -scoring are performed and all data points are normalized to having an Euclidean norm of 1 as a preprocessing step. The results on four of the data sets are presented in Figure 2. As we can see, SSP is unstable for small data. OBJPERT suffers from a pre-defined bound $\|\Theta\|$ and

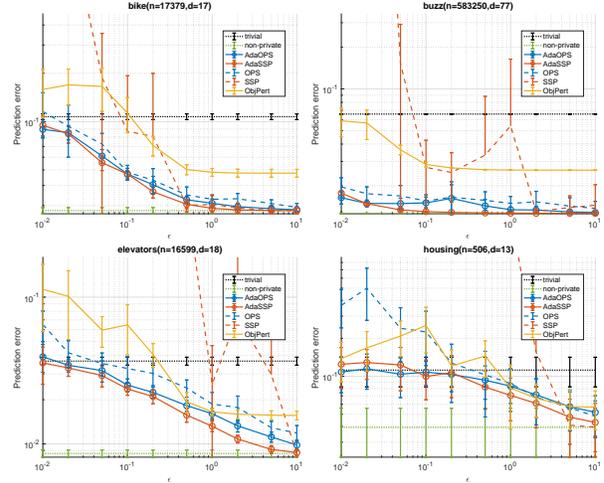


Figure 2: Example of results of differentially private linear regression algorithms on UCI data sets for a sequence of ϵ . Reported on the y-axis is the cross-validation prediction error in MSE and their confidence intervals.

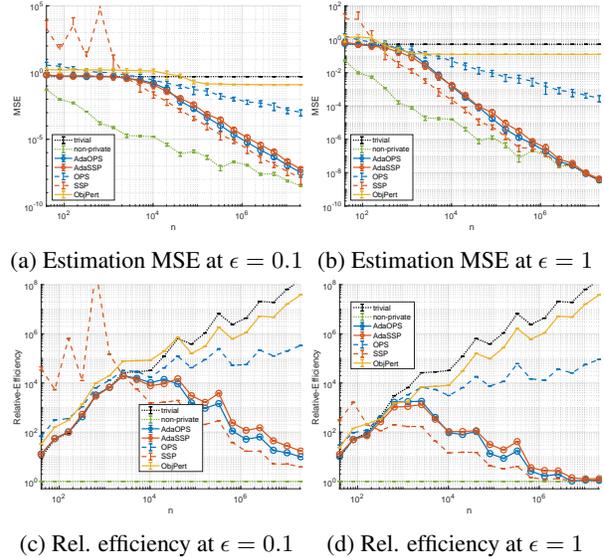


Figure 3: Example of differentially private linear regression under linear Gaussian model with an increasing data size n . We simulate the data from $d = 10$, θ_0 drawn from a uniform distribution defined on $[0, 1]^d$. We generate $X \in \mathbb{R}^{n \times d}$ as a Gaussian random matrix and then generate $y \sim \mathcal{N}(X\theta_0, I_d)$. We used $\epsilon = 1$ and $\epsilon = 0.1$, both with $\delta = 1/n^2$. The results clearly illustrate the asymptotic efficiency of the proposed approaches.

does not converge to nonprivate solution even with a large ϵ . OPS performs well but still does not take advantage of the strong convexity that is intrinsic to the data set. ADAOPS and ADASSP on the other hand are able to nicely interpolate between the trivial solution and the non-private baseline and performed as well as or better than baselines for all ϵ . More detailed quantitative results on all the 36 UCI data sets are presented in Table 3.

⁶The code to reproduce all experimental results are available at https://github.com/yuxiangw/optimal_dp_linear_regression.

Table 3: Summary of UCI data experiments at $\epsilon = 0.1$, $\delta = \min\{1e-6, 1/n^2\}$. The boldface denotes the DP algorithm where the standard deviation is smaller than the error (a positive quantity), and the 95% confidence interval covers the observed best performance among benchmarked DP algorithms.

	Trivial	non-private	OBJPERT	OPS	SSP	ADAOPS	ADASSP
3droad	0.0275±0.00014	0.0265±0.00012	0.0267±0.00013	0.027±0.00026	0.0265±0.00019	0.0265±0.00019	0.0265±0.00019
airfoil	0.103±0.0069	0.0533±0.0074	0.356±0.064	0.138±0.086	0.232±0.28	0.0914±0.015	0.0878±0.014
autopmg	0.113±0.011	0.0221±0.0032	0.143±0.096	0.242±0.11	5.44±6.1	0.098±0.03	0.115±0.047
autos	0.13±0.042	0.0274±0.011	0.17±0.13	0.308±0.13	1.7e+03±2.5e+03	0.136±0.066	0.132±0.064
bike	0.107±0.0028	0.0279±0.00078	0.113±0.018	0.0484±0.005	0.0869±0.067	0.0471±0.004	0.0471±0.0026
breastcancer	0.194±0.027	0.139±0.025	0.212±0.078	0.269±0.13	9.54e+03±1.9e+04	0.204±0.037	0.196±0.051
buzz	0.0658±0.00015	0.0127±4.6e-05	0.0285±0.00071	0.0156±0.001	0.0272±0.0097	0.0151±0.00095	0.013±9.7e-05
challenger	0.141±0.084	0.138±0.088	0.323±0.28	0.338±0.13	3.07±3.9	0.159±0.13	0.146±0.093
concrete	0.127±0.0043	0.0445±0.0033	0.237±0.076	0.181±0.042	1.94±1.8	0.12±0.011	0.119±0.016
concreteslump	0.149±0.039	0.0245±0.0071	0.349±0.094	0.549±0.24	3.14±2.5	0.151±0.064	0.165±0.065
elevators	0.0367±0.0014	0.00861±0.00031	0.0647±0.015	0.0327±0.0042	0.645±0.98	0.0252±0.0026	0.0237±0.0022
energy	0.235±0.012	0.0232±0.0023	0.332±0.09	0.161±0.083	1.7e+03±3.4e+03	0.167±0.034	0.15±0.032
fertility	0.0977±0.024	0.0863±0.024	0.203±0.04	0.639±0.16	439±8.6e+02	0.108±0.048	0.115±0.032
forest	0.0564±0.0081	0.0571±0.0086	0.12±0.022	0.177±0.036	41.9±77	0.0622±0.017	0.0675±0.013
gas	0.112±0.0062	0.0214±0.0028	0.109±0.015	0.0546±0.012	0.923±0.63	0.0801±0.0078	0.0875±0.0073
houseelectric	0.122±0.00017	0.0136±1.4e-05	0.0409±0.00027	0.0144±0.00017	0.0136±2.2e-05	0.0136±2.2e-05	0.0136±2.2e-05
housing	0.112±0.019	0.0394±0.01	0.253±0.063	0.225±0.065	2.24±2.3	0.108±0.023	0.0997±0.035
keggdirected	0.117±0.00095	0.0188±0.0011	0.0637±0.0042	0.0266±0.0019	0.23±0.33	0.0227±0.0015	0.0212±0.0011
keggundirected	0.0694±0.00074	0.00475±8.9e-05	0.0365±0.0028	0.0166±0.0033	0.353±0.4	0.0107±0.0012	0.00912±0.00046
kin40k	0.0634±0.0012	0.0632±0.0013	0.0871±0.0092	0.0717±0.0026	0.0633±0.002	0.0639±0.0021	0.064±0.0021
machine	0.121±0.013	0.0395±0.0051	0.282±0.14	0.347±0.14	2.27e+03±4.5e+03	0.105±0.025	0.141±0.068
parkinsons	0.17±0.0026	0.128±0.0024	0.211±0.014	0.157±0.011	132±2.6e+02	0.159±0.0065	0.156±0.0064
pendulum	0.0226±0.0061	0.0181±0.0049	0.118±0.027	0.122±0.041	24.8±45	0.0276±0.011	0.0346±0.0069
pol	0.345±0.0028	0.135±0.0023	0.302±0.032	0.196±0.02	281±5.3e+02	0.214±0.0056	0.214±0.0061
protein	0.167±0.0011	0.119±0.0014	0.158±0.01	0.137±0.0044	0.149±0.06	0.129±0.0015	0.125±0.0026
pumadyn32nm	0.0935±0.0039	0.0941±0.0039	0.124±0.0046	0.111±0.005	8.92e+03±1.8e+04	0.0968±0.0065	0.0966±0.0063
servo	0.184±0.039	0.0752±0.022	0.366±0.077	0.574±0.26	2.03±1.5	0.195±0.065	0.198±0.081
skillcraft	0.0439±0.0021	0.0203±0.0017	0.0817±0.013	0.0519±0.0099	4.72±4.3	0.037±0.008	0.039±0.0056
slice	0.196±0.0021	0.0283±0.00051	0.174±0.0053	0.0924±0.0035	11.2±9.4	0.0992±0.0021	0.132±0.0015
sml	0.211±0.0089	0.0143±0.00066	0.23±0.03	0.0955±0.029	59.9±80	0.134±0.0075	0.147±0.013
solar	0.0118±0.0042	0.0106±0.0038	0.0994±0.023	0.0667±0.017	5.95±9.6	0.0165±0.0062	0.0204±0.0073
song	0.0917±0.0003	0.0636±0.00033	0.0838±0.0014	0.072±0.00035	0.0644±0.0005	0.0685±0.00045	0.0697±0.00029
stock	0.0583±0.0095	0.013±0.0023	0.122±0.026	0.157±0.055	46.8±66	0.0582±0.023	0.0651±0.024
tamielectric	0.334±0.002	0.334±0.0021	0.341±0.0021	0.343±0.0065	0.335±0.0033	0.337±0.0047	0.335±0.0033
wine	0.0566±0.0028	0.0202±0.00099	0.153±0.028	0.0911±0.016	11.7±17	0.058±0.011	0.0599±0.01
yacht	0.105±0.017	0.0176±0.0055	0.273±0.076	0.371±0.14	4.92±6.8	0.0967±0.035	0.109±0.03

Parameter estimation under linear Gaussian model.

To illustrate the performance of the algorithms under standard statistical assumptions, we also benchmarked the algorithms on synthetic data generated by a linear Gaussian model. The results, shown in Figure 3 illustrates that as n gets large, ADAOPS and ADASSP with $\epsilon = 0.1$ and $\epsilon = 1$ converge to the maximum likelihood estimator at a rate faster than the optimal statistical rate that MLE estimates θ^* , therefore at least for large n , differential privacy comes for free. Note that there is a gap in SSP and ADASSP for large n , this can be thought of as a cost of adaptivity as ADASSP needs to spend some portion of its privacy budget to release λ_{\min} , which SSP does not, this can be fixed by using more careful splitting of the privacy budget.

