

# Analyzing the Differentially Private Theil-Sen Estimator for Simple Linear Regression

Jayshree Sarathy  
Northeastern University  
Boston, MA, USA  
j.sarathy@northeastern.edu

Salil Vadhan  
Harvard University  
Boston, MA, USA  
salil\_vadhan@harvard.edu

## Abstract

In this paper, we study differentially private point and confidence interval estimators for simple linear regression. Motivated by recent work that highlights the strong empirical performance of an algorithm based on robust statistics, `DPTHeilSen`, we provide a rigorous, finite-sample analysis of its privacy and accuracy properties, offer guidance on setting hyperparameters, and show how to produce differentially private confidence intervals to accompany its point estimates.

## Keywords

differential privacy, linear regression, robust statistics, confidence intervals

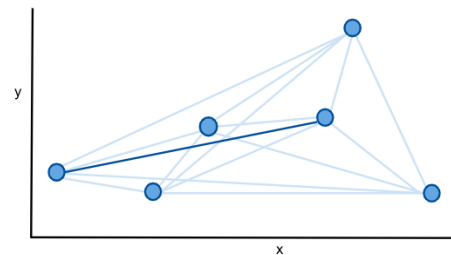
## 1 Introduction

Science and social science research often requires analyzing sensitive datasets. However, decades of study and real-world attacks have shown that release of many, accurate pieces of statistical information can enable reconstruction of the data subjects' sensitive attributes [12, 25]. One promising solution is *differential privacy* (DP) [29], a rigorous mathematical framework for characterizing privacy loss. Over the last several years, DP has become a widely accepted standard for protecting the privacy of data subjects while releasing useful statistical information about datasets [1, 4, 15]. Yet, designing *usable* DP methods for common statistical inference tasks remains an ongoing challenge [10, 38, 48].

In this work, we focus on the problem of creating usable DP methods for simple (i.e. one-dimensional) linear regression, which is one of the most fundamental tasks in data analysis. Practitioners from the social sciences have found that there is a lack of guidance and theoretical tools to help researchers choose accurate DP algorithms for simple linear regression on regimes commonly used in practice [10]. For example, in 2018, the prominent economics research group, Opportunity Insights, searched for a DP algorithm that would maintain high accuracy in the setting of small-area analysis, with 40 to 400 datapoints per regression [21]. Despite much review of the literature and engagement with DP experts, the group could not find DP techniques that provided adequate utility. Instead, they turned to a heuristic method that did not satisfy the formal guarantees of DP to release linear regression estimates within their high-profile Opportunity Atlas tool [21, 22].

Recent work has started to address these gaps around practical DP algorithms for simple linear regression in real-world settings. In particular, Alabi et al. [2] conducted an empirical evaluation of several DP algorithms for simple linear regression. They found that a suite of robust, median-based algorithms, `DPTHeilSen`, based on the non-private Theil-Sen estimator developed by Theil [52] and Sen [49], performed better than standard OLS-based algorithms across a range of practical regimes. In particular, `DPTHeilSen` provided significant accuracy benefits over sufficient statistics perturbation and gradient descent approaches when the dataset size, variance of the independent variable, and privacy-loss parameter is small. Alabi et al.'s work opened up a new line of research around this estimator [5, 43], yet our work is the first to analyze the versions of `DPTHeilSen` that exhibit the strongest empirical performance.

Studying the Theil-Sen estimator is fruitful for enhancing our practical toolkit around linear regression as well advancing our theoretical understanding of robust and private algorithms. In the non-private setting, not only is Theil-Sen one of the most commonly used robust estimators in practice [33], offering better accuracy compared to Ordinary Least Squares (OLS) for data that is skewed or has outliers, it is also a easy-to-implement algorithm with connections to a wide range of other robust or nonparametric techniques. As shown in Figure 1, the non-private algorithm proceeds in two straightforward steps: first, it computes the slope for some or all pairs of points and second, it uses a median sub-routine to output a single estimate of the slope. To make the algorithm satisfy DP, the median sub-routine can be replaced with a DP analogue.<sup>1</sup>



**Figure 1: Illustration of the standard non-private Theil-Sen algorithm [49, 52], which computes the slopes between all pairs of points (light blue) and outputs the median slope (dark blue).**

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit <https://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

*Proceedings on Privacy Enhancing Technologies 2025(1)*, 216–235  
© 2025 Copyright held by the owner/author(s).  
<https://doi.org/10.56553/popets-2025-0013>

<sup>1</sup>The intercept can be computed either along with the slope or using the final estimate of the slope, as described in [49] and [2].

While Alabi et al.'s empirical study was a valuable starting point in highlighting the strong performance of DPTheilSen, the authors stated that further theoretical understanding of the accuracy guarantees, as well as design of uncertainty estimates, would be needed to make this set of algorithms fully usable in practice. This assessment is shared by Barrientos et al. [10], who in their survey of DP linear regression algorithms emphasize various criteria for designing feasible and practical algorithms in practice, including: assumptions that align with practical applications, ease of implementation, computational efficiency, minimal tuning parameters, and development of uncertainty estimates.

In this paper, we address these open questions by analyzing the accuracy guarantees of the DPTheilSen algorithms. Our contributions can be summarized as follows.

- (1) We provide a rigorous theoretical analysis of the DPTheilSen algorithms shown to perform strongly by Alabi et al. [2]. Our analyses offer finite-sample convergence bounds and shed light on *why* and *when* DPTheilSen outperforms other DP linear regression algorithms.
- (2) We design and analyze DP confidence intervals for simple linear regression via DPTheilSen.

We intentionally restrict our focus in this work to the one-dimensional setting. There is a rich literature around DP linear regression, but most of these works jump directly to high-dimensional data and machine learning contexts [13, 18, 35, 50, 53, 54, e.g.]. However, results about optimal algorithms in high-dimensional contexts are not directly applicable to the one-dimensional problem, which is a setting still widely used in social science applications and one that has posed barriers to adoption of DP [21]. In particular, Alabi et al. [2] show that leading algorithms in the multi-dimensional setting, such as gradient descent approaches, do not necessarily exhibit strong performance in the one-dimensional context. Rather, a tailored analysis of algorithms such as DPTheilSen that have proven to be empirically strong is essential. Explaining the performance of DPTheilSen in the one-dimensional setting is a natural theoretical question and is a stepping stone to understanding and designing better DP linear regression methods in higher dimensions, as well as other DP algorithms based on robust statistics.

Overall, our work aims to make DP linear regression significantly more usable for practitioners. Before providing an overview of our main results, we describe the problem of simple linear regression and the assumptions we make in this work, which are minimal.

## 1.1 Simple linear regression

We are given  $n$  values,  $x_1, \dots, x_n$ , of the predictor variable  $x$ . For each  $x_i$ , we observe the corresponding value  $y_i$  of the response random variable  $y$ . The model is  $y_i = \beta_0 + \beta_1 x_i + e_i$  for  $i = 1, \dots, n$ , where  $\beta_0$  and  $\beta_1$  are unknown parameters. We make the following assumptions:

**Assumption 1.1.1.**  $x_1, \dots, x_n$  are fixed and not all equal.

**Assumption 1.1.2.** Each  $e_i$  is sampled independently from the same continuous, symmetric, mean-0 distribution  $F_e$ .

Note that these assumptions are relevant only to the utility analysis of the linear regression algorithms.<sup>2</sup> Our privacy analysis does not rely on these assumptions and provides the usual protections of DP on  $(x, y)$  pairs. Our goal is to design and analyze  $\epsilon$ -DP point and interval estimators for the slope  $\beta_1$ .

A common formulation of linear regression is the Ordinary Least Squares (OLS) objective, which is characterized by the following optimization problem:

$$(\hat{\beta}_0, \hat{\beta}_1) = \arg \min_{\beta_0, \beta_1 \in \mathbb{R}} \|\mathbf{y} - \beta_1 \mathbf{x} - \beta_0 \mathbf{1}\|_2,$$

where  $\mathbf{x} = (x_1, \dots, x_n)^T$ ,  $\mathbf{y} = (y_1, \dots, y_n)^T$ , and  $\mathbf{1}$  is the all-ones vector. OLS has a simple closed form solution:

$$\hat{\beta}_1 = \frac{\text{ncov}(\mathbf{x}, \mathbf{y})}{\text{nvar}(\mathbf{x})} \quad \text{and} \quad \hat{\beta}_0 = \bar{y} - \hat{\beta}_1 \bar{x},$$

where  $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ ,  $\bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$ ,  $\text{ncov}(\mathbf{x}, \mathbf{y}) = \langle \mathbf{x} - \bar{x}\mathbf{1}, \mathbf{y} - \bar{y}\mathbf{1} \rangle$ , and  $\text{nvar}(\mathbf{x}) = \langle \mathbf{x} - \bar{x}\mathbf{1}, \mathbf{x} - \bar{x}\mathbf{1} \rangle$ . When  $\mathbf{y}$  is generated according to the model  $y_i = \beta_0 + \beta_1 \cdot x_i + e_i, \forall i \in [n]$  for i.i.d. Gaussian noise  $e_i$ , then the OLS solution is the maximum likelihood estimator. If we remove the assumption of Gaussian noise and add privacy constraints, however, robust estimators such as Theil-Sen have been shown to provide better accuracy [2, 30]. In this work, we analyze DP algorithms based on Theil-Sen, comparing them to the OLS-based approaches. Below, we provide brief descriptions of these two approaches:

- **OLS-based algorithms:** The DPSuffStats algorithm [2, 32, 53] follows the OLS approach closely, in that it involves perturbing the sufficient statistics  $\text{ncov}(\mathbf{x}, \mathbf{y})$  and  $\text{nvar}(\mathbf{x})$ . While this algorithm is computationally efficient and enables releasing the DP sufficient statistics at no extra privacy cost, it has been shown to not perform well in common regimes.<sup>3</sup> A second algorithm is DPOLSEXP [3, 11], which implements the exponential mechanism [46] with the OLS objective function.
- **Theil-Sen-based algorithms:** Theil-Sen [49, 52] is a family of robust linear regression estimators that proceed via two steps (as illustrated in Fig. 1) for estimating the slope  $\beta_1$ : (1) compute the slope for some or all pairs of points, and (2) output the median of these estimates. To make this algorithm DP, we can simply replace the median with a DP median. Although there are many choices for the DP median, we consider a version of this algorithm, DPWideTS, which uses the *widened exponential mechanism* [2, 46] as the DP median sub-routine, as this version has been shown to exhibit strong empirical performance by [2]. The DPWideCIUnion version of the algorithm does so by outputting an interval that contains the non-private interval with high probability, while the DPWideCI algorithm outputs a tighter interval via more nuanced coverage analysis.

## 1.2 Overview of results

This work offers two main contributions: finite-sample guarantees and confidence intervals for DPTheilSen. First, we provide

<sup>2</sup>In particular for the first assumption, we analyze accuracy as a function of the  $x$ -values, as is common in regression analyses in the statistics literature. Analyses for random  $x$ 's can be interpreted as being done conditional on the  $x$ -values.

<sup>3</sup>In particular, [2] showed that DPSuffStats performs poorly in the high privacy, small dataset, and/or clustered independent variable regime.

a finite-sample convergence bound for DPWideTS, the variant of DP Theil-Sen that was recommended by Alabi et al. [2]. We attain the convergence bound by developing a finite-sample analysis of non-i.i.d.  $U$ -statistics [20, 39], which may be of independent interest.

We state our convergence bound informally below. While our main analysis does not require any data assumptions beyond the ones stated above (Assumptions 1.1.1 and 1.1.2), the theorem is stated for a special case, where the independent variables  $x_1, \dots, x_n$  are evenly split between the endpoints of an interval of length  $\Delta_x$  (known as an *asymptotically optimal design* [49]), and the noise variables  $e_1, \dots, e_n$  are drawn i.i.d. from  $\mathcal{N}(0, \sigma_e^2)$ . The asymptotically optimal design is common in the non-private literature and often found in practice (e.g. to model treatment and control groups).

**Theorem 1.2 (Main result applied for a special case of asymptotically optimal design, informally stated).** Let  $\tilde{\beta}_1^{\text{DPWideTS}}$  be the DPWideTS estimator with privacy loss parameter  $\epsilon$ , hyperparameter  $R$  for the range of the outputs, and hyperparameter  $\theta$  for the granularity of the outputs. Assume that the true slope  $\beta_1$  lies in the interval  $[-R + \theta, R - \theta]$ . Let  $\tau$  be defined as follows.

$$\tau = \Phi^{-1} \left( 1 - \frac{p}{8} \right) \cdot \sqrt{\frac{4}{3n}} + O \left( \frac{\ln(R/p\theta)}{\epsilon n} \right)$$

where  $\Phi^{-1}$  is the inverse standard normal distribution function. Then, for suff. large  $n$ , and suff. small  $\tau$  and  $\sigma_e/\Delta_x$ , we have that with probability at least  $1 - p$ ,

$$\begin{aligned} \tilde{\beta}_1^{\text{DPWideTS}} &\in [\beta_1 - z - \theta, \beta_1 + z + \theta] \\ \text{for } z &= \frac{\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \left( \tau + O \left( \tau^{3/2} \right) \right). \end{aligned}$$

The constants in our accuracy bounds are universal and do not depend on any parameters of the problem. Thus our results are considered finite-sample. As the accuracy bounds (intentionally) depend on the private  $x$ -values, it is not useful to specify these constants; in practice, one should use our DP confidence intervals to estimate uncertainty.

In Table 1 below, we provide an informal comparison between the convergence bounds for DPWideTS (described above) and the OLS-based DPSuffStats algorithm for this setting (analyzed in [3]). We also compare these DP estimators with their non-private counterparts. Notation is provided in the caption.

We can see that DPWideTS maintains the same leading constant of  $2\sqrt{\pi}/3$  as that of non-private TS, while non-private OLS and DPSuffStats have a leading constant of 2, so the latter are slightly better in the asymptotic  $n \rightarrow \infty$  regime. The bounds for DPWideTS and DPSuffStats both contain lower-order terms corresponding to the noise due to privacy. For DPWideTS, we see a logarithmic dependence on the output range  $R$ , as compared to the quadratic dependence shown by DPSuffStats on the input range  $r$ . Our comparison provides theoretical backing to the empirical finding of Alabi et al. [2]—that the quantity  $\epsilon n \Delta_x^2$  is important in choosing between the standard DPSuffStats algorithm and the robust DPWideTS algorithm. In particular, when  $\epsilon n \Delta_x^2$  is small, which indicates a high privacy, small dataset size, and/or clustered independent variable regime, DPWideTS is the more accurate estimator.

Finally, our convergence bound enables us to provide guidance on setting the  $\theta$  hyperparameter (corresponding to the granularity of the widened exponential mechanism) for DPWideTS, which was a key open problem raised by Alabi et al. [2] towards making this algorithm usable for practitioners.

Estimator	$1 - p$ Convergence Bound
Non-priv OLS	$\frac{2\sigma_e}{\Delta_x} \cdot \frac{c_{p/2}}{\sqrt{n}}$
Non-priv TS	$\sqrt{\frac{\pi}{3}} \cdot \frac{2\sigma_e}{\Delta_x} \cdot \frac{c_{p/4}}{\sqrt{n}}$
DPSuffStats [3]	$\frac{2\sigma_e}{\Delta_x} \cdot \frac{c_{p/6}}{\sqrt{n}} \cdot (1 + \tau) + \tau (1 + \tau +  \beta_1 ),$ $\tau \approx \frac{(1-1/n)r^2 \log(3/p)}{\epsilon \cdot n \cdot \Delta_x^2}$
DPWideTS (Thm. 1.2)	$\sqrt{\frac{\pi}{3}} \cdot \frac{2\sigma_e}{\Delta_x} \cdot \left( \frac{c_{p/8}}{\sqrt{n}} + \gamma \right) (1 + o(1))$ $+ \gamma, \gamma \approx \frac{\ln(R/p\theta)}{\epsilon n}$

**Table 1:  $(1 - p)$ -convergence bounds for simple linear regression point estimators in special case of asymptotically optimal design.  $r$  is range for both the input  $x_i, y_i$  datapoints,  $R$  is range for the output estimate of  $\beta_1$ , and  $c_{p/2} = \Phi^{-1}(1 - p/2) = \Theta(\log(1/p))$  for small  $p$ .**

In addition to analyzing the DPWideTS point estimator, we design and analyze corresponding confidence interval estimators for simple linear regression. We describe two algorithms—DPWideTSCUnion and DPWideTSCI—and analyze their privacy, coverage, and accuracy guarantees.

We use the DP median estimators proposed by Drechsler et al. [27] as sub-routines in our algorithms, making them additionally usable by analyzing the width of the confidence intervals they provide. We show that the confidence interval for DPWideTSCUnion is approximately twice as large as the convergence bound for DPWideTS, and can be further improved using the algorithm DPWideTSCI with some tradeoff in computational efficiency.

### 1.3 Related work

Linear regression is one of the most fundamental tasks in statistics and has received much attention in the DP literature [8, 9, 13, 18, 35, 43–45, 47, 50, 53, 54]. Although we cannot provide a full survey here, we note that most prior works focus on non-robust methods, require additional assumptions on the data or model, or only provide asymptotic analysis. With respect to simple linear regression, Alabi et al. [2] conducted an experimental evaluation of DP algorithms, demonstrating that DP analogues of robust algorithms, such as DPTheilSen, perform better than non-robust methods in practical settings—in particular, when the dataset size, variance of the independent variables, and/or privacy loss parameter is small. However, Alabi et al. did not provide theoretical bounds or DP confidence intervals for this estimator, which are open questions we address in this work.

Our work draws on the rich connections between robust statistics and DP [6, 30, 40]. Dwork and Lei [30] stated that “robust estimators are a useful starting point for constructing highly accurate differentially private estimators.” They gave an asymptotic analysis of what they called the “Short-Cut Regression Method,” which is similar to a simplified variant of DPTheilSen. However, they did not consider the more statistically efficient variants that we do in this work, provide finite sample guarantees, or offer measures of uncertainty for the estimates like the confidence intervals we provide. Other works [7, 23] confirm the findings of Dwork and Lei in the context of hypothesis testing, showing that robust estimators perform better than parametric estimators under differential privacy, even when the data comes from a parametric model. However, these works provide either empirical or asymptotic guarantees rather than finite-sample analysis.

Our confidence interval algorithms build upon Drechsler et al. [27]’s non-parametric DP confidence intervals for the median, but ours are more general in that they provide finite-sample validity for some forms of non-i.i.d. variables and characterizes the width of the confidence intervals. Prior work has also considered DP confidence intervals for mean estimation [28, 37, 41], but these cannot directly be applied for the median-based estimator we consider. Other work produces DP confidence intervals using bootstrapping [9, 16, 26, 36], but these can be expensive to compute and rely on assumptions, such as normally distributed errors, that our work avoids. To the best of our knowledge, our work is the first to theoretically analyze the different variants of DPTheilSen as well as to design and analyze non-parametric, differentially private confidence intervals to accompany its point estimates.