6 CONCLUSION

In this paper, we presented a detailed case-study of the problem of differentially private linear regression. We clarified the relationships between various quantities of the problems as they appear in the private and non-private

information-theoretic lower bounds. We also surveyed the existing algorithms and highlighted that the main drawback using these algorithms relative to their non-private counterpart is that they cannot adapt to data-dependent quantities. This is particularly true for linear regression where the ordinary least square algorithm is able to work optimally for a large class of different settings.

We proposed ADAOPS and ADASSP to address the issue and showed that they both work in unbounded domain. Moreover, they smoothly interpolate the two regimes studied in Bassily et al. (2014) and behave nearly optimally for every instance. We tested the two algorithms on 36 real-life data sets from the UCI machine learning repository and we see significant improvement over popular algorithms for almost all configurations of ϵ .

Acknowledgements

The author thanks the anonymous reviewers for helpful feedbacks and Zichao Yang for sharing the 36 UCI regression data sets as was used in (Yang et al., 2015).

References

- Agresti, A., & Finlay, B. (1997). Statistical methods for the social sciences.
- Armitage, P., Berry, G., & Matthews, J. N. S. (2008). *Statistical methods in medical research*. John Wiley & Sons.
- Bassily, R., Smith, A., & Thakurta, A. (2014). Private empirical risk minimization: Efficient algorithms and tight error bounds. In *Foundations of Computer Science (FOCS-14)*, (pp. 464–473). IEEE.
- Birgé, L., & Massart, P. (2001). Gaussian model selection. *Journal of the European Mathematical Society*, 3(3), 203–268.
- Chaudhuri, K., Monteleoni, C., & Sarwate, A. D. (2011). Differentially private empirical risk minimization. *The Journal of Machine Learning Research*, 12, 1069–1109.
- Dimitrakakis, C., Nelson, B., Mitrokotsa, A., & Rubinstein, B. I. (2014). Robust and private Bayesian inference. In *Algorithmic Learning Theory*, (pp. 291–305). Springer.
- Donoho, D. L. (1995). De-noising by soft-thresholding. *IEEE transactions on information theory*, 41(3), 613–627.
- Draper, N. R., & Smith, H. (2014). *Applied regression analysis*, vol. 326. John Wiley & Sons.
- Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., & Naor, M. (2006a). Our data, ourselves: Privacy via distributed noise generation. In *International Conference on the Theory and Applications of Cryptographic Techniques*, (pp. 486–503). Springer.
- Dwork, C., & Lei, J. (2009). Differential privacy and robust statistics. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, (pp. 371–380). ACM.
- Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006b). Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography*, (pp. 265–284). Springer.
- Dwork, C., Roth, A., et al. (2014a). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4), 211–407.
- Dwork, C., & Smith, A. (2010). Differential privacy for statistics: What we know and what we want to learn. *Journal of Privacy and Confidentiality*, 1(2), 2.
- Dwork, C., Talwar, K., Thakurta, A., & Zhang, L. (2014b). Analyze gauss: optimal bounds for privacy-preserving principal component analysis. In *ACM symposium on Theory of computing (STOC-14)*, (pp. 11–20). ACM.
- Foulds, J., Geumlek, J., Welling, M., & Chaudhuri, K. (2016). On the theory and practice of privacy-preserving Bayesian data analysis. In *Conference on Uncertainty in Artificial Intelligence (UAI-16)*, (pp. 192–201). AUAI Press.
- Friedman, J., Hastie, T., & Tibshirani, R. (2001). *The elements of statistical learning*, vol. 1. Springer series in statistics Springer, Berlin.
- Galton, F. (1886). Regression towards mediocrity in hereditary stature. *The Journal of the Anthropological Institute of Great Britain and Ireland*, 15, 246–263.
- Greene, W. H. (2003). *Econometric analysis*. Pearson Education India.
- Kifer, D., Smith, A., & Thakurta, A. (2012). Private convex empirical risk minimization and high-dimensional regression. *Journal of Machine Learning Research*, 1, 41.
- Koren, T., & Levy, K. (2015). Fast rates for exp-concave empirical risk minimization. In *Advances in Neural Information Processing Systems*, (pp. 1477–1485).
- Laurent, B., & Massart, P. (2000). Adaptive estimation of a quadratic functional by model selection. *Annals of Statistics*, (pp. 1302–1338).
- Lei, J., Charest, A.-S., Slavkovic, A., Smith, A., & Fienberg, S. (2017). Differentially private model selection with penalized and constrained likelihood. *Journal of the Royal Statistical Society*.
- Minami, K., Arai, H., Sato, I., & Nakagawa, H. (2016). Differential privacy without sensitivity. In *Advances in Neural Information Processing Systems*, (pp. 956–964).
- Mir, D. J. (2013). *Differential privacy: an exploration of the privacy-utility landscape*. Ph.D. thesis, Rutgers University.
- Shamir, O. (2015). The sample complexity of learning linear predictors with the squared loss. *Journal of Machine Learning Research*, 16, 3475–3486.
- Sheffet, O. (2017). Differentially private ordinary least squares. In *International Conference on Machine Learning (ICML-17)*, (pp. 3105–3114).
- Smith, A. (2008). Efficient, differentially private point estimators. *arXiv preprint arXiv:0809.4794*.
- Stewart, G. W. (1998). Perturbation theory for the singular value decomposition. Tech. rep.
- Talwar, K., Thakurta, A., & Zhang, L. (2014). Private empirical risk minimization beyond the worst case: The effect of the constraint set geometry. *arXiv preprint arXiv:1411.5417*.
- Talwar, K., Thakurta, A. G., & Zhang, L. (2015). Nearly optimal private lasso. In *Advances in Neural Information Processing Systems*, (pp. 3025–3033).

- Vu, D., & Slavkovic, A. (2009). Differential privacy for clinical trial data: Preliminary evaluations. In *Data Mining Workshops, 2009. ICDMW'09. IEEE International Conference on*, (pp. 138–143). IEEE.
- Wang, Y.-X. (2017). Per-instance differential privacy and the adaptivity of posterior sampling in linear and ridge regression. *arXiv preprint arXiv:1707.07708*.
- Wang, Y.-X., Fienberg, S., & Smola, A. (2015). Privacy for free: Posterior sampling and stochastic gradient monte carlo. In *International Conference on Machine Learning (ICML-15)*, (pp. 2493–2502).
- Wasserman, L. (2013). *All of statistics: a concise course in statistical inference*. Springer Science & Business Media.
- Yang, Z., Wilson, A., Smola, A., & Song, L. (2015). A la carte–learning fast kernels. In *Artificial Intelligence and Statistics (AISTATS-15)*, (pp. 1098–1106).

A Results on the 36 real regression data sets in UCI repository

The detailed results on the 36 UCI data sets are presented in Table 3 for $\epsilon = 0.1, \delta = \min\{1e-6, 1/n^2\}$ and Table 4 for $\epsilon = 1, \delta = \min\{1e-6, 1/n^2\}$. The boldface denotes the DP algorithm where the standard deviation is smaller than the error (a positive quantity), and the 95% confidence interval covers the observed best performance among benchmarked DP algorithms.

Table 4: Summary of UCI data experiments at $\epsilon = 1$

	Trivial	non-private	OBJPERT	OPS	SSP	ADAOPS	ADASSP
3droad	0.0275±0.00014	0.0265±0.00012	0.0267±0.00013	0.0266±0.00012	0.0265±0.00019	0.0265±0.00019	0.0265±0.00019
airfoil	0.103±0.0069	0.0533±0.0074	0.0681±0.0074	0.0674±0.011	0.0535±0.013	0.0686±0.006	0.0585±0.012
autompng	0.113±0.011	0.0221±0.0032	0.0651±0.0072	0.0783±0.027	0.169±0.1	0.0522±0.0074	0.044±0.016
autos	0.13±0.042	0.0274±0.011	0.0868±0.044	0.0761±0.038	2.07±1.6	0.108±0.076	0.0971±0.053
bike	0.107±0.0028	0.0279±0.00078	0.0484±0.0017	0.0328±0.0011	0.0305±0.0045	0.031±0.0012	0.0288±0.0015
breastcancer	0.194±0.027	0.139±0.025	0.181±0.047	0.198±0.083	25.1±37	0.186±0.036	0.184±0.038
buzz	0.0658±0.00015	0.0127±4.6e-05	0.026±8e-05	0.015±0.0011	0.0541±0.069	0.0135±0.00038	0.0127±7.1e-05
challenger	0.141±0.084	0.138±0.088	0.181±0.13	0.529±0.35	5.27±8.1	0.142±0.13	0.145±0.14
concrete	0.127±0.0043	0.0445±0.0033	0.0759±0.0077	0.084±0.013	0.0569±0.03	0.0811±0.0044	0.0658±0.0051
concretelump	0.149±0.039	0.0245±0.0071	0.197±0.18	0.177±0.076	0.27±0.11	0.143±0.053	0.138±0.027
elevators	0.0367±0.0014	0.00861±0.00031	0.0165±0.00057	0.0187±0.0024	0.0255±0.021	0.0161±0.00091	0.0132±0.0011
energy	0.235±0.012	0.0232±0.0023	0.086±0.0061	0.0596±0.025	0.0983±0.065	0.0675±0.0084	0.051±0.0094
fertility	0.0977±0.024	0.0863±0.024	0.182±0.058	0.185±0.055	2.81±3	0.102±0.043	0.112±0.055
forest	0.0564±0.0081	0.0571±0.0086	0.0774±0.0092	0.0802±0.0099	0.13±0.041	0.0593±0.012	0.0585±0.0094
gas	0.112±0.0062	0.0214±0.0028	0.0593±0.0044	0.0432±0.0033	5.64±9	0.0471±0.0068	0.047±0.0063
houseelectric	0.122±0.00017	0.0136±1.4e-05	0.0406±6.3e-05	0.0138±7e-05	0.0136±2.2e-05	0.0136±2.2e-05	0.0136±2.2e-05
housing	0.112±0.019	0.0394±0.01	0.0805±0.042	0.0877±0.017	1.89±2.4	0.0835±0.031	0.0705±0.026
keggdirected	0.117±0.00095	0.0188±0.0011	0.0435±0.00054	0.0234±0.0022	0.0289±0.019	0.0215±0.0018	0.0192±0.00064
keggundirected	0.0694±0.00074	0.00475±8.9e-05	0.0213±0.00023	0.00942±0.0016	0.0195±0.023	0.00633±0.00027	0.00552±0.00014
kin40k	0.0634±0.0012	0.0632±0.0013	0.0633±0.002	0.065±0.0012	0.0632±0.002	0.0632±0.002	0.0633±0.002
machine	0.121±0.013	0.0395±0.0051	0.104±0.016	0.0825±0.027	0.77±1.3	0.0809±0.013	0.0671±0.016
parkinsons	0.17±0.0026	0.128±0.0024	0.14±0.0019	0.142±0.004	4.21±8.1	0.134±0.0026	0.133±0.0036
pendulum	0.0226±0.0061	0.0181±0.0049	0.0426±0.01	0.0473±0.012	0.0233±0.0066	0.0247±0.011	0.0233±0.0089
pol	0.345±0.0028	0.135±0.0023	0.19±0.0026	0.145±0.0028	0.338±0.32	0.144±0.0031	0.14±0.0033
protein	0.167±0.0011	0.119±0.0014	0.131±0.0012	0.128±0.0047	0.119±0.0022	0.124±0.0036	0.12±0.0021
pumadyn32nm	0.0935±0.0039	0.0941±0.0039	0.0948±0.0061	0.101±0.0038	0.0944±0.0065	0.0957±0.0065	0.0952±0.0066
servo	0.184±0.039	0.0752±0.022	0.152±0.077	0.209±0.079	0.126±0.072	0.149±0.051	0.124±0.06
skillcraft	0.0439±0.0021	0.0203±0.0017	0.0298±0.0018	0.0325±0.0024	0.0303±0.012	0.0268±0.0033	0.0247±0.0029
slice	0.196±0.0021	0.0283±0.00051	0.0875±0.00082	0.0518±0.00099	100±1.8e+02	0.0483±0.0013	0.0556±0.00059
sml	0.211±0.0089	0.0143±0.00066	0.0751±0.0037	0.0391±0.0042	52.6±1e+02	0.0502±0.0034	0.0405±0.0029
solar	0.0118±0.0042	0.0106±0.0038	0.0174±0.0069	0.031±0.0084	0.0182±0.0099	0.0137±0.0076	0.014±0.0054
song	0.0917±0.0003	0.0636±0.00033	0.0706±0.00029	0.0657±0.00039	0.0636±0.00052	0.0641±0.00029	0.0637±0.00052
stock	0.0583±0.0095	0.013±0.0023	0.06±0.016	0.051±0.0088	0.53±0.41	0.0399±0.014	0.0364±0.0076
tamielelectric	0.334±0.002	0.334±0.0021	0.334±0.0032	0.338±0.0028	0.334±0.0033	0.335±0.0027	0.334±0.0032
wine	0.0566±0.0028	0.0202±0.00099	0.0327±0.0031	0.0423±0.0064	0.023±0.0016	0.039±0.0023	0.0348±0.0028
yacht	0.105±0.017	0.0176±0.0055	0.0588±0.024	0.0736±0.021	0.133±0.2	0.0676±0.0096	0.0469±0.018