## 1.4 Concurrent Work

Since our results were first announced,<sup>4</sup> there has been a flurry of work that uses median-based approaches for DP tasks [17, 24, 43, 45, 47] and clarifies the connections between privacy and robustness [6, 40]. We do not provide a comprehensive survey here but touch on the most relevant works.

Amin et al. [5] provide empirical evaluation of higher-dimensional variations of Theil-Sen, but unlike our work, do not offer theoretical bounds on accuracy or convergence. Knop and Steinke [43], on the other hand, do provide theoretical privacy and utility analysis of some of the DP Theil-Sen algorithms in higher dimensions, as well as an experimental evaluation. They offer a finite-sample convergence bound that is consistent with our results, but their statement only applies for the highly simplified variant of DPTheilSen where each data point is used only once, so only  $n/2$  slopes are computed and the slopes are independent of each other. Our results are more general and can handle cases that achieve provably stronger performance by reusing data points and introducing correlations. Examples include the asymptotically optimal design of Thm. 1.2 and the full Theil-Sen variant where all  $\binom{n}{2}$  points are used.<sup>5</sup> In addition, Knop and Steinke’s results are stated for the setting where features and noise are Gaussian, and they do not aim to match the leading constant of the non-private estimators, which is an

<sup>4</sup>This work was presented at the Workshop on Theory and Practice of DP in 2021.

<sup>5</sup>Note that the simplified variant of Theil-Sen can be analyzed using a Chernoff-Hoeffding bound, while the versions of Theil-Sen with correlated slopes require more complex analytical tools such as U-statistics.

important feature of our results. While Knop and Steinke analyze these algorithms in the high-dimensional setting, we find that the one-dimensional case is already a challenging and understudied regime to analyze with correlated slopes.

Recent work has also significantly advanced our understanding of the connection between robust and private algorithms. Asi et al. [6] establish a tight connection between privacy and robustness, providing a black-box transformation from optimal robust to optimal differentially private algorithms. They also design and analyze estimators for DP linear regression for high-dimensional tasks under assumptions of Gaussianity. Hopkins et al. [40] show how to implement this black-box transformation in a computationally efficient manner via the sum-of-squares method. While these methods provide important general toolkits for designing DP algorithms, they do not provide finite-sample bounds for specific estimators such as DPTheilSen.

Finally, studies analyzing the practical use of DP have further highlighted the need for more usable DP algorithms for basic statistical tasks such as simple linear regression. A study of data practitioners’ use of DP by Sarathy et al. [48] calls for algorithms with minimal hyperparameters and assumptions, as well as useful uncertainty measures, that will enable data analysts to navigate the constraints of the DP analysis process. In addition, work by Barrientos et al. [10] evaluates a range of DP linear regression algorithms in terms of feasibility for real-world use. They develop criteria for usable algorithms, including: assumptions that align with practical applications, ease of implementation, computational efficiency, minimal tuning parameters, and accompanied by uncertainty estimates. Barrientos et al. find that a surprisingly few number of DP algorithms satisfy these criteria. We believe that developing the design and analysis of DPTheilSen enables this suite of algorithms to better align with these criteria, making DPTheilSen more usable for real-world DP deployments.

## 2 Preliminaries

We consider datasets that are multisets. The space of datasets is denoted by  $\text{Multisets}(\mathcal{D}, n)$ , where  $\mathcal{D}$  is the underlying set of elements and  $n$  is the cardinality of each multiset. Let  $\text{dist}_{\text{ms}}(\mathbf{d}, \mathbf{d}')$  be the number of records that must be changed to transform dataset  $\mathbf{d}$  into another dataset  $\mathbf{d}'$ .<sup>6</sup>

Since our algorithms include hyperparameters, we state a definition of DP for algorithms that take as input not only the dataset, but also the desired privacy parameters and any required hyperparameters. Two datasets  $\mathbf{d}, \mathbf{d}' \in \text{Multisets}(\mathcal{D}, n)$  are *neighboring*, denoted  $\mathbf{d} \sim \mathbf{d}'$ , if  $\text{dist}(\mathbf{d}, \mathbf{d}') = 1$ . Let  $\mathcal{H}$  be a hyperparameter space and  $\mathcal{Y}$  be an output space.

**Definition 2.0.1** (Differential Privacy [31]). For  $\epsilon \in \mathbb{R}_{\geq 0}$ , a randomized algorithm  $M : \text{Multisets}(\mathcal{D}, n) \times \mathbb{R}_{\geq 0} \times \mathcal{H} \rightarrow \mathcal{Y}$  is  $\epsilon$ -DP if and only if for all neighboring datasets  $\mathbf{d} \sim \mathbf{d}' \in \text{Multisets}(\mathcal{D}, n)$  hyperparams  $\in \mathcal{H}$ , and sets  $E \subseteq \mathcal{Y}$ ,

$$\begin{aligned} \Pr[M(\mathbf{d}, \epsilon, \text{hyperparams}) \in E] \\ \leq e^\epsilon \cdot \Pr[M(\mathbf{d}', \epsilon, \text{hyperparams}) \in E]. \end{aligned}$$

where the probabilities are taken over the random coins of  $M$ .

<sup>6</sup>I.e. “change-one distance” [19]).

Now, we will define the non-private Theil-Sen family of estimators.

**Definition 2.0.2** (Theil-Sen Estimator [49, 52]). Let  $(x_1, y_1), \dots, (x_n, y_n)$  be an arbitrary ordering of dataset  $\mathbf{d} \in \text{Multisets}(\mathbb{R} \times \mathbb{R}, n)$ . Let  $S$  be a set of  $N$  unordered pairs of elements of  $[n] = \{1, \dots, n\}$  such that for each pair  $\{i, j\} \in S$ ,  $x_i \neq x_j$ . Then, for each  $\{i, j\} \in S$ , compute the slope  $s_{ij}$  between the points  $(x_i, y_i)$  and  $(x_j, y_j)$  as follows:  $s_{ij} = (y_j - y_i)/(x_j - x_i)$ . Let  $\mathbf{s} = \{s_{ij}\}_{\{i,j\} \in S}$  denote the multiset of the slopes. The *Theil-Sen estimator*  $\hat{\beta}_1^{\text{TS}}$  with corresponding set  $S$  is computed as follows:  $\hat{\beta}_1^{\text{TS}} = \text{median}(\mathbf{s})$ .

### 3 DPTheilSen Algorithm

---

#### Algorithm 3.1: DPTheilSen: $\epsilon$ -DP Algorithm

---

**Data:**  $\mathbf{d} = (x_i, y_i)_{i=1}^n \in \text{Multisets}(\mathbb{R} \times \mathbb{R}, n)$ ,  
**Privacy params:**  $\epsilon \in \mathbb{R}_{\geq 0}$   
**Hyperparams:**  $S \in \binom{[n]}{2}$ , DPmed, hyperparams  $\in \mathcal{H}$   
 $\mathbf{s} = \{\}$   
**for each**  $\{i, j\} \in S$  **do**  
     **if**  $x_j \neq x_i$  **then**  
          $s_{ij,1} = (y_j - y_i)/(x_j - x_i)$   
          $s_{ij,2} = s_{ij,1}$   
     **else**  
          $s_{ij,1} = -\infty$   
          $s_{ij,2} = \infty$   
     Add  $s_{ij,1}$  and  $s_{ij,2}$  to  $\mathbf{s}$   
 Let  $k = \max_{i \in [n]} \#\{j \in [n] : \{i, j\} \in S\}$   
 $\tilde{\beta}_1^{\text{TS}} = \text{DPmed}(\mathbf{s}, \epsilon/2k, \text{hyperparams})$   
**return**  $\tilde{\beta}_1^{\text{TS}}$

---

In the differentially private version of Theil-Sen, which we call DPTheilSen (Algorithm 3.1), we similarly compute pairwise estimates of the slope. However, we replacing the computation of the median of the slopes with a differentially private median algorithm (denoted by DPmed, which can be one of several algorithms). DPmed takes as input the multiset of slopes,  $\mathbf{s} \in \text{Multisets}(\mathbb{R} \cup \{-\infty, \infty\}, N)$ , the scaled privacy parameter  $\epsilon/2k \in \mathbb{R}_{\geq 0}$ , where  $k$  is the max number of slopes computed using each datapoint, and the hyperparameters  $\in \mathcal{H}$  for the given median algorithm.

Note that the set  $S$  and value  $k$  are chosen independently of the dataset and are meant to capture different variants of the Theil-Sen algorithm. For example,  $S$  could be constructed by matching the  $i$ 'th data point with the  $(i + \lfloor n/2 \rfloor)$  th point, for  $1 \leq i \leq \lfloor n/2 \rfloor$ , or with a randomly chosen set of  $k \in [1, n-1]$  other points. Under bounded DP, changing one data point will not change  $S$  or  $k$ . In order to handle the cases where  $x_i = x_j$  under bounded DP, the DPTheilSen algorithm adds  $\infty$  and  $-\infty$  for that case, and otherwise adds each slope twice to the multiset  $\mathbf{s}$ .

**Lemma 3.0.1** ([2]). *Algorithm 3.1 (DPTheilSen) is  $\epsilon$ -DP.*

In this work, we consider a version of DPTheilSen called DPWideTS, which uses for DPmed the widened exponential mechanism, DPWide [2, 46], described below (Algorithm 3.2). This variant of DPTheilSen was found to have strong performance in the empirical work of [2].