B Alternative illustration of the private and nonprivate lower bounds

In Section 3 we discuss the relationships of lower bounds for statistical learning minimax rate of linear regression problems due to Shamir (2015) and the lower bounds on optimization error due to Bassily et al. (2014). In particular, we addressed the question of “when is differential privacy for free in statistical learning?”. In this section, we provide an alternative view of the same question which allows us to more easily quantify the “price of differential privacy” really is, even if it is not “for free”.

In particular, we plot Shamir’s lower bound (4) and the smaller of Bassily et. al.’s differential privacy lower bounds (5) and (6) for all configurations of d, n graphically in Figure 4. We also use multiple lines to illustrate the shifts in these lower bounds when parameters such as ϵ and α^* change. In all figures δ is assumed to be $o(1/n)$ and all logarithmic terms are ignored. The price of differential privacy is highlighted as a shaded area in the figures. Interestingly, in the first case when $\|\Theta\|$ is small, then substantial price only occurs in the non-standard region where $n < d$. Arguably this is OK because in that regime, people should use Ridge regression or Lasso anyways rather than OLS. In the case when $\|\Theta\|$ is large, the price is more substantial and it applies to all $n > d$ unless we can exploit the strong convexity in the data set. When we do, then the cost only occur for a interval in n and eventually differential privacy becomes completely free.

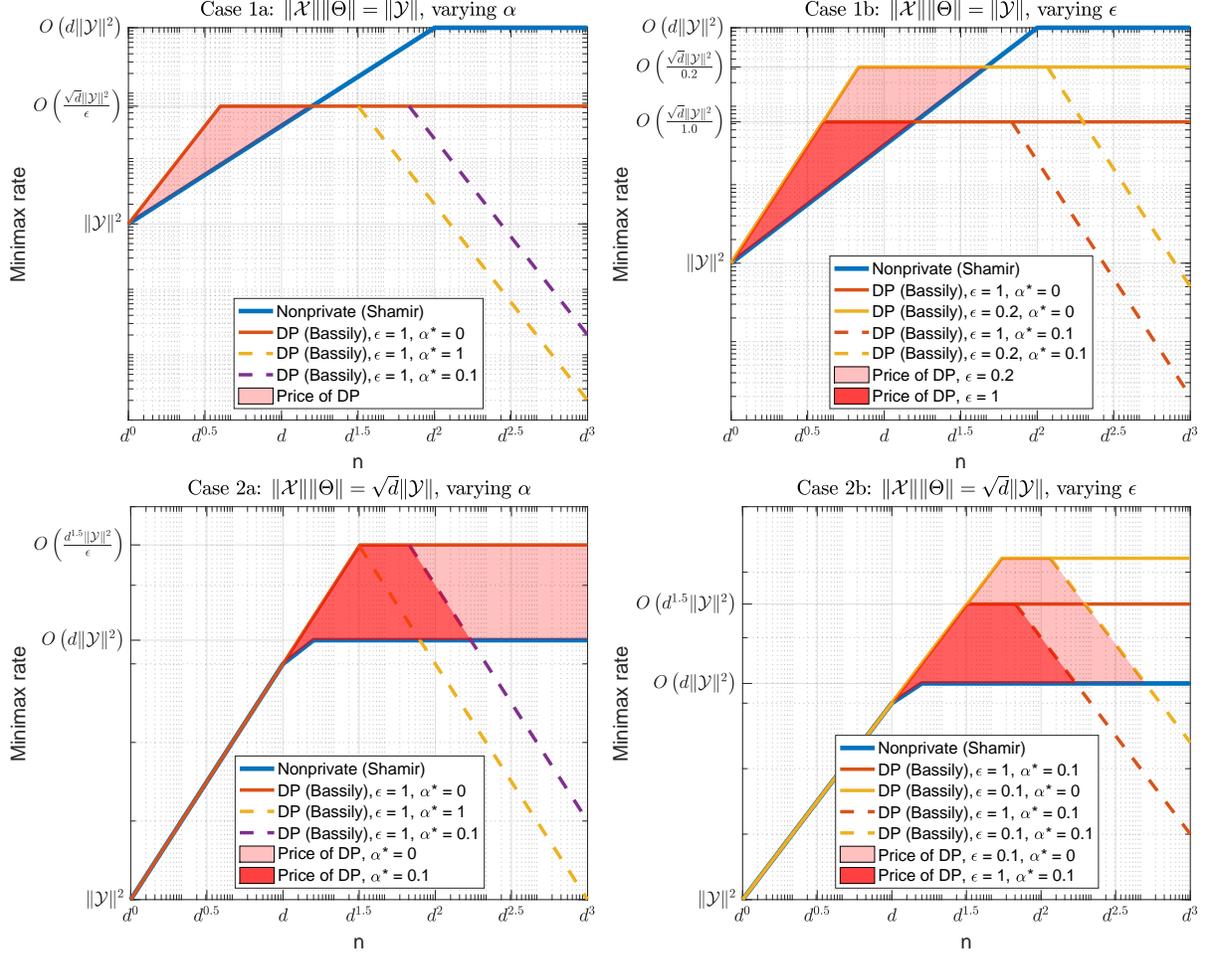


Figure 4: Illustration of the lower bounds for non-private and private linear regression.

C Proof of the results for SSP and ADASSP

In this section, we first derive the rate for the optimization and parameter estimation error of the sufficient statistics perturbation (SuffPert) approach as was shown in Table 1 and Table 2. This will build intuition towards ADASSP, which we will present the proof of it towards the end of the section.

C.1 Analysis of SSP for linear regression

Recall that SSP is the naive approach that uses Gaussian mechanism to release $X^T X$ and $X \mathbf{y}$ then estimate θ^* using the plug-in estimator.

Lemma 4. Let $\theta^* = (X^T X)^{-1} X \mathbf{y}$, and $\hat{\theta} = (X^T X + E_1)^{-1} (X \mathbf{y} + E_2)$ for any $E_1 \in \mathbb{R}^{d \times d}$, $E_2 \in \mathbb{R}^d$ such that $X^T X + E_1$ is invertible, then

$$\hat{\theta} - \theta^* = -(X^T X + E_1)^{-1} E_1 \theta^* + (X^T X + E_1)^{-1} E_2.$$

In SSP, E_1 is a symmetric Gaussian random matrix where each element in the upper triangular part of this matrix is iid $\mathcal{N}(0, \frac{4\|\mathcal{X}\|^4 \log(4/\delta)}{\epsilon^2})$, and E_2 is an iid Gaussian vector drawn from $\mathcal{N}(0, \frac{4\|\mathcal{X}\|^2 \|\mathcal{Y}\|^2 \log(4/\delta)}{\epsilon^2})$.

By Lemma 4, and Cauchy-Schwartz, we can write

$$\begin{aligned}\|\hat{\theta} - \theta^*\|^2 &\leq 2[\theta^*]^T E_1^T [(X^T X + E_1)^{-1}]^T (X^T X + E_1)^{-1} E_1 \theta^* \\ &\quad + 2E_2^T [(X^T X + E_1)^{-1}]^T (X^T X + E_1)^{-1} E_2.\end{aligned}$$

This equation highlights the key artifact of this method, as when $X^T X$ has a small eigenvalue, there is a non-trivial probability that $X^T X + E_1$ will be nearly singular and that could potentially blow up the variance.

We could however analyze the high probability error bound, which becomes meaningful when $\|E_1\| < \lambda_{\min}(X^T X) = \frac{\alpha n \|\mathcal{X}\|^2}{d}$ as then we can show that with high probability, $X^T X + E_1$ has a smallest singular value that is bounded away from zero. In particular if $\|E_1\| \leq \lambda_{\min}(X^T X)/2$ with high probability, then we can derive an error bound using Lemma 4:

$$\|\hat{\theta} - \theta^*\|^2 = O\left(\frac{d^3 \|\theta^*\|^2}{\alpha^2 n^2 \epsilon^2}\right)$$

under the simplifying assumption that $\|\mathcal{Y}\| = O(\|\mathcal{X}\| \|\theta^*\|)$.