---

#### Algorithm 3.2: Widened Exponential Mechanism for Quantile (DPWide): $\epsilon$ -DP Algorithm

---

**Data:**  $\mathbf{s} = (s_1, \dots, s_N) \in \mathbb{R}^N$   
**Privacy params:**  $\epsilon \in \mathbb{R}_{\geq 0}$   
**Hyperparams:**  $q \in (0, 1)$ ,  $-R, R \in \mathbb{R}^2$ ;  $\theta \in \mathbb{R}_{>0}$   
**Sort**  $\mathbf{s}$   
 /\* Clip  $\mathbf{s}$  to the range  $[-R, R]$  and insert space  $\theta$  around the  $q$ th quantile: \*/  
**for**  $i \in [1, \lfloor Nq \rfloor]$  **do**  
      $\lfloor \mathbf{s}[i] = \min(\max(-R, \mathbf{s}[i] - \theta), R)$   
**for**  $i \in [\lfloor Nq \rfloor + 1, N]$  **do**  
      $\lfloor \mathbf{s}[i] = \max(\min(R, \mathbf{s}[i] + \theta), -R)$   
 Insert  $-R$  and  $R$  into  $\mathbf{s}$  and set  $N = N + 2$   
 Set  $\text{maxNoisyScore} = -\infty$   
 Set  $\text{argMaxNoisyScore} = -1$   
**for**  $i \in [2, N)$  **do**  
      $\text{score} = \log(\mathbf{s}[i] - \mathbf{s}[i-1]) - \frac{\epsilon}{2} \cdot [|i - Nq|]$   
      $Z \sim \text{Gumbel}(0, 1)$   
      $\text{noisyScore} = \text{score} + Z$   
     **if**  $\text{noisyScore} > \text{maxNoisyScore}$  **then**  
          $\text{maxNoisyScore} = \text{noisyScore}$   
          $\text{argMaxNoisyScore} = i$   
 $\text{left} = \mathbf{s}[\text{argMaxNoisyScore} - 1]$   
 $\text{right} = \mathbf{s}[\text{argMaxNoisyScore}]$   
 Sample  $\tilde{q}^{\text{DPWide}} \sim \text{Unif}[\text{left}, \text{right}]$   
**return**  $\tilde{q}^{\text{DPWide}}$

---

Below, we state the standard utility theorem for DPWide with widening hyperparameter  $\theta$  on a fixed dataset  $\mathbf{s}$ . Let  $F_s^{-1}$  be the inverse empirical distribution function for the set of slopes,  $\mathbf{s}$ . We use the following assumption on the range and widening hyperparameters  $R, \theta \in \mathbb{R}_{>0}$ .

**Assumption 3.0.2.** For a target  $q \in (0, 1)$  and fixed dataset  $\mathbf{s} \in \mathbb{R}^N$ , the true quantile  $F_s^{-1}(q) \in [-R + \theta, R - \theta]$ .

**Theorem 3.0.3** (Utility of DPWide). *Let  $\mathbf{s} \in \mathbb{R}^N$  be a fixed sample of  $N$  points, and let  $F_s^{-1}$  be the inverse empirical distribution function. For  $q \in (0, 1)$ , let  $[-R, R]$ , the range hyperparameter, satisfy Assumption 3.0.2, and let  $\theta, \epsilon > 0$ . Let  $\tilde{q}^{\text{DPWide}} = \text{DPWide}(\mathbf{s}, \epsilon, (q, -R, R, \theta))$ . Then, for  $0 < c < \min(q, 1/2)$ ,*

$$\Pr_{\substack{\text{DPWide}(\mathbf{s}, \epsilon, \\ (q, -R, R, \theta))}} \left( \tilde{q}^{\text{DPWide}} \notin [F_s^{-1}(q - c) - \theta, F_s^{-1}(q + c) + \theta] \right) \leq \frac{R}{\theta} \exp\left(-\frac{\epsilon c N}{2}\right)$$

The widening parameter  $\theta$  needs to be carefully chosen. All outputs within  $\theta$  of the target quantile are given the same utility score, so a large  $\theta$  represents a lower bound on the performance. Conversely, choosing  $\theta$  too small may result in the area around the target quantile not being given sufficient weight in the sampled distribution. We describe how to set  $\theta$  for DPWideTS in Section 5.1.

## 4 Convergence Bound for DPWideTS

In this section, we provide a finite-sample analysis of DPWideTS. We look beyond asymptotics solely in  $n$ , as this will not explain the

strong empirical performance of the DPWideTS algorithm compared to others such as DPSuffStats, as shown by [2]. In addition, finite-sample analysis will allow us to better understand the *conditions* under which DPWideTS outperforms non-robust algorithms.

The main challenge of analyzing DPWideTS is that the slopes computed from  $S$  are correlated.<sup>7</sup> To deal with correlated slopes, [49] relies on the properties of *U-statistics* [39] for an asymptotic analysis of the non-private Theil-Sen algorithm.

**Definition 4.0.1** (U-statistic for simple linear regression [49]). Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1, and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$ . The U-statistic takes as input a “guess”  $\hat{\beta}_1 \in \mathbb{R}$  for the true slope  $\beta_1$ , as well as the datapoints  $(x_i, y_i)_{i=1}^n$ , indexed arbitrarily. Then, the *U-statistic for simple linear regression* is defined as follows.

$$U(\hat{\beta}_1, (x_i, y_i)_{i=1}^n) = \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign} \left( \frac{y_j - y_i}{x_j - x_i} - \hat{\beta}_1 \right), \quad (1)$$

where  $S$  is the set of unordered pairs of datapoints used to compute the slopes (where each pair has distinct  $x$  values),  $N = |S|$  is the number of such pairs, and  $\text{sign}(q) = -1$  if  $q < 0$ ,  $0$  if  $q = 0$ , and  $1$  if  $q > 0$ . For ease of notation, we will let  $\hat{\beta}_1 = \beta_1 + z$ , for some  $z \in \mathbb{R}$ , and use  $U_z$  as shorthand for  $U(\hat{\beta}_1, (x_i, y_i)_{i=1}^n)$ .

We build on this approach, adapting finite-sample ‘Berry-Esseen-type’ bounds for the convergence of the U-statistic in order to develop a finite-sample convergence bound for the DPWideTS estimate.

**Theorem 4.0.2** (Convergence bound for  $\tilde{\beta}_1^{\text{DPWideTS}}$ ). Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 and have empirical variance  $\sigma_x^2$ . Let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$ . Let  $\tilde{\beta}_1^{\text{DPWideTS}} = \text{DPTheilSen}(\{x_i, y_i\}_{i=1}^n, \varepsilon, (R, \theta))$ , where  $\varepsilon, R, \theta > 0$ ,  $\beta_1 \in [-R + \theta, R - \theta]$ , and  $S \in \binom{[n]}{2}$  is a set of unordered pairs with distinct  $x$ -values. Let  $U_z$  be the U-statistic defined with respect to  $S$ .

Then, there exists a constant  $c > 0$  such that for sufficiently large  $n$ , with probability at least  $1 - p$ ,  $\tilde{\beta}_1^{\text{DPWideTS}} \in [\beta_1 - z - \theta, \beta_1 + z + \theta]$  for every  $z$  that satisfies the following:

$$\frac{\mu(z) - \frac{4 \ln(4R/p\theta)}{\varepsilon \cdot n}}{\sigma(z)} \geq \Phi^{-1} \left( 1 - \frac{p}{2} + \frac{c}{n^2 \cdot \sigma^3(z)} \right)$$

where  $\mu(z) = \mathbb{E}[U_z]$ ,  $\sigma^2(z) = \text{Var}[U_z]$ , and  $\Phi$  is the std. normal cdf.

The quantities  $\mu(z)$  and  $\sigma^2(z)$  can be further described and evaluated, as shown in Sections B.1 and 5. In the next section, we provide an overview of the analysis and the use of the U-statistic. However, this result will be easier to interpret when applied to a special setting, as described in Section 5.

<sup>7</sup>We can avoid correlated slopes if we use an ‘incomplete’ version of the algorithm where each data point is only used in one slope, ie.  $k = 1$ . Our general analysis applies to this simplified version, as well as to variants that compute a linear # of total slopes for computational efficiency.

## 4.1 Overview of analysis

To analyze the performance of DPTheilSen, we further consider the U-statistic from Definition 4.0.1. In particular, we can rewrite statistic (1) in the form of a *Kendall’s tau statistic* [42] that measures the rank correlation between the  $x$ ’s and the residuals from a line of slope  $\beta_1 + z$ .

$$\begin{aligned} U_z &= U(\beta_1 + z, (x_i, y_i)_{i=1}^n) \\ &= \frac{1}{N} \sum_{\substack{\{i,j\} \in S \\ i < j}} \text{sign}(x_j - x_i) \cdot \text{sign}(e_j - e_i - z \cdot (x_j - x_i)) \end{aligned} \quad (2)$$

Suppose  $z = 0$ . Then, we define the *null U-statistic* as

$$\begin{aligned} U_0 &= U(\beta_1, (x_i, y_i)_{i=1}^n) \\ &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign}(x_j - x_i) \cdot \text{sign}(e_j - e_i) \end{aligned} \quad (3)$$

Furthermore, the distribution of  $U_0$  matches the null distribution of the Kendall’s  $\tau$ -statistic, which is known to be asymptotically normal [42]. Observe that  $\mathbb{E}_{e_1, \dots, e_n}[U_z] = 0$  since  $e_1, \dots, e_n$  are i.i.d. In fact, we have:

**Fact 4.1.1** ([49]).  $\mathbb{E}_{e_1, \dots, e_n}[U_z] = 0$  iff  $z = 0$ .

We will also point out another fact about the U-statistic, which will be used in our proof of Theorem 4.0.2.

**Fact 4.1.2** ([49]). For all  $z \in \mathbb{R}$ ,  $U_z$  is a non-increasing function.

Using these properties of the U-statistic, we proceed with the algorithm analysis in two steps.