The eigenvalue condition suggests that such reasonable error bound only starts to apply when

$$n = \tilde{\Omega}\left(\frac{d^{1.5} \sqrt{\log(4/\delta)}}{\alpha \epsilon}\right).$$

Now, using the following lemma, we can convert the optimization error into estimation in a different norm.

Lemma 5. *Let $\theta^* = (X^T X)^{-1} X \mathbf{y}$, for any θ ,*

$$\|\mathbf{y} - X\theta\|^2 - \|\mathbf{y} - X\theta^*\|^2 = (\theta - \theta^*)^T X^T X (\theta - \theta^*) = \|\theta - \theta^*\|_{X^T X}^2.$$

Proof. The result follows directly by the second order Taylor expansion of $\|\mathbf{y} - X\theta\|^2$ at θ^* and the fact that the gradient at θ^* is 0. \blacksquare

A direct calculation leads to the following bound

$$\begin{aligned}\|\hat{\theta} - \theta^*\|_{X^T X}^2 &\leq 2[\theta^*]^T E_1^T [(X^T X + E_1)^{-1}]^T (X^T X) (X^T X + E_1)^{-1} E_1 \theta^* \\ &\quad + 2E_2^T [(X^T X + E_1)^{-1}]^T (X^T X) (X^T X + E_1)^{-1} E_2\end{aligned}$$

The idea is that by random matrix theory, we get $\|E_1\| \leq \tilde{O}(\sqrt{d} \|\mathcal{X}\|^2 \sqrt{\log 12\delta}/\epsilon)$ with high probability. For large enough n , $X^T X$ has a smallest eigenvalue on that order, which allows us to prove:

$$0.5X^T X \prec X^T X + E_1 \prec 2X^T X.$$

with high probability. It follows that under this high probability event

$$\|\hat{\theta} - \theta^*\|_{X^T X}^2 \leq 8\|E_1 \theta^*\|_{(X^T X)^{-1}}^2 + 8\|E_2\|_{(X^T X)^{-1}}^2. \quad (9)$$

We first prove the following Johnson-Lindenstrauss type lemma for symmetric Gaussian random matrices and ellipsoid distance.

Lemma 6. *Let $\theta \in \mathbb{R}^d$ be a fixed and E be a symmetric random Gaussian matrix where the upper triangular region is iid Gaussian with $\mathcal{N}(0, w^2)$ With probability $1 - \rho$, and let A be a positive semi-definite matrix,*

$$\|E\theta\|_A^2 \leq w^2 \text{tr}(A) \|\theta\|^2 \log(2d^2/\rho)$$

Proof. Take the eigenvalue decomposition $A = U \Lambda U^T$, we can write

$$\|E\theta\|_A^2 = [\theta]^T E^T U \Lambda U^T E \theta = \sum_{i=1}^d \lambda_i \sum_{j=1}^d [U^T E]_{i,j}^2 [\theta]_i^2. \quad (10)$$

Note $[U^T E]_{i,j} = \sum_{k=1}^d U_{i,k} [E]_{j,k}$ where $[E]_{j,\cdot}$ is an independent Gaussian vector, despite that E itself is constrained to be a symmetric matrix. Using that U is orthogonal, we have that marginally for each $i, j \in [d]^2$,

$$[U^T E]_{i,j} \sim \mathcal{N}(0, w^2).$$

Using the Gaussian tail bound and a union bound over all $(i, j) \in [d]^2$, we get that

$$\mathbb{P}\left(\max_{(i,j) \in [d]^2} |[U^T E]_{i,j}| \geq \sqrt{w^2 \log(2d^2/\varrho)}\right) \leq \varrho.$$

Substitute this into (10), we have

$$\|E\theta\|_{(X^T X)^{-1}}^2 = O\left(w^2 \|\theta\|^2 \text{tr}[A] \log(2d^2/\varrho)\right).$$

■

Apply the above lemma with $A := (X^T X)^{-1}$, $E = E_1$ (hence $w^2 = \frac{\log(6/\delta) \|\mathcal{X}\|^4}{\epsilon^2/9}$) we get

$$\|E_1 \theta^*\|_{(X^T X)^{-1}}^2 = O\left(\frac{\|\theta^*\|^2 \|\mathcal{X}\|^4 \text{tr}[(X^T X)^{-1}] \log(6/\delta) \log(2d^2/\varrho)}{\epsilon^2/9}\right).$$

Similarly, note that $E_2 \sim U E_2$ for any unitary transformation, we can bound the tail of every eigendirection separately and that gives:

$$\|E_2\|_{(X^T X)^{-1}}^2 = O\left(\frac{\|\mathcal{X}\|^2 \|\mathcal{Y}\|^2 \text{tr}[(X^T X)^{-1}] \log(6/\delta) \log(d/\varrho)}{\epsilon^2/9}\right). \quad (11)$$

Substitute the above two inequalities into (9), and take union bound with the small probability event that $\|E_1\| \leq 0.5\lambda_{\min}(X^T X)$ we get that with high probability

$$\|\hat{\theta} - \theta^*\|_{X^T X}^2 \leq O\left(\frac{\|\mathcal{X}\|^2 (\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \text{tr}[(X^T X)^{-1}] \log(6/\delta) \log(2d^2/\rho)}{\epsilon^2/9}\right).$$

In other word, a naive SSP can perform arbitrarily poorly as λ_{\min} gets close to 0.

A natural idea to address this problem is to use regularization and do ridge regression instead. We now analyze the modified case for a fixed Ridge regression parameter λ .

C.2 Analysis of SSP for ridge regression

First note that SSP for ridge regression is nothing but the case when we replace E_1 with $\lambda I + E_1$. This view allows us to reuse the lemmas we derived above. In particular, Lemma 4 implies the following corollary.

Corollary 7. *Let $\hat{\theta}_\lambda = (X^T X + \lambda I + E_1)^{-1} (X \mathbf{y} + E_2)$ for $\lambda > 0$, then*

$$\hat{\theta}_\lambda - \theta^* = -(X^T X + \lambda I + E_1)^{-1} E_1 \theta^* - \lambda (X^T X + \lambda I + E_1)^{-1} \theta^* + (X^T X + \lambda I + E_1)^{-1} E_2.$$

For any psd matrix A

$$\begin{aligned} \|\hat{\theta}_\lambda - \theta^*\|_A^2 &\leq 3 \|(X^T X + \lambda I + E_1)^{-1} E_1 \theta^*\|_A^2 \\ &\quad + 3 \|(X^T X + \lambda I + E_1)^{-1}\|_A^2 \\ &\quad + 3\lambda^2 \|(X^T X + \lambda I + E_1)^{-1} \theta^*\|_A^2. \end{aligned}$$

Under the high probability event such that $\|E_1\| \leq (\lambda_{\min}(X^T X) + \lambda)/2$, we have $X^T X + \lambda I + E_1 \prec 0.5(X^T X + \lambda I)$ and it implies that

$$\|\hat{\theta}_\lambda - \theta^*\|^2 = O\left(\|E_1 \theta^*\|_{(X^T X + \lambda I)^{-2}}^2 + \|E_2\|_{(X^T X + \lambda I)^{-2}}^2 + \lambda^2 \|\theta^*\|_{(X^T X + \lambda I)^{-2}}^2\right).$$

Similarly by Lemma 5

$$\begin{aligned} F(\hat{\theta}_\lambda) - F(\theta^*) &= \frac{1}{2} \|\hat{\theta}_\lambda - \theta^*\|_{(X^T X)^{-1}}^2 \\ &= O \left(\|E_1 \theta^*\|_{(X^T X + \lambda I)^{-1}}^2 + \|E_2\|_{(X^T X + \lambda I)^{-1}}^2 + \lambda^2 \|\theta^*\|_{(X^T X + \lambda I)^{-1}}^2 \right). \end{aligned}$$

Apply the distance preserving results in Lemma 6 to the first term above with $A = (X^T X + \lambda I)^{-2}$ and $A = (X^T X + \lambda I)^{-1}$ respectively, we can write

$$\|\hat{\theta}_\lambda - \theta^*\|^2 = O \left(\frac{\|\mathcal{X}\|^2 (\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \log(6/\delta) \log(2d^2/\rho)}{\epsilon^2} \text{tr}[(X^T X + \lambda I)^{-2}] + \lambda^2 \|\theta^*\|_{(X^T X + \lambda I)^{-2}}^2 \right), \quad (12)$$

$$\begin{aligned} F(\hat{\theta}_\lambda) - F(\theta^*) &= O \left(\frac{\|\mathcal{X}\|^2 (\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \log(6/\delta) \log(2d^2/\rho)}{\epsilon^2} \text{tr}[(X^T X + \lambda I)^{-1}] + \lambda^2 \|\theta^*\|_{(X^T X + \lambda I)^{-1}}^2 \right) \\ &= O \left(\frac{d \|\mathcal{X}\|^2 (\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \log(6/\delta) \log(2d^2/\rho)}{(\lambda + \lambda_{\min}) \epsilon^2} + \lambda \|\theta^*\|^2 \right). \end{aligned} \quad (13)$$

Note that when $\lambda_{\min} = 0$, choosing

$$\lambda = \Theta \left(\sqrt{d \log(6/\delta) \log(2d^2/\rho)} \left(\frac{\|\mathcal{X}\| \|\mathcal{Y}\|}{\|\theta^*\|} + \|\mathcal{X}\|^2 \right) / \epsilon \right) \quad (14)$$

balances the two terms and results in a bound that is on the order of \sqrt{d}/ϵ which matches the lower bound for the Lipschitz private ERM (5). Similarly, when λ_{\min} is larger than the above quantity, the optimal choice of λ is 0 and we get a rate of $d/(\lambda_{\min} \epsilon^2)$ which matches the lower bound for the private strongly convex ERM (6).

It remains to check whether such choices are feasible, because recall that the entire analysis hinges upon the event that

$$\|E_1\| \leq (\lambda_{\min} + \lambda)/2. \quad (15)$$

Recall that $\|E_1\| \leq 2\sqrt{d \log(6/\delta) \log(d^2/\rho)} \|\mathcal{X}\|^2 / (\epsilon/3)$ with high probability, so the a choice of λ that satisfies (14) with appropriate constant automatically obeys (15).

C.3 Analysis of ADASSP. Proof of Theorem 3.

The proof of Statement (i) is a straightforward application of the composition theorem over standard releases of $X^T X$, $X^T \mathbf{y}$ and $\lambda_{\min}(X^T X)$.

The extension from SSP to ADASSP involves choosing λ adaptively. By our analysis above, the desired choice is (14) but it depends on unknown quantities of the data λ_{\min} and $\|\theta^*\|$.