(1) By the utility theorem of the widened exponential mechanism (Theorem 3.0.3), we show that with high probability,  $U(\tilde{\beta}_1^{\text{DPWideTS}}, (x_i, y_i)_{i=1}^n) \approx 0$ .

(2) Putting together  $U(\tilde{\beta}_1^{\text{DPWideTS}}, (x_i, y_i)_{i=1}^n) \approx 0$ , and the asymptotic normality of  $U_z$  for appropriate  $z$  (Theorem 4.2.1), we show that  $\tilde{\beta}_1^{\text{DPWideTS}} \approx \beta_1$  and characterize the finite-sample convergence of the estimator.

Note that the second step requires showing that  $U_z$ , not just  $U_0$ , is asymptotically normal, and we must characterize the convergence using the quantity  $z$  itself. We do so in the next section.

## 4.2 Finite-sample convergence of U-statistic

We develop a finite-sample bound for the absolute value difference between the distribution function of  $U_z$  and the standard normal distribution function  $\Phi$ . To do so, we modify Berry-Esseen bounds for linear functions, such as U-statistics, of i.i.d mean-0 random variables (see, e.g., [20]). In the case of the U-statistic  $U_z$  described in (2), the terms  $\text{sign}(e_j - e_i - z \cdot (x_j - x_i))$  for  $\{i, j\} \in S, i < j$  are non-identically distributed since  $x_j - x_i$  may be different for different pairs  $(i, j)$ . Therefore, we adapt the Berry-Esseen bounds to work for U-statistics of independent, *non-identical* random variables. Our finite-sample convergence bound is stated in Theorem 4.2.1 below and proved in the Appendix.

**Theorem 4.2.1.** Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 (ie. not all equal) and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is

sampled i.i.d from a continuous, symmetric, mean-0 distribution. Let  $S$  be a set of unordered pairs of datapoints such that each pair has distinct  $x$ -values, and let  $U_z$  be defined with respect to  $S$  as in (2). Let  $\mu(z) = \mathbb{E}_{e_1, \dots, e_n} [U_z]$ , and let  $\sigma^2(z) = \text{Var}_{e_1, \dots, e_n} [U_z]$ . Then, for sufficiently large  $n$ ,

$$\sup_{t \in \mathbb{R}} \left| \Pr \left[ \frac{U_z - \mu(z)}{\sigma(z)} \leq t \right] - \Phi(t) \right| = O \left( \frac{1}{n^2 \cdot \sigma^3(z)} \right)$$

where  $\Phi$  is the cdf of a standard normal distribution.

This result shows that the normalized U-statistic,  $U_z$ , converges to a standard normal distribution at a rate of  $O(1/(n^2 \cdot \sigma^3(z)))$ , where  $\sigma^2(z) = \Theta(1/n)$  is the variance of the U-statistic.<sup>8</sup>

### 4.3 Proof of Theorem 4.0.2

Here, we prove our first main result: the finite-sample convergence bound for  $\tilde{\beta}_1^{\text{DPWideTS}}$ . As described earlier in Section 4.1, the proof of Theorem 4.0.2 follows in two main steps; first, we argue that  $U(\tilde{\beta}_1^{\text{DPWideTS}})$  is close to 0 with high probability by utility theorem of the exponential mechanism (Theorem 3.0.3). Second, we use the convergence of the U-statistic distribution (Theorem 4.2.1) to show that  $\tilde{\beta}_1^{\text{DPWideTS}}$  is close to  $\beta_1$ .

**PROOF OF THEOREM 4.0.2.** First, we consider the event that  $\tilde{\beta}_1^{\text{DPWideTS}} > \beta_1 + z + \theta$ . We take a union bound over two possibilities that could lead to this event: the first is that  $U(\tilde{\beta}_1^{\text{DPWideTS}} - \theta)$  is less than an arbitrary value  $-c \in (-1, 0)$  (ie. DPWide returned an output that is more than  $cN/2$  away in rank from the median of the  $N$  slopes), which implies that  $\tilde{\beta}_1^{\text{DPWideTS}}$  is not within  $z$  of  $\beta_1$  with high probability. The second that  $U(\tilde{\beta}_1^{\text{DPWideTS}} - \theta)$  is within  $c$  of 0, yet  $\tilde{\beta}_1^{\text{DPWideTS}} - \theta$  is still more than  $z$  greater than  $\beta_1$ . We can simplify these expressions by noting that  $U$  is a non-increasing function (Fact 4.1.2). Then, for all  $z \in \mathbb{R}$  and sufficiently large  $n$ , we have that

$$\begin{aligned} & \Pr_{Y, \text{DPWide}} \left[ \tilde{\beta}_1^{\text{DPWideTS}} > \beta_1 + z + \theta \right] \\ & \leq \Pr_{Y, \text{DPWide}} \left[ U(\tilde{\beta}_1^{\text{DPWideTS}} - \theta, (x_i, y_i)_{i=1}^n) < -c \right] + \\ & \quad \Pr_{Y, \text{DPWide}} \left[ U(\tilde{\beta}_1^{\text{DPWideTS}} - \theta, (x_i, y_i)_{i=1}^n) \geq -c \cap \right. \\ & \quad \left. \tilde{\beta}_1^{\text{DPWideTS}} - \theta > \beta_1 + z \right] \\ & \leq \Pr_{Y, \text{DPWide}} \left[ U(\tilde{\beta}_1^{\text{DPWideTS}}, (x_i, y_i)_{i=1}^n) < -c \right] + \\ & \quad \Pr_{Y, \text{DPWide}} \left[ U(\beta_1 + z + \theta, (x_i, y_i)_{i=1}^n) \geq -c \right] \\ & \leq \Pr_{Y, \text{DPWide}} \left[ 1/2 - F_s(\tilde{\beta}_1^{\text{DPWideTS}}) < -c/2 \right] + \\ & \quad \Pr_{Y, \text{DPWide}} \left[ U(\beta_1 + z, (x_i, y_i)_{i=1}^n) \geq -c \right] \\ & \leq \frac{R}{\theta} \exp(-\varepsilon \cdot c \cdot N/4) + \left( 1 - \Phi \left( \frac{-c - \mu(z)}{\sigma(z)} \right) \right) + O \left( \frac{1}{n^2 \cdot \sigma^3(z)} \right) \end{aligned}$$

<sup>8</sup>For example, the variance of the U-statistic evaluated for the asymptotically optimal design is  $4/3n + O(1/n)$ , as shown in Lemma C.0.3. The general case is shown in Lemma B.1.2.

where  $F_s$  is the empirical distribution function for the set of slopes computed by DPWideTS. Then, the first term in the last line comes from Theorem 3.0.3 and the second term follows from Lemma 4.2.1. We can run through a similar analysis for the event that  $\tilde{\beta}_1^{\text{DPWideTS}} < \beta_1 - z - \theta$  to get the following:

$$\Pr_{Y, \text{DPWide}} \left[ \tilde{\beta}_1^{\text{DPWideTS}} < \beta_1 - z - \theta \right] \leq \frac{R}{\theta} \exp(-\varepsilon \cdot c \cdot N/4) + \Phi \left( \frac{c - \mu(-z)}{\sigma(-z)} \right) + O \left( \frac{1}{n^2 \cdot \sigma^3(-z)} \right)$$

Setting the first terms less than or equal to  $p/4$  and then solving for  $c$  and  $z$  gives the desired result. Finally, the expressions for  $\mu(z)$  and  $\sigma(z)$  follow directly from Lemmas B.1.1 and B.1.2.  $\square$

To make this result more interpretable, we apply this bound to a special setting in Section 5, providing intuition and comparison with convergence bounds for other non-DP and DP algorithms.

## 5 Evaluating Bound for Special Case

In this section, we will consider the special setting (called an asymptotically optimal design [49]) where the  $x$ -values are evenly split between the endpoints of an interval of length  $\Delta_x$ . The DPWideTS algorithm computes  $N = \lfloor n/2 \rfloor \cdot \lceil n/2 \rceil$  slopes<sup>9</sup> from pairs of datapoints on opposite ends of the interval. In addition, we assume that the noise variables are sampled i.i.d from a normal distribution.

**Assumption 5.0.1.**  $x_1, \dots, x_{\lfloor n/2 \rfloor} = 0, x_{\lfloor n/2 \rfloor + 1}, \dots, x_n = \Delta_x$ .

**Assumption 5.0.2.**  $F_e = \mathcal{N}(0, \sigma_e^2)$ .

In Theorem 1.2 below, we state a convergence bound for this special case. The bound relies on the general bound of Theorem 4.0.2 along with evaluations of the expectation and variance of the U-statistic. We are able to simplify the expressions for the expectation and variance because in this special case, all of the slopes are drawn from an identical distribution, yet we still require Theorem 4.0.2 because the slopes are correlated.

**Theorem 1.2.** Let  $x_1, \dots, x_n$  be at two endpoints of an interval of size  $\Delta_x$  such that they satisfy Assumption 5.0.1, and let  $e_1, \dots, e_n$  be drawn i.i.d from  $F_e = \mathcal{N}(0, \sigma_e^2)$  according to Assumption 5.0.2. Let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$ . Let  $\tilde{\beta}_1^{\text{DPWideTS}} = \text{DPTheilSen}(\{x_i, y_i\}_{i=1}^n, \varepsilon, (\text{DPWide}, \theta, -\tau))$  where  $\varepsilon, R, \theta > 0$ , and  $\beta_1 \in [-R + \theta, R - \theta]$  as in Assumption 3.0.2. Let  $\tau$  be defined as follows.

$$\tau = \Phi^{-1} \left( 1 - \frac{p}{8} \right) \cdot \sqrt{\frac{4}{3n} + \frac{8 \ln(4R/p\theta)}{\varepsilon n}}$$

where  $\Phi^{-1}$  is the inverse standard normal distribution function. Then, we have that for sufficiently large  $n$ , where for some constant  $c$ ,  $n \geq c \left( \log(R/p\theta) / \varepsilon \sqrt{\log(1/p)} \right)^2$ , and sufficiently small  $\tau$ , we have that with probability at least  $1 - p$ ,

$$\begin{aligned} & \tilde{\beta}_1^{\text{DPWideTS}} \in [\beta_1 - z - \theta, \beta_1 + z + \theta] \\ & \text{for } z = \frac{2\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \left( \tau + O \left( \tau^{3/2} \right) \right). \end{aligned}$$

<sup>9</sup>Our analysis extends to efficient versions of this algorithm that compute a linear, rather than quadratic, number of slopes.