Our choice of λ in Algorithm 2 is that

$$\lambda = \max \left\{ 0, \frac{\sqrt{d \log(6/\delta) \log(2d^2/\rho)} \|\mathcal{X}\|^2}{\epsilon/3} - \lambda_{\min}^* \right\}$$

where λ_{\min}^* is a differentially private high probability lower bound of λ_{\min} . Check that the choice obeys (15) so the error analysis above is valid. Substitute this choice of λ into (13) and (12), we get the results in Theorem 3(ii) and Theorem 3(iii).

Note that because we do not know $\|\theta^*\|$, we cannot set the $\frac{\|\mathcal{X}\| \|\mathcal{Y}\|}{\|\theta^*\|}$ as part of the oracle λ choice in (14). As a result, the final optimization error is proportional to the constant of $\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2$ instead of the optimal $\|\mathcal{Y}\| \|\mathcal{X}\| \|\theta^*\| + \|\mathcal{X}\|^2 \|\theta^*\|^2$. They are on the same order under our assumption that $\|\mathcal{Y}\| \asymp \|\mathcal{X}\| \|\theta^*\|$.

D Proofs related to ADAOPS

The proof uses the pDP technique that first analyzes OPS for fixed set of tuning parameters and then do pDP to DP conversion with differential privately chosen tuning parameters.

D.1 Utility of OPS with fixed (γ, λ)

Lemma 8 (Parameter estimation error). *Let X be fixed and θ_λ^* be the maximum a posteriori estimator (MLE if $\lambda = 0$), and $\tilde{\theta}$ be the output of OPS with parameter γ, λ , then:*

1. for all $0 < \varrho < 1$, with probability $1 - \varrho$

$$\|\tilde{\theta} - \theta_\lambda^*\|_{X^T X + \lambda I}^2 \leq \frac{d + 2\sqrt{d \log(1/\varrho)} + 2 \log(1/\varrho)}{\gamma} \leq \frac{5d \log(1/\varrho)}{\gamma}.$$

2. It holds that

$$\mathbb{E}[\tilde{\theta}|X, \mathbf{y}] = \theta_\lambda^* \text{ and } \text{Cov}[\tilde{\theta}|X, \mathbf{y}] = \gamma^{-1}(X^T X + \lambda I)^{-1}.$$

3. If we assume that $\mathbf{y} \sim \mathcal{N}(X\theta_0, \sigma^2 I)$ and $\lambda = 0$, then

$$\mathbb{E}[\tilde{\theta}|X] = \theta_0 \text{ and } \text{Cov}[\tilde{\theta}|X] = (\sigma^2 + \gamma^{-1})(X^T X)^{-1}.$$

Proof. Let $H := X^T X + \lambda I = Q\Lambda Q^T$, and let $Z \sim \mathcal{N}(0, \gamma^{-1}I_d)$

$$\|\tilde{\theta} - \theta_\lambda^*\|_H^2 = (\tilde{\theta} - \theta_\lambda^*)^T H (\tilde{\theta} - \theta_\lambda^*) = Z^T \Lambda^{-1/2} Q^T Q \Lambda Q^T Q \Lambda^{-1/2} Z = \|Z\|_2^2$$

Note that $\gamma\|Z\|_2^2$ has a χ^2 -distribution with degree of freedom d , by the standard right tail bound inequality of χ^2 R.V., we get the results as claimed. The second statement is trivial and it follows directly from the algorithm. For the third statement, note that the MLE θ^* is unbiased for linear regression, also, it has covariance matrix $\sigma^2(X^T X)^{-1}$. The second part of the randomness comes from sampling from the posterior distribution which has covariance matrix $\gamma^{-1}(X^T X)^{-1}$ by the algorithm. The results follows after noting that the we are adding independent noise. ■

Lemma 9 (Optimization error / regret bound). *Let θ^* be a local minimum of a convex quadratic function F and*

$$\tilde{\theta} \sim \mathcal{N}(\theta^*, \gamma^{-1}[\nabla^2 F(\theta^*)]^{-1}),$$

then for all $0 < \varrho < 1$, with probability $1 - \varrho$

$$F(\tilde{\theta}) - F(\theta^*) \leq \frac{d + 2\sqrt{d \log(1/\varrho)} + 2 \log(1/\varrho)}{2\gamma} \leq \frac{2.5d \log(1/\varrho)}{\gamma}.$$

Proof. Since F is quadratic, $\nabla^2 F \equiv H$ for some fixed matrix H (independent to location). By Taylor's theorem

$$F(\tilde{\theta}) - F(\theta^*) = \langle \nabla F(\theta^*), \tilde{\theta} - \theta^* \rangle + \frac{1}{2} \|\tilde{\theta} - \theta^*\|_H^2.$$

Substitute Lemma 8 into the above we get the result as claimed. ■

D.2 pDP analysis of OPS for fixed (γ, λ)

We now cite the per-instance differential privacy of OPS for a fixed set of parameters from (Wang, 2017).

Theorem 10 (Theorem 15 of Wang (2017)). *Consider the algorithm that samples from*

$$p(\theta|X, \mathbf{y}) \propto e^{-\frac{\gamma}{2}(\|\mathbf{y} - X\theta\|^2 + \lambda\|\theta\|^2)}.$$

Let $\hat{\theta}$ and $\hat{\theta}'$ be the ridge regression estimate with data set $X \times \mathbf{y}$ and $[X, x] \times [\mathbf{y}, y]$ and defined the out of sample leverage score $\mu := x^T (X^T X + \lambda I)^{-1} x = x^T H^{-1} x$ and in-sample leverage score $\mu' := x^T [(X')^T X' + \lambda I]^{-1} x = x^T (H')^{-1} x$. Then for every $\delta > 0$, privacy target (x, y) , the algorithm is (ϵ, δ) -pDP with

$$\epsilon(Z, z) \leq \frac{1}{2} \left| -\log(1 + \mu) + \frac{\gamma\mu}{(1 + \mu)} (y - x^T \hat{\theta})^2 \right| + \frac{\mu}{2} \log(2/\delta) + \sqrt{\gamma\mu \log(2/\delta)} |y - x^T \hat{\theta}| \quad (16)$$

$$= \frac{1}{2} \left| -\log(1 - \mu') - \frac{\gamma\mu'}{1 - \mu'} (y - x^T \hat{\theta}')^2 \right| + \frac{\mu'}{2} \log(2/\delta) + \sqrt{\gamma\mu' \log(2/\delta)} |y - x^T \hat{\theta}'|. \quad (17)$$

Remark 11. Let $L := \|\mathcal{X}\|(\|\mathcal{X}\|\|\theta_\lambda^*\| + \|\mathcal{Y}\|)$, The OPS algorithm for ridge regression with parameter (λ, γ) obeys (ϵ, δ) -pDP for each data set (X, y) and all target (x, y) with

$$\epsilon = \sqrt{\frac{\gamma L^2 \log(2/\delta)}{\lambda + \lambda_{\min}}} + \frac{\gamma L^2}{2(\lambda + \lambda_{\min} + \|\mathcal{X}\|^2)} + \frac{(1 + \log(2/\delta))\|\mathcal{X}\|^2}{2(\lambda + \lambda_{\min})}.$$

D.3 pDP to DP conversion

The hallmark of DP algorithm design is that one needs to calibrate the amount of noise so that no matter what data set is sent into the algorithm, the algorithm meets a prescribed privacy budget (ϵ, δ) . The pDP guarantees of OPS says that for a fixed randomized algorithm, if the data set is nice, then the privacy guarantee is strong, while if the data set is poorly-conditioned, then the privacy loss is big. What is more, the pDP analysis illustrates that the key ingredients of that appears in the pDP bound is the smallest eigenvalue of $X^T X$ and the local Lipschitz constant L (given as a function of $\|\mathcal{X}\|$ and $\|\mathcal{Y}\|$ and the magnitude of the solution $\|\theta_\lambda^*\|$).

The approach used in Wang (2017) is to differentially privately release λ_{\min} and an adaptive amount of regularization λ is added so that a pre-specified strong convexity parameter α^* is met with high probability. Then a crude upper bound of $\|\theta_\lambda^*\|$ is used based on λ^* or λ_{\min} (if larger than λ^*) to calibrate γ . The outcome is an asymptotically efficient differentially private estimator of linear regression coefficients when the data set is well-conditioned. However, there are two issues. First, it is unclear how λ^* is chosen; second, the crude upper bound of $\|\theta_\lambda^*\|$ leads to unnecessary dimension dependence in the bound.

In this section, we further extend the idea by proposing a novel way of releasing the $\|\theta_\lambda^*\|$ differentially privately by injecting a multiplicative noise, which allows us to design a DP algorithm that adapts to small local Lipschitz constant near the optimal solution and also a principled approach of choosing the regularization parameter λ , such that (1) the algorithm is (ϵ, δ) -DP for all input data, (2) it is statistically efficient with an improved dimension-dependence when the data follows a linear Gaussian model (3) the optimization error is optimal up to a logarithmic term for each (unknown) strong convexity parameter and local Lipschitz constant separately.

The algorithm basically looks like the following:

1. Differentially privately release λ_{\min} using $(\epsilon/4, \delta/3)$, and choose regularization parameter λ accordingly.
2. Condition on a high probability event of λ_{\min} , and choose λ .
3. Differentially privately release $\|\theta_\lambda^*\|$ using $(\epsilon/4, \delta/3)$, where $\theta_\lambda^* = (X^T X + \lambda I)^{-1} X^T \mathbf{y}$.
4. Condition on a high probability event of both λ_{\min} and $\|\theta_\lambda^*\|$, calibrate the noise to meet the $(\epsilon/2, \delta/3)$ requirement.

We start by showing how we can release λ_{\min} and $\|\theta_\lambda^*\|$. By Weyl's lemma, λ_{\min} has a global sensitivity of $\|\mathcal{X}\|^2$. It turns out that while $\|\theta_\lambda^*\|$ does not have a well-behaved global or local sensitivity, a logarithmic transformation $\log(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$ has a very stable local sensitivity that is parameterized only by the smallest eigenvalue, which we can easily construct a differentially private upper bound.

Lemma 12. Let θ_λ^* be the ridge regression estimate with parameter λ and the smallest eigenvalue of $X^T X$ be λ_{\min} , then the function $\log(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$ has a local sensitivity of $\log(1 + \frac{\|\mathcal{X}\|^2}{\lambda_{\min} + \lambda})$.

Proof. Denote $\|\mathcal{Y}\| =: \alpha$ and $\|\mathcal{X}\| =: \beta$. Let the data point being added to the data set be (x, y) . For a fixed λ , denote $\hat{\theta}$ and $\hat{\theta}'$ as the ridge regression estimate with parameter λ on data set X, \mathbf{y} and $[X, x], [\mathbf{y}, y]$ respectively.