PROOF. We start with the bound from Theorem 4.0.2 and substitute the expressions for  $\mu(z)$  and  $\sigma^2(z)$  using Lemmas C.0.2 and C.0.3 in the Appendix. This gives the following: for sufficiently large  $n$  and sufficiently small  $z \cdot \Delta_x / \sigma_e$ ,  $\hat{\beta}_1^{\text{DPWideTS}} \in [\beta_1 - z - \theta, \beta_1 + z + \theta]$  provided that

$$z \geq \frac{\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \left( \Phi^{-1} \left( 1 - \frac{p}{4} + \frac{c_1}{n^2 \cdot \sigma^3(z)} \right) \cdot \sqrt{\left( \frac{4}{3n} + e_{\sigma^2}(z) \right) + \frac{8 \ln(4R/p\theta)}{\epsilon n} + e_{\mu}(z)} \right) \quad (4)$$

where the error terms  $e_{\sigma^2}(z)$  and  $e_{\mu}(z)$  are bounded as follows

$$e_{\sigma^2}(z) \leq \frac{c_2 \cdot \Delta_x \cdot z}{n \cdot \sigma_e} + \frac{c_3}{n^2} \text{ and } e_{\mu}(z) \leq \frac{c_4 \cdot \Delta_x^3 \cdot z^3}{\sigma_e^3}$$

and where  $c_1, c_2, c_3, c_4 > 0$  are constants. Now, we will show that  $z$  can actually be set so as to satisfy condition (4). In particular, it can be shown that setting  $z$  as

$$z := \frac{2\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \left( \tau + c_2 \cdot \tau^{3/2} \right) \\ \text{for } \tau = \Phi^{-1} \left( 1 - \frac{p}{8} \right) \cdot \sqrt{\frac{4}{3n} + \frac{8 \ln(4R/p\theta)}{\epsilon n}}$$

satisfies condition (4). To see this, first note that for any  $z \in \mathbb{R}$ ,  $\sigma^2(z) \geq 4/3n$  by Lemma C.0.3. Then, for  $n \geq (6c_1/p)^2$ , we have that

$$\Phi^{-1} \left( 1 - \frac{p}{4} + \frac{c_1}{n^2 \cdot \sigma^3(z)} \right) \leq \Phi^{-1} \left( 1 - \frac{p}{8} \right).$$

Using this, we can see that for  $n \geq \max(3c_3/4, 8c_2^2(\Phi^{-1}(1-p/8))^2, (6c_1/p)^2)$ , we can bound the highest-order term on the right-hand side of (4) as follows.

$$\begin{aligned} & \frac{\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \Phi^{-1} \left( 1 - \frac{p}{4} + \frac{c_1}{n^2 \cdot \sigma^3(z)} \right) \cdot \sqrt{\left( \frac{4}{3n} + e_{\sigma^2}(z) \right)} \\ & \leq \frac{\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \Phi^{-1} \left( 1 - \frac{p}{8} \right) \cdot \left( \sqrt{\frac{4}{3n}} + \sqrt{\frac{2 \cdot c_2 \cdot \tau}{n}} + \sqrt{\frac{2 \cdot c_2^2 \cdot \tau^{3/2}}{n}} + \sqrt{\frac{c_3}{n^2}} \right) \\ & \leq \frac{\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \tau \cdot \left( 1 + \sqrt{3 \cdot c_2 \cdot \tau} + \sqrt{3 \cdot c_2 \cdot \tau^4} \right) \\ & \leq \frac{2\sqrt{\pi} \cdot \sigma_e}{\Delta_x} \cdot \left( \tau + c_2 \cdot \tau^{3/2} \right) \\ & = z \end{aligned}$$

where the first inequality follows from the condition that  $n > (6c_1/p)^2$ , the second inequality follows for  $n > 3c_3/4$  and the definition of  $\tau$ , and the third inequality follows from  $n > 8(c_2 \cdot \Phi^{-1}(1-p/8))^2$ . From this, we can see that there exists a setting of  $z$  that satisfies condition (4), which completes the proof.  $\square$

Table 2 shows the DPWideTS convergence bound for this special setting, along with convergence bounds for the non-private algorithms OLS and Theil-Sen and the private algorithms DPSuffStats and DPOLSEXP [3] (these were described briefly in Section 1.1), all under the same assumptions.

The first two bounds in the table correspond to the non-private algorithms OLS and Theil-Sen. Both of these non-private algorithms have a convergence rate of  $O(\sigma_e \cdot c_p / \Delta_x \cdot \sqrt{n})$ . Looking at the leading constant, we see that Theil-Sen nearly recovers the accuracy of OLS, up to a factor of  $\sqrt{\pi/3}$ . The Theil-Sen bound has the term  $c_{p/4}$  instead of  $c_{p/2}$ , which comes from the convergence of the U-statistic to a standard normal distribution at a rate of  $O(1/\sqrt{n})$  (Theorem 4.2.1).

The bounds for DPSuffStats and DPTheilSen have the same constant factors for the highest order term as OLS and Theil-Sen, respectively, but they also contain two main differences from their non-private counterparts. First, the DP estimators have constant factor changes in  $p$  in the  $c_p$  terms compared to those in the non-private bounds; this comes from the DP estimators taking a union bound over both the sampling and privacy error, which splits up the failure probability  $p$  further. Note that  $c_p = \Theta(\sqrt{\log(1/p)})$  for small  $p$ , so these constant factor changes in  $p$  are not impactful.

Second, the DP estimators include lower order terms corresponding to the noise due to privacy,<sup>10</sup> which provide insight into the relative performance of the DP algorithms in practical regimes. For example, we can see that DPSuffStats's lower order term  $\tau$  is  $O(r^2/\epsilon \cdot n \cdot \Delta_x^2)$ ; the  $\epsilon n \Delta_x^2$  quantity in the denominator was highlighted in the empirical work of [2] as important for the performance of the algorithm but lacked theoretical backing prior to our work.<sup>11</sup> Meanwhile, the lower order term in DPOLSEXP has the quantity  $\sqrt{\epsilon n} \Delta_x$  in the denominator, which indicates that it performs better than DPSuffStats for small  $n$  and for small  $\epsilon$ . The lower order term in DPWideTS has the quantity  $\epsilon n \Delta_x$  in the denominator, which indicates that it performs better than DPSuffStats for small  $\Delta_x$ , but not as well as DPOLSEXP in the small  $\epsilon$  regime.

Finally, we can compare the DPSuffStats, DPOLSEXP, and DPWideTS bounds in terms of their dependence on hyperparameters. While DPSuffStats has a quadratic dependence on  $r$ , the range of the input datapoints, the other two algorithms avoid any dependence on the range of the inputs. Instead, DPOLSEXP has a square root dependence on the range  $R$  of the output estimate, while DPWideTS has a milder logarithmic dependence on  $R$ . The bound for DPWideTS also includes the parameter  $\theta$  (corresponding to the granularity of outputs in DPWide). In Section 5.1, we discuss how to set this parameter, addressing an open question of [3].

## 5.1 Choosing the widening parameter, $\theta$

Theorem 1.2 offers insight on how to set  $\theta$  in the DPWideTS algorithm, which was an open question raised by [2]. For fixed  $p, \epsilon, R, \sigma_e, \Delta_x$ , and  $n$  that satisfy the conditions stated in the Theorem, we can set  $\theta$  to minimize the bound as follows:

$$\theta \approx \max \left( \frac{\sigma_e \cdot \ln(R\epsilon n \Delta_x / p \sigma_e)}{\epsilon n \Delta_x}, \frac{R}{p} \exp(-\epsilon n) \right)$$

The first term in the max comes from allowing the two terms involving  $\theta$  in Thm. 1.2 to be approximately equal, whereas the second

<sup>10</sup>For example, the  $\ln(R/p\theta)/\epsilon n$  term for DPWideTS corresponds to the noise due to privacy, which is  $O(1/\epsilon n)$  and thus overshadowed by the sampling error  $O(1/\sqrt{n})$  for sufficiently large  $n$ .

<sup>11</sup>Alabi et al. specifically looked at the quantity  $\epsilon \cdot n \cdot \sigma_x^2$ , where  $\sigma_x^2$  is the empirical variance of the constants  $x_1, \dots, x_n$ , but they did not provide theoretical basis for the importance of this quantity. In our special setting,  $\Delta_x^2 = 4\sigma_x^2$ .



Estimator	Size of $1 - p$ Convergence Bound	Constraints
OLS	$2 \cdot \frac{\sigma_e}{\Delta_x} \cdot \frac{c_{p/2}}{\sqrt{n}}$	
Theil-Sen [49]	$2 \cdot \sqrt{\frac{\pi}{3}} \cdot \frac{\sigma_e}{\Delta_x} \cdot \frac{c_{p/4}}{\sqrt{n}}$	
DPSuffStats [3]	$2 \cdot \frac{\sigma_e}{\Delta_x} \cdot \frac{c_{p/6}}{\sqrt{n}} \cdot (1 + \tau) + \tau (1 + \tau +  \beta_1 ),$ $\tau \approx \frac{12(1-1/n)r^2 \log(3/p)}{\epsilon \cdot n \cdot \Delta_x^2}$	$p \in (3 \exp(-\epsilon n \Delta_x^2 / 12), 1)$
DPOLSExp [3]	$2 \cdot \frac{\sigma_e}{\Delta_x} \cdot \frac{c_{p/4}}{\sqrt{n}} + \sqrt{\frac{64R \cdot (3 \log(3) + \log(2/p))}{\epsilon n \Delta_x^2}}$	
DPWideTS (Thm 1.2)	$2 \cdot \sqrt{\frac{\pi}{3}} \cdot \frac{\sigma_e}{\Delta_x} \cdot \left( \frac{c_{p/8}}{\sqrt{n}} + \frac{4\sqrt{3} \ln(4R/p\theta)}{\epsilon \cdot n} \right) + \theta$	$p \in (0, 4R/\theta),$ $\frac{\sigma_e}{\Delta_x}$ suff. small, $n$ suff. large

**Table 2: High-probability  $(1 - p)$  convergence bounds for estimators for special setting (Assumptions 5.0.1 and 5.0.2). Note that  $r$  is a hyperparameter range for both the input  $x_i, y_i$  datapoints, while  $R$  is a range for the output estimate of the slope.**

term in the max comes from upper bounding  $O(\ln(R/p\theta)/\epsilon n)$  by some constant. The reason for having both terms is to account for both widespread and concentrated slopes.<sup>12</sup> The factor  $\sigma_e/(n\Delta_x)$  in the first term corresponds to the standard deviation of the slopes computed by DPWideTS; when the slopes are highly concentrated, the first term becomes small. The second term, however, is independent of  $\sigma_e$  and  $\Delta_x$ , which allows  $\theta$  to remain bounded away from 0 and prevents a blowup in the convergence bound. Note that  $R, \epsilon, n$  and  $p$  are known in practice; if the experimental design suggests that the slopes may be concentrated (e.g. if the x-values are located at one of two endpoints of an interval as in this special case), our analysis suggests setting  $\theta$  to scale with the second term.

### 6 Confidence Intervals for DPWideTS

In this section, we design and analyze DP confidence intervals for the linear regression slope  $\beta_1$ . We adapt the ExpMech(Union) algorithm from Drechsler et al. [27] as a subroutine for our setting (see Algorithm 6.1) and prove its validity and accuracy in Theorem 6.3.1 (See Appendix). We begin by describing both the non-private Theil-Sen and DPTheilSen confidence intervals.

**Definition 6.0.1** (Confidence intervals for simple linear regression.). Let  $\mathbf{d} = (x_i, y_i)_{i=1}^n$  be a dataset real-valued pairs, where  $x_1, \dots, x_n$  are fixed values that are not all equal, and  $y_1, \dots, y_n$  are the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$ . Let  $I_{\mathbb{R}}$  be the set of all intervals in  $\mathbb{R}$ , and let  $M_{\text{nonpriv}} : \text{Multisets}(\mathbb{R} \times \mathbb{R}, n) \times \mathcal{H} \rightarrow I_{\mathbb{R}}$  be a deterministic mechanism that outputs an interval. For any  $\alpha_1 \in (0, 1)$ ,  $M_{\text{nonpriv}}$  outputs a  $(1 - \alpha_1)$ -confidence interval for the

slope  $\beta_1$  if for all hyperparams  $\in \mathcal{H}$ , and sufficiently large  $n$ ,

$$\Pr_{e_1, \dots, e_n \sim F_e} [\beta_1 \in M_{\text{nonpriv}}(\mathbf{d}, \text{hyperparams})] \geq 1 - \alpha_1$$

where the probability is over the randomness of the dataset  $\mathbf{d}$ .

Next, let  $M_{\text{DP}} : \text{Multisets}(\mathbb{R} \times \mathbb{R}, n) \times \mathbb{R}_{>0} \times \mathcal{H} \rightarrow I_{\mathbb{R}}$  be a randomized  $\epsilon$ -DP mechanism that outputs an interval. For any  $\alpha \in (0, 1)$ ,  $M_{\text{DP}}$  outputs a  $(1 - \alpha)$ -DP confidence interval for the slope  $\beta_1$  if for all privacy loss parameters  $\epsilon \in \mathbb{R}_{>0}$ , hyperparams  $\in \mathcal{H}$ , and sufficiently large  $n$ ,

$$\Pr_{e_1, \dots, e_n \sim F_e}^{M_{\text{DP}}} [\beta_1 \in M_{\text{DP}}(\mathbf{d}, \epsilon, \text{hyperparams})] \geq 1 - \alpha$$

where the probability is over the randomness of both the dataset  $\mathbf{d}$  and the mechanism  $M_{\text{DP}}$ .

### 6.1 Nonprivate Confidence Intervals for Theil-Sen

Now, we briefly describe the *non-private* confidence interval for Theil-Sen. This estimator returns the  $(1/2 - b)$ th and  $(1/2 + b)$ th quantiles of the set of Theil-Sen slopes,  $\mathbf{s}$ , where  $b$  is computed according to the distribution of the corresponding U-statistic.

**Definition 6.1.1.** Let  $S$  be a set of  $N$  unordered pairs of points, and let  $U_0$  be the corresponding null U-statistic given by Definition 4.0.1, Equation 3). For the corresponding set of slopes  $\mathbf{s}$ , let  $F_{\mathbf{s}}$  be the empirical distribution function for  $\mathbf{s}$ . Let  $\sigma^2(0) = \text{Var}_{e_1, \dots, e_n} [U_0]$  as evaluated in Corollary B.1.3. For any  $\alpha_1 \in (0, 1)$ , let  $b$  be defined as follows:

$$b := \frac{1}{2} \cdot \Phi^{-1} \left( 1 - \frac{\alpha_1}{8} \right) \cdot \sigma(0)$$

where  $\Phi$  is the standard normal cdf. Let  $\hat{\beta}_{1L} = F_{\mathbf{s}}^{-1}(1/2 - b)$  and  $\hat{\beta}_{1U} = F_{\mathbf{s}}^{-1}(1/2 + b)$ . Then, the *non-private  $1 - \alpha_1$ -Theil-Sen confidence interval* is  $[\hat{\beta}_{1L}, \hat{\beta}_{1U}]$ .

<sup>12</sup>Handling the case of concentrated slopes was [2]’s original motivation for designing the widened exponential mechanism.

**Lemma 6.1.2.** For any  $\alpha_1 \in (0, 1)$ , let  $[\hat{\beta}_{1L}, \hat{\beta}_{1U}]$  be the non-private Theil-Sen confidence interval as in Definition 6.1.1. Then, there exists a constant  $c > 0$  such that for all  $n \geq c/\alpha_1^2$ ,  $[\hat{\beta}_{1L}, \hat{\beta}_{1U}]$  is a  $(1 - \alpha_1)$ -confidence interval for the true slope  $\beta_1$ .

The proof of validity can be found in the Appendix.

## 6.2 DPTSCI Algorithm

Now, we consider the differentially private confidence interval for  $\beta_1$ , DPTSCI, which we describe in Algorithm 6.1 (See Appendix). This algorithm is similar to the DPTheilSen point estimator (Alg. 3.1), except that we replace the call to DPMed with a call to an  $\epsilon$ -DP confidence interval algorithm for the median, DPMedCI.

---

### Algorithm 6.1: DPTSCI: $\epsilon$ -DP Algorithm

---

**Data:**  $\mathbf{d} = (x_i, y_i)_{i=1}^n \in \text{Multisets}(\mathbb{R} \times \mathbb{R}, n)$

**Privacy params:**  $\epsilon \in \mathbb{R}_{\geq 0}$

**Hyperparams:**  $S \in \binom{[n]}{2}$ , DPMedCI, hyperparams  $\in \mathcal{H}$   
 $\mathbf{s} = \{ \}$

**for each**  $\{i, j\} \in S$  (such that  $x_i \neq x_j$ ) **do**

**if**  $x_j \neq x_i$  **then**  
 $s_{ij,1} = (y_j - y_i)/(x_j - x_i)$   
 $s_{ij,2} = s_{ij,1}$

**else**  
 $s_{ij,1} = -\infty$   
 $s_{ij,2} = \infty$

Add  $s_{ij,1}$  and  $s_{ij,2}$  to  $\mathbf{s}$

Let  $k = \max_{i \in [n]} \{ \#j \in [n] : \{i, j\} \in S \}$

$[\tilde{\beta}_{1L}^{\text{TS}}, \tilde{\beta}_{1U}^{\text{TS}}] = \text{DPMedCI}(\mathbf{s}, \epsilon/2k, \text{hyperparams})$

**return**  $[\tilde{\beta}_{1L}^{\text{TS}}, \tilde{\beta}_{1U}^{\text{TS}}]$

---

**Lemma 6.2.1.** Algorithm 6.1 is  $\epsilon$ -DP.

**PROOF.** The call to DPMedCI is  $\epsilon/k$ -DP by definition, so by simple composition and post-processing, DPTSCI is  $\epsilon$ -DP.  $\square$

## 6.3 DPWideCIUnion

In Algorithm 6.2, we describe one possible algorithm for the DPMedCI subroutine: DPWideCI(Union). This algorithm is based on a non-parametric confidence interval for the median designed by Drechsler et al. [27]. The idea is to run the DPWide point estimator twice such that with high probability, the two estimates capture the true slope  $\beta_1$ . The DPWideCIUnion algorithm does so by outputting an interval that contains the non-private interval with high probability, while the DPWideCI algorithm outputs a tighter interval via more nuanced coverage analysis. While Drechsler et al. [27] assume that the inputs to the confidence interval mechanism are sampled i.i.d. from a population distribution, here we only assume that we have a uniform bound on the convergence of the empirical distribution  $F_s$  to the standard normal distribution (which we develop in Thm. 4.2.1).