By Lemma 17, we have

$$\left| \|\hat{\theta}\| - \|\hat{\theta}'\| \right| \leq \|\hat{\theta} - \hat{\theta}'\| = |y - x^T \hat{\theta}| \sqrt{x^T ([X, x]^T [X, x] + \lambda I)^{-2} x} \leq \frac{\beta}{\lambda_{\min} + \lambda} (\alpha + \beta \min\{\|\hat{\theta}'\|, \|\hat{\theta}\|\}).$$

Multiplying β on both sides and use triangular inequality, we have

$$\begin{cases} (\alpha + \beta\|\hat{\theta}\|) - (\alpha + \beta\|\hat{\theta}'\|) \leq \frac{\beta^2}{\lambda_{\min} + \lambda} (\alpha + \beta\|\hat{\theta}'\|) \\ ((\alpha + \beta\|\hat{\theta}'\|) - (\alpha + \beta\|\hat{\theta}\|)) \leq \frac{\beta^2}{\lambda_{\min} + \lambda} (\alpha + \beta\|\hat{\theta}\|) \end{cases}$$

Rearrange the terms and take log on both sides, we get

$$\left| \log \frac{\alpha + \beta \|\hat{\theta}\|}{\alpha + \beta \|\hat{\theta}'\|} \right| \leq \log\left(1 + \frac{\beta^2}{\lambda_{\min} + \lambda}\right).$$

■

D.4 Automatically choosing λ

We will do this by minimizing an upper bound of the empirical risk. Note that this is a somewhat circular problem because the empirical risk is a function of $\|\theta_\lambda^*\|$, but in order to release it differentially privately, we need to choose λ to begin with. The main idea is to express the DP upper bound of the Lipschitz constant analytically as a function of λ and also take the additional noise from differential privacy into account.

Let a differentially private lower bound of λ_{\min} be $\tilde{\lambda}_{\min}$, and \bar{L} be a high-probability upper bound of the local Lipschitz constant $L = \|\mathcal{X}\|(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$. Consider the fixed OPS algorithm with the parameter choice of $\gamma^{-1} = \frac{\log(2/\delta)L^2}{(\tilde{\lambda}_{\min} + \lambda)\epsilon^2}$. Define

$$C_1(\epsilon, \delta, \varrho, d) := \frac{[d/2 + \sqrt{d \log(1/\varrho)} + \log(1/\varrho)] \log(2/\delta)}{\epsilon^2} \quad (18)$$

$$C_2(\epsilon, \delta) := \frac{\log(2/\delta)}{\epsilon} \quad (19)$$

We know from Lemma 12, that we can construct a high probability upper bound L from a differentially private release of $\log(\|\mathcal{Y}\| + \|\theta_\lambda^*\|\|\mathcal{X}\|)$ satisfying that with probability $1 - \delta$

$$\|\mathcal{X}\|(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|) := L \leq \bar{L} \leq L(1 + \|\mathcal{X}\|^2/(\tilde{\lambda}_{\min} + \lambda))^{C_2}$$

Recall that θ^* is the least square solution $\operatorname{argmin}_\theta F(\theta)$. The optimization error obeys that

$$\begin{aligned} F(\tilde{\theta}) - F(\theta^*) &= F(\tilde{\theta}) + \lambda\|\tilde{\theta}\|^2 - F(\theta_\lambda^*) - \lambda\|\theta_\lambda^*\|^2 \\ &\quad + F(\theta_\lambda^*) + \lambda\|\theta_\lambda^*\|^2 - F(\theta^*) - \lambda\|\theta^*\|^2 + \lambda\|\theta^*\|^2 \\ &\leq \frac{[d/2 + \sqrt{d \log(1/\varrho)} + \log(1/\varrho)]}{\gamma} + 0 + \lambda\|\theta^*\|^2 \\ &= \frac{C_1(\epsilon, \delta, \varrho, d)\|\mathcal{X}\|^2(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)^2(1 + \frac{\|\mathcal{X}\|^2}{\lambda + \tilde{\lambda}_{\min}})^{2C_2(\epsilon, \delta)}}{\lambda + \tilde{\lambda}_{\min}} + \lambda\|\theta^*\|^2 \\ &\leq \frac{C_1(\epsilon, \delta, \varrho, d)\|\mathcal{X}\|^4(\|\mathcal{Y}\|/\|\mathcal{X}\| + \|\theta^*\|)^2(1 + \frac{\|\mathcal{X}\|^2}{\lambda + \tilde{\lambda}_{\min}})^{2C_2(\epsilon, \delta)}}{\lambda + \tilde{\lambda}_{\min}} + \lambda(\|\mathcal{Y}\|/\|\mathcal{X}\| + \|\theta^*\|)^2 \end{aligned}$$

The first inequality uses Lemma 5, Lemma 8 and used the optimality of θ_λ^* for the regularized objective. In the last line, we used the monotonicity of ridge regression which says that for all $\lambda > 0$, we have $\|\theta_\lambda^*\| \leq \|\theta^*\|$. We also $\|\theta^*\|$ into $\|\mathcal{Y}\|/\|\mathcal{X}\| + \|\theta^*\|$.

This relaxation allows us to choose λ that is independent to $\|\theta^*\|$, by minimizing the second part of the upper bound

$$F(\tilde{\theta}) - F(\theta^*) \leq (\|\mathcal{Y}\|/\|\mathcal{X}\| + \|\theta^*\|)^2 \left[\frac{C_1(\epsilon, \delta, \varrho, d)\|\mathcal{X}\|^4(1 + \frac{\|\mathcal{X}\|^2}{\lambda + \tilde{\lambda}_{\min}})^{2C_2(\epsilon, \delta)}}{\lambda + \tilde{\lambda}_{\min}} + \lambda \right]. \quad (20)$$

The only thing that we need to privately release to choose λ is $\tilde{\lambda}_{\min}$ which has a fixed global sensitivity. The detailed procedure was summarized in Algorithm 1.

D.5 Proof of Theorem 2

We will now formally prove the theoretical guarantees of ADAOPS that we stated in Theorem 2.

Proof of Theorem 2 (i). First of all, $\tilde{\lambda}_{\min}$ has global sensitivity $\|\mathcal{X}\|^2$ by Weyl's lemma (Lemma 16). Using Gaussian mechanism, $\tilde{\lambda}_{\min}$ is an $(\epsilon/4, \delta/3)$ -DP release. Now, by the standard Gaussian tail bound, under the same probability event that holds with probability $1 - \delta/3$, we know that

$$\left| \tilde{\lambda}_{\min} - \lambda_{\min} \right| \leq \frac{\log(6/\delta)}{\epsilon/4}.$$

Condition on this event, and apply Lemma 12, we know $\log(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$ has (conditional) global sensitivity of $\log(1 + \frac{\|\mathcal{X}\|^2}{\tilde{\lambda}_{\min} + \lambda})$. So for any choice of λ (that uses only privately released information), the algorithm release $\log(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$ using Gaussian mechanism. Again by Gaussian tail bound, we know that Δ (in Algorithm 2) is a high probability upper bound of $\log(\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|)$ and the event is the same as the event of success in this $(\epsilon/4, \delta/3)$ -DP. In other word, we have that conditioning on the event with probability $1 - 2\delta/3$, for any data set (X, \mathbf{y}) and any target (x, y) .

$$|y - x^T \theta_\lambda^*| \leq \|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\| \leq e^\Delta \leq (\|\mathcal{Y}\| + \|\mathcal{X}\|\|\theta_\lambda^*\|) \left(1 + \frac{\|\mathcal{X}\|^2}{\lambda + \tilde{\lambda}_{\min}}\right)^{\frac{\log(6/\delta)}{\epsilon/4}}.$$

Denote $L := \|\mathcal{X}\|e^\Delta$ and choose γ according to the Step 7 of the algorithm block. Condition on the high probability event on the eigenvalue and local Lipschitz constant, the results in Theorem 10 (and the remark underneath it) implies that $\tilde{\theta}$ is an $(\epsilon/2, \delta/3)$ -pDP for all pairs of adjacent data sets that differs by adding or removing one data point. This by definition implies that we have converted the pDP guarantee to $(\epsilon/2, \delta/3)$ -DP.

Finally, by the adaptive simple composition of the three DP mechanisms, we conclude that ADAOPS is (ϵ, δ) -DP. ■

We now move on to analyze the utility of ADAOPS in terms of optimization error and estimation error (Statement (ii) and (iii) in Theorem 2).

Proof of Theorem 2 (ii). The key idea of the proof is to establish that the way λ is chosen according to (7) is effectively minimizing an upper bound of the optimization error, according to our derivation to that leads to (20). To start, note that C_1 and C_2 in (7) are both positive for any parameters that are passed into them, so the first term in the upper bound is monotonically decreasing in λ and the second term is monotonically increasing in λ so there is a unique λ minimizing the criterion.

Let \tilde{C}_1 be an arbitrary upper bound of C_1 . Also recall that $t_{\min} = \max\left\{\frac{\|\mathcal{X}\|^2(1+\log(6/\delta))}{2\epsilon} - \tilde{\lambda}_{\min}, 0\right\}$

$$\begin{aligned} \min_{t \geq t_{\min}} \frac{C_1 \|\mathcal{X}\|^4 \left(1 + \frac{\|\mathcal{X}\|^2}{t + \tilde{\lambda}_{\min}}\right)^{2C_2}}{t + \tilde{\lambda}_{\min}} + t &\leq \min_{t \geq \max\{t_{\min}, \|\mathcal{X}\|^2 C_2 - \tilde{\lambda}_{\min}\}} \frac{\tilde{C}_1 \|\mathcal{X}\|^4 \left(1 + \frac{1}{\lambda + \tilde{\lambda}_{\min}}\right)^{2C_2}}{t + \tilde{\lambda}_{\min}} + t \\ &\leq \min_{t \geq \max\{t_{\min}, \|\mathcal{X}\|^2 C_2 - \tilde{\lambda}_{\min}\}} \frac{e^2 \tilde{C}_1 \|\mathcal{X}\|^4}{t + \tilde{\lambda}_{\min}} + t \\ &\lesssim \min \left\{ \frac{e^2 \tilde{C}_1 \|\mathcal{X}\|^4}{\tilde{\lambda}_{\min}}, e \|\mathcal{X}\|^2 \sqrt{\tilde{C}_1} \right\}. \end{aligned} \quad (21)$$

The first inequality follows because we are increasing C_1 and also restricting the domain we optimize over, the second inequality uses that $(1 + 1/x)^x \leq e$ for all $x > 0$.