Let DPWideTSCIUnion = DPTSCI( $\mathbf{d}, \epsilon, S, \text{DPWideCIUnion}, (\alpha, r_\alpha, \theta, -R, R, \text{Union}=1)$ ), where DPWideCIUnion is defined in Algorithm 6.2.

---

### Algorithm 6.2: DPWideCI(Union): $\epsilon$ -DP Algorithm

---

**Data:**  $\mathbf{s} = (s_1, \dots, s_N) \in \mathbb{R}^N$

**Privacy params:**  $\epsilon \in \mathbb{R}_{> 0}$

**Hyperparams:**  $\alpha \in (0, 1), r_\alpha \in (0, 1), \theta \in \mathbb{R}_{> 0}, [-R, R] \subset \mathbb{R}, \text{Union} \in \{0, 1\}$

**if Union then**

Let  $\alpha_1 = r_\alpha \cdot \alpha$  and  $\alpha_2 = (1 - r_\alpha) \cdot \alpha$   
 Let  $b = \frac{1}{2} \cdot \Phi^{-1}(1 - \alpha_1/8) \cdot \sigma(0) // \sigma^2(0)$  is the variance of the null U-statistic,  $U_0$ , corresponding to the set of slopes  $\mathbf{s}$ . As shown in Corollary B.1.3, it does not depend on the data.

Let  $c = 2 \ln(4R/\alpha_2\theta)/(\epsilon N)$

Set  $q_L = 1/2 - b - c$  and  $q_U = 1/2 + b + c$

**else**

$q_L, q_U = \text{ComputeExpMechCITargets}(\mathbf{s}, \epsilon, \alpha, -R, R, \theta)$   
// Algorithm 6.3

$\tilde{L}_\alpha(\mathbf{s}) = \text{DPWide}(\mathbf{s}, \epsilon/2, (q_L, R, \theta)) // \text{Algorithm 3.2}$

$\tilde{U}_\alpha(\mathbf{s}) = \text{DPWide}(\mathbf{s}, \epsilon/2, (q_U, R, \theta))$

**return**  $[\tilde{L}_\alpha(\mathbf{s}) - \theta, \tilde{U}_\alpha(\mathbf{s}) + \theta]$

---

The theorem below describes the validity and width of the DP confidence interval when we use DPWideCIUnion (Alg 6.2) as the DPMedCI algorithm. The proof of the validity relies on the validity of the non-private interval (Lemma 6.1.2), along with the utility of DPWide (Thm. 3.0.3). The proof of the width is similar to the proof of Thm. 4.0.2.

**Theorem 6.3.1** (Validity and width of DPWideTSCIUnion). Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1, and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$ . Let  $S$  be a set of  $N$  unordered datapoints. For  $\alpha \in (0, 1), r_\alpha \in (0, 1), \epsilon, R, \theta > 0$ , and  $\beta_1 \in [-R + \theta, R - \theta]$  as in Assumption 3.0.2, let  $[\tilde{\beta}_{1L}^{\text{DPWideTS}}, \tilde{\beta}_{1U}^{\text{DPWideTS}}] = \text{DPTSCI}(\{x_i, y_i\}_{i=1}^n, \epsilon, S, \text{DPWideCIUnion}, (\alpha, r_\alpha, \theta, -R, R, \text{Union} = 1))$ . Then, the interval  $[\tilde{\beta}_{1L}^{\text{DPWideTS}}, \tilde{\beta}_{1U}^{\text{DPWideTS}}]$  is a  $1 - \alpha$ -confidence interval for the true slope  $\beta_1$  over the randomness in  $(x_i, y_i)_{i=1}^n$  and DPWideTSCIUnion.

In addition, let  $U_z$  be defined as in Definition 4.0.1, Equation (2) according to set  $S$ . Then, there exists a constant  $v > 0$  such that for sufficiently large  $n$ , we have that with probability at least  $1 - \alpha$ ,

$$\tilde{\beta}_{1U}^{\text{DPWideTS}} - \tilde{\beta}_{1L}^{\text{DPWideTS}} < 2z + 2\theta \text{ for all } z \text{ that satisfies the following.}$$

$$\frac{-\mu(z) - \frac{8 \ln(2R/\alpha\theta)}{\epsilon \cdot n}}{\sigma(z)} \geq 2 \cdot \Phi^{-1} \left( 1 - \frac{\alpha}{2} + \frac{v}{n^2 \cdot \sigma^3(z)} \right)$$

where  $\mu(z) = \mathbb{E}[U_z]$ ,  $\sigma^2(z) = \text{Var}[U(z)]$ , and  $\Phi$  is the standard normal cdf.

**PROOF.** First, let us prove the validity of the confidence interval  $[\tilde{\beta}_{1L}^{\text{DPWideTS}}, \tilde{\beta}_{1U}^{\text{DPWideTS}}]$ . We consider the upper limit of the interval,  $\tilde{\beta}_{1U}^{\text{DPWideTS}}$ , for simplicity. First, we will bound the probability that the upper limit of the private interval fails ( $\tilde{\beta}_{1U}^{\text{DPWideTS}} < \beta_1$ ) conditioned on the success of the upper limit of the non-private

interval  $(\beta_1 < \hat{\beta}_{1U})$ . This analysis uses a translation between the  $U$ -statistic and the distribution function  $F_s$ , as well as the utility of the exponential mechanism (Theorem 3.0.3) with target quantile  $q_U = 1/2 + b + c$ .

$$\begin{aligned} & \Pr_{d, \text{DPWideCI}} \left( \tilde{\beta}_{1U}^{\text{DPWideTS}} < \beta_1 \wedge \beta_1 \leq \hat{\beta}_{1U} \right) \\ & \leq \mathbb{E}_d \left[ \Pr_{\text{DPWideCI}} \left( \tilde{\beta}_{1U}^{\text{DPWideTS}} < \hat{\beta}_{1U} \mid \mathbf{d} \right) \right] \\ & \leq \mathbb{E}_d \left[ \Pr_{\text{DPWideCI}} \left( U(\tilde{\beta}_{1U}^{\text{DPWideTS}}) > U(\hat{\beta}_{1U}) \mid \mathbf{d} \right) \right] \\ & = \mathbb{E}_d \left[ \Pr_{\text{DPWideCI}} \left( 1 - 2F_s(\tilde{\beta}_{1U}^{\text{DPWideTS}}) > -2b \mid \mathbf{d} \right) \right] \\ & = \mathbb{E}_d \left[ \Pr_{\text{DPWideCI}} \left( F_s(\tilde{\beta}_{1U}^{\text{DPWideTS}}) < 1/2 + b \mid \mathbf{d} \right) \right] \\ & = \mathbb{E}_d \left[ \Pr_{\text{DPWideCI}} \left( F_s(\tilde{\beta}_{1U}^{\text{DPWideTS}}) - q_U < -c \mid \mathbf{d} \right) \right] \\ & \leq \mathbb{E}_d [\alpha_2/2] \\ & = \alpha_2/2 \end{aligned}$$

We use this bound to evaluate the total failure probability of the private upper limit. We also use the failure probability of the upper limit of the *non-private* confidence interval,  $\hat{\beta}_{1U}$ , as characterized in Lemma 6.1.2.

$$\begin{aligned} & \Pr_{d, \text{DPWideCI}} \left[ \tilde{\beta}_{1U}^{\text{DPWideTS}} < \beta_1 \right] \\ & = \Pr_{d, \text{DPWideCI}} \left[ \tilde{\beta}_{1U}^{\text{DPWideTS}} < \beta_1 \wedge \beta_1 > \hat{\beta}_{1U} \right] + \\ & \quad \Pr_{d, \text{DPWideCI}} \left[ \tilde{\beta}_{1U}^{\text{DPWideTS}} < \beta_1 \wedge \beta_1 \leq \hat{\beta}_{1U} \right] \\ & \leq \Pr_d \left[ \beta_1 > \hat{\beta}_{1U} \right] + \Pr_{\text{DPWideCI}} \left[ \tilde{\beta}_{1U}^{\text{DPWideTS}} < \hat{\beta}_{1U} \right] \\ & \leq \alpha_1/2 + \alpha_2/2 \\ & = \alpha/2 \end{aligned}$$

The same analysis holds for the other end of the interval, so this proves the validity of the confidence interval. Next, let us consider the width of the interval. For simplicity, let us consider the event that  $\tilde{\beta}_{1U}^{\text{DPWideTS}} > \beta_1 + z + \theta$ . The analysis is similar to the proof of Theorem 4.0.2. For all  $z \in \mathbb{R}$  and sufficiently large  $n$ , we have that

$$\begin{aligned} & \Pr_{Y, \text{DPWideCI}} \left[ \tilde{\beta}_{1U}^{\text{DPWideTS}} > \beta_1 + z + \theta \right] \\ & \leq \Pr_{Y, \text{DPWideCI}} \left[ U(\tilde{\beta}_{1U}^{\text{DPWideTS}}) - \theta < -d \right] + \\ & \quad \Pr_Y \left[ U(\tilde{\beta}_{1U}^{\text{DPWideTS}}) - \theta \geq -d \wedge \tilde{\beta}_{1U}^{\text{DPWideTS}} - \theta > \beta_1 + z \right] \\ & \leq \Pr_{Y, \text{DPWideCI}} \left[ U(\tilde{\beta}_{1U}^{\text{DPWideTS