The third inequality is true when

$$e\sqrt{\tilde{C}_1} \geq \max \left\{ C_2, \frac{1 + \log(6/\delta)}{2\epsilon} \right\}.$$

To check this, discuss two cases of $\tilde{\lambda}$. In the first case, if $\tilde{\lambda}_{\min} \leq e\sqrt{\tilde{C}_1}\|\mathcal{X}\|^2$ we can take the feasible $t = e\|\mathcal{X}\|^2\sqrt{\tilde{C}_1}$ and obtain the second expression. In the second case, we know that taking $t = 0$ is feasible, which gives rise to the first bound.

Take $\tilde{C}_1 = C_1 \vee e^{-2}C_2^2 \vee e^{-2} \frac{(1+\log(6/\delta))^2}{4\epsilon^2}$.

We now look closer into parameters in C_1 and C_2 of (7).

First of all, since $\tilde{\epsilon} < \epsilon/2$,

$$\bar{\epsilon} = \epsilon/2 - \frac{\epsilon^2}{8} \left[\frac{1}{\log(6/\delta)} + \frac{1 + \log(6/\delta)}{\log(6/\delta)} \right] \leq \epsilon/2 - \frac{\tilde{\epsilon}^2}{2} \left[\frac{1}{\log(6/\delta)} + \frac{1 + \log(6/\delta)}{\log(6/\delta)} \right] \leq \tilde{\epsilon}.$$

This implies that $\bar{\epsilon} < \epsilon/2$. On the other hand, by the assumption that $\epsilon < 2 \log(6/\delta)/(1 + \log(6/\delta))$, $\bar{\epsilon} > \epsilon/2 - \epsilon/4 = \epsilon/4$.

It follows that

$$\begin{aligned} \tilde{C}_1 &= \max\{C_1(\bar{\epsilon}, \delta/3, \varrho, d), C_2(\epsilon/4, \delta/3)^2 e^{-2}, e^{-2} \frac{(1 + \log(6/\delta))^2}{4\epsilon^2}\} \\ &= \max\left\{ \frac{[d/2 + \sqrt{d \log(1/\varrho)} + \log 1/\varrho] \log(6/\delta)}{\bar{\epsilon}^2}, \frac{16 \log(6/\delta)^2}{\epsilon^2 \epsilon^2}, \frac{(1 + \log(6/\delta))^2}{4\epsilon^2 \epsilon^2} \right\} \\ &\leq \frac{16 \log(6/\delta) \max\{[d/2 + \sqrt{d \log(1/\varrho)} + \log 1/\varrho], \frac{\log(6/\delta)}{\epsilon^2}\}}{\epsilon^2} \\ &= O\left(\frac{\max\{d, \log(1/\varrho)\} \log(6/\delta) + \log^2(6/\delta)}{\epsilon^2}\right). \end{aligned}$$

Apply the above upper bound to (21) and then to (20), we get that with probability $1 - 2\delta/3 - \varrho$, then simultaneously,

$$\begin{aligned} F(\tilde{\theta}) - F(\theta^*) &\leq O\left(\frac{(\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \|\mathcal{X}\|^2 (d + \log(1/\varrho)) \log(6/\delta) + \log^2(6/\delta)}{\epsilon^2 \tilde{\lambda}_{\min}}\right), \\ F(\tilde{\theta}) - F(\theta^*) &\leq O\left(\frac{(\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta^*\|^2) \sqrt{(d + \log(1/\varrho)) \log(6/\delta) + \log^2(6/\delta)}}{\epsilon}\right). \end{aligned}$$

The first bound is the smaller of the two only when $\tilde{\lambda}_{\min} \geq \sqrt{\tilde{C}_1}$ and in such cases

$$\frac{1}{\lambda_{\min}} \leq \frac{1}{\tilde{\lambda}_{\min} - \|\mathcal{X}\|^2 \frac{\log(6/\delta)}{\epsilon/4}} = O\left(\frac{1}{\|\mathcal{X}\|^2 \sqrt{\tilde{C}_1}}\right).$$

The proof is complete by converting λ_{\min} into the alternative normalized representation with $\alpha = \frac{d\lambda_{\min}}{n\|\mathcal{X}\|^2}$. ■

It remains to prove the results about the estimation error under the linear Gaussian model.

Proof of Theorem 2 (iii). Note that $\lambda_{\min} \geq \alpha n/d$. As we've seen in the proof of Statement (ii), with probability $1 - \delta/3$,

$$\tilde{\lambda}_{\min} \geq \lambda_{\min} - \|\mathcal{X}\|^2 \frac{4 \log(6/\delta)}{\epsilon}.$$

Let this be event E . Event E ensures that (under the stated assumption on ϵ, δ) we have $\frac{4 \log(6/\delta)}{\epsilon} < \frac{\alpha n}{2d}$, this implies that $\tilde{\lambda}_{\min} > 0.5\lambda_{\min}$ and in addition, the automatic choice of λ using (7) will be $\lambda = 0$.

$$\mathbb{E}(\tilde{\theta}|X, E) = \mathbb{E}\left[\mathbb{E}[\tilde{\theta}|X, E, \mathbf{y}, L, \tilde{\lambda}] \mid X, E\right] \stackrel{\text{Lemma 8}}{=} \mathbb{E}[\theta_\lambda^*|X, E] \stackrel{\lambda=0 \text{ under } E}{=} \mathbb{E}[\theta^*|X, E] = \theta_0$$

$$\begin{aligned} \text{Cov}(\tilde{\theta}|X, E) &= \mathbb{E}\left[\text{Cov}[\tilde{\theta}|X, E, \mathbf{y}, L, \tilde{\lambda}] \mid X, E\right] + \text{Cov}\left[\mathbb{E}[\tilde{\theta}|X, E, \mathbf{y}, L, \tilde{\lambda}] \mid X, E\right] \\ &= \mathbb{E}\left[\frac{L^2 \log(6/\delta)}{\tilde{\lambda}_{\min} \tilde{\epsilon}^2} \mid X, E\right] (X^T X)^{-1} + \text{Cov}[\theta^*|X, E] \\ &\prec \frac{\mathbb{E}[L^2|X, E] \log(6/\delta)}{(\lambda_{\min}/2)(\epsilon/4)^2} (X^T X)^{-1} + \sigma^2 (X^T X)^{-1} \end{aligned} \tag{22}$$

Plugging in the consequence of E into the expression of L in the Algorithm 1, we have

$$\begin{aligned}
L &= \|\mathcal{X}\| e^\Delta = e^{\log(\|\mathcal{Y}\| + \|\mathcal{X}\| \|\theta^*\|) + \frac{\log(1 + \|\mathcal{X}\|^2 / \tilde{\lambda}_{\min})}{\epsilon/4} \sqrt{\log(6/\delta)} Z + \frac{\log(1 + \|\mathcal{X}\|^2 / \tilde{\lambda}_{\min})}{\epsilon/4} \log(6/\delta)} \\
&= \|\mathcal{X}\| (\|\mathcal{Y}\| + \|\mathcal{X}\| \|\theta^*\|) (1 + \|\mathcal{X}\|^2 / \tilde{\lambda}_{\min})^{\frac{\log(6/\delta)}{\epsilon/4}} (1 + \|\mathcal{X}\|^2 / \tilde{\lambda}_{\min})^{\frac{\sqrt{\log(6/\delta)}}{\epsilon/4}} Z \\
&\leq \|\mathcal{X}\| (\|\mathcal{Y}\| + \|\mathcal{X}\| \|\theta^*\|) e^{\frac{\|\mathcal{X}\|^2 \log(6/\delta)}{\lambda_{\min} \epsilon/8}} e^{\frac{\|\mathcal{X}\|^2 \sqrt{\log(6/\delta)}}{\lambda_{\min} \epsilon/8}} Z \\
&\leq \|\mathcal{X}\| (\|\mathcal{Y}\| + \|\mathcal{X}\| \|\theta^*\|) e \cdot e^Z
\end{aligned}$$

Take expectation of L^2 , use the independence of Z and \mathbf{y} we get

$$\begin{aligned}
\mathbb{E}[L^2 | X, E] &= \mathbb{E}[\|\mathcal{X}\|^2 (\|\mathcal{Y}\| + \|\mathcal{X}\| \|\theta^*\|)^2] e^2 \mathbb{E}[e^{2Z}] \\
&= e^4 (2\|\mathcal{X}\|^2 \|\mathcal{Y}\|^2 + 2\|\mathcal{X}\|^4 \mathbb{E}[\|\theta^*\|^2 | X]) \\
&= 2e^4 \|\mathcal{X}\|^2 (\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta_0\|^2 + \sigma^2 \|\mathcal{X}\|^2 \text{tr}[(X^T X)^{-1}])
\end{aligned}$$

where in the second line, we used the formula for the moment generating function of standard normal distribution, and then in the third line, we used that $\theta^* \sim \mathcal{N}(\theta_0, \sigma^2 (X^T X)^{-1})$. Substitute into (22) and replace λ_{\min} with $n\|\mathcal{X}\|^2 \alpha/d$ we get

$$\text{Cov}(\tilde{\theta} | X, E) \prec \left(1 + \frac{64e^4 \left[\|\mathcal{Y}\|^2 + \|\mathcal{X}\|^2 \|\theta_0\|^2 + \sigma^2 \|\mathcal{X}\|^2 \text{tr}[(X^T X)^{-1}] \right] d \log(6/\delta)}{\alpha \sigma^2 n \epsilon^2} \right) \sigma^2 (X^T X)^{-1}$$

as claimed. ■

E Utility lemmas

Lemma 13 (Gaussian tail bound). *Let $X \sim \mathcal{N}(0, 1)$. Then*

$$\mathbb{P}(|X| > \epsilon) \leq \frac{2e^{-\epsilon^2/2}}{\epsilon}.$$

Lemma 14 (χ^2 -distribution tail bound (Laurent & Massart, 2000, Lemma 1)). *Let X follows a χ^2 distribution with k degree of freedom, then for all $t > 0$, we have*

$$\begin{aligned}
\mathbb{P}(X - k \geq 2\sqrt{kt} + 2t) &\leq e^{-t}, \\
\mathbb{P}(k - X > 2\sqrt{kt}) &\leq e^{-t}.
\end{aligned}$$

Lemma 15 (Tail bound to (ϵ, δ) -DP conversion). *Let $\epsilon(\theta) = \log(\frac{p(\theta)}{p'(\theta)})$ where p and p' are densities of θ . If*

$$\mathbb{P}(|\epsilon(\theta)| > t) \leq \delta$$

then for any measurable set \mathcal{S}

$$\mathbb{P}_p(\theta \in \mathcal{S}) \leq e^t \mathbb{P}_{p'}(\theta \in \mathcal{S}) + \delta.$$

and

$$\mathbb{P}_{p'}(\theta \in \mathcal{S}) \leq e^t \mathbb{P}_p(\theta \in \mathcal{S}) + \delta$$

Proof. Since $\log(\frac{p(\theta)}{p'(\theta)}) = -\log(\frac{p'(\theta)}{p(\theta)})$ and the tail bound is two-sided. It suffices for us to prove just one direction. Let E be the event that $|\epsilon(\theta)| > t$.

$$\mathbb{P}_p(\theta \in \mathcal{S}) = \mathbb{P}_p(\theta \in \mathcal{S} \cup E^c) + \mathbb{P}_p(\theta \in \mathcal{S} \cup E) \leq \mathbb{P}_{p'}(\theta \in \mathcal{S} \cup E) e^t + \mathbb{P}_p(\theta \in E) \leq e^t \mathbb{P}_{p'}(\theta \in \mathcal{S}) + \delta.$$

■

Lemma 16 (Weyl’s eigenvalue bound (Stewart, 1998, Theorem 1)). *Let $X, Y, E \in \mathbb{R}^{m \times n}$, w.l.o.g., $m \geq n$. If $X - Y = E$, then $|\sigma_i(X) - \sigma_i(Y)| \leq \|E\|$ for all $i = 1, \dots, n$.*

Lemma 17 (Stability of smooth learning problems, Lemma 14 of (Wang, 2017)). *Assume ℓ and r be differentiable and their gradients be absolute continuous. Let $\hat{\theta}$ be a stationary point of $\sum_i \ell(\theta, z_i) + r(\theta)$, $\hat{\theta}'$ be a stationary point $\sum_i \ell(\theta, z_i) + \ell(\theta, z) + r(\theta)$ and in addition, let $\eta_t = t\hat{\theta} + (1 - t)\hat{\theta}'$ denotes the interpolation of $\hat{\theta}$ and $\hat{\theta}'$. Then the following identity holds:*

$$\begin{aligned} \hat{\theta} - \hat{\theta}' &= \left[\int_0^1 \left(\sum_i \nabla^2 \ell(\eta_t, z_i) + \nabla^2 \ell(\eta_t, z) + \nabla^2 r(\eta_t) \right) dt \right]^{-1} \nabla \ell(\hat{\theta}, z) \\ &= - \left[\int_0^1 \left(\sum_i \nabla^2 \ell(\eta_t, z_i) + \nabla^2 r(\eta_t) \right) dt \right]^{-1} \nabla \ell(\hat{\theta}', z). \end{aligned}$$

F (ϵ, δ) -DP calibration of OPS for linear regression.

This appendix describes the details of how we implement the non-adaptive version of OPS as a baseline.

OPS was proposed as a ϵ -pure-DP mechanism via the use of the exponential mechanism. In this paper, we are working with (ϵ, δ) -DP and it is only fair to compare to a version of OPS with (ϵ, δ) -DP. Such guarantees are studied by Mir (2013, Chapter 5) and later by Minami et al. (2016), but neither can be straightforwardly and satisfactorily applied to the linear regression problem.

Minami et al. (2016) requires that the loss function is Lipschitz. Linear regression is not Lipschitz unless we constraint $|\Theta|$ as in Assumption A2 just like for OBJPERT then it becomes Lipschitz. With appropriate choice of λ and γ and using ideas in Section D.4. Unfortunately, unlike OBJPERT, OPS is not an optimization based method. Sampling from the posterior distribution subject to the additional constraint requires techniques such as rejection sampling, which we find very costly, and prone to numerical issues.

Mir (2013) does not require an explicit constraint on the parameter space. Instead, they use a large regularization parameter λ , so that with probability $1 - \delta$ over the distribution of the OPS mechanism, the output is not too much larger than Ridge regression solution, which effectively produces a constraint on the domain. Then they apply an exponential mechanism-based argument after conditioning on this high-probability event. See Section 5.4.1 of (Mir, 2013) for details. Unfortunately, this approach yields a suboptimal rate under (ϵ, δ) -DP, which depends linearly in d rather than the optimal \sqrt{d} dependence.

The pDP analysis of linear regression of Wang (2017) suggests that we do not actually need global Lipschitz constant, instead the local Lipschitz constant at θ_λ^* is sufficient for us to obtain differential privacy. For any data set (X, \mathbf{y}) , we can show that

$$\|\theta_\lambda^*\| \leq \|(X^T X + \lambda I)^{-1} X^T\|_2 \sqrt{n} \|\mathcal{Y}\| \leq \min \left\{ \frac{\sqrt{n} \|\mathcal{Y}\|}{\sqrt{2\lambda}}, \frac{n \|\mathcal{X}\| \|\mathcal{Y}\|}{\lambda} \right\}. \quad (23)$$

The local Lipschitz constant at θ_λ^* is therefore smaller than

$$\frac{\sqrt{n} \|\mathcal{X}\|^2 \|\mathcal{Y}\|}{\sqrt{2\lambda}} + \|\mathcal{X}\| \|\mathcal{Y}\| = \|\mathcal{X}\| \|\mathcal{Y}\| \left(\frac{\sqrt{n} \|\mathcal{X}\|}{\sqrt{2\lambda}} + 1 \right) =: L(\lambda).$$

Apply Remark 11 with the above Lipschitz constant upper bound and also take $\lambda_{\min} = 0$, we get a pDP guarantee for any pairs of adjacent data sets, which by definition, upgrades into a DP guarantee. In other word, we can achieve a prescribed (ϵ, δ) -DP by choosing choose any (λ, γ) such that they obey

$$\epsilon \leq \sqrt{\frac{\gamma L(\lambda)^2 \log(2/\delta)}{\lambda}} + \frac{\gamma L(\lambda)^2}{2(\lambda + \|\mathcal{X}\|^2)} + \frac{(1 + \log(2/\delta)) \|\mathcal{X}\|^2}{2\lambda}.$$

There are many ways of doing it. If we fix $\lambda > \frac{(1 + \log(2/\delta)) \|\mathcal{X}\|^2}{2\epsilon}$, then we can calibrate γ to achieve any (ϵ, δ) -DP guarantee for any (ϵ, δ) . If we instead fix γ so that we have a comfortable level of variance, then similarly we can calibrate λ to achieve any (ϵ, δ) -DP guarantee for any (ϵ, δ) .

Specifically, we will experiment with the following three approaches:

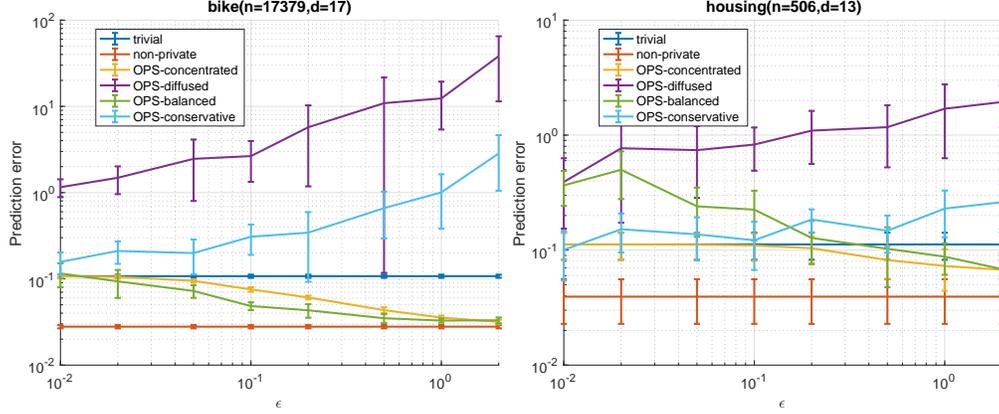


Figure 5: Comparison of the utility of (ϵ, δ) -DP OPS using four different ways of calibrating noise to privacy. The results show that how we calibrate noise plays an important role in the utility of the algorithms.

1. OPS-Diffuse: Take $\lambda = \frac{(1+\log(2/\delta))\|\mathcal{X}\|^2}{\epsilon}$ and calibrate γ .
2. OPS-Concentrated: Take $\gamma = 1$ and calibrate λ .
3. OPS-Balanced: Choose λ to minimize the prediction accuracy upper bound that we have from Section D.4

$$F(\hat{\theta}) - F(\theta^*) \leq \frac{C_1(\min(\epsilon, \sqrt{\epsilon}), \delta, \varrho, d)L(\lambda)^2}{\lambda} + \lambda B^2 \quad (24)$$

subject to $\lambda \geq \frac{(1+\log(2/\delta))\|\mathcal{X}\|^2}{\epsilon}$ ⁷. Once λ is chosen, we then calculate γ properly using the “diffused” approach given this λ . In (24), the function C_1 is defined in (18) and we choose $\varrho = 0.05$. B is a more delicate hyperparameter since there isn’t an upper bound of $\|\theta^*\|$ that holds uniformly for all data sets. We will be using $B = 1$ as we are being optimistic.

4. OPS-Conservative: An alternative approach that avoids choosing B is to use $\|\theta_\lambda^*\| \leq \|\theta^*\|$ so that the minimizer of the upper bound λ does not depend on $\|\theta^*\|$.

In our experiments, we find that no single approach dominates the others. In general, we find that the “concentrated” approach and the “balanced” approach with $B = 1$ work significantly better than the “diffused” and the “conservative” approaches (see Figure 5 for details). The experimental results with legend label “OPS” in Figure 2, Table 3 and Table 4 are for the “balanced” approach.

Below, we provide an error bound of the balanced approach.

Proposition 18. Assume $\|\theta^*\| \asymp B$ on this specific data set. Then OPS in unbounded domain with $\gamma = \frac{\epsilon^2 \lambda}{4 \log(2/\delta) L(\lambda)^2}$ and $\lambda = \left(\frac{C_1(\epsilon, \delta, \varrho, d) \|\mathcal{X}\|^4 \|\mathcal{Y}\|^2 n}{B^2} \right)^{1/3}$. obeys (ϵ, δ) -DP, and also

$$F(\hat{\theta}) - F(\theta^*) \leq O\left(\frac{d^{1/3} n^{1/3} \log(2/\delta)^{1/3} \|\mathcal{X}\|^{4/3} \|\mathcal{Y}\|^{2/3} \|\theta^*\|^{4/3}}{\epsilon^{2/3}} \right).$$

Proof. The result follows straightforwardly by substituting the $L(\lambda)$ and our choice of λ, γ into (24) checking that λ ’s choice balances the two terms. ■

⁷Note that this upper bound is obtained for $\gamma = \frac{\lambda \min(\epsilon^2, \epsilon)}{4 \log(2/\delta) L(\lambda)^2}$ and assuming $\|\theta^*\| \leq B$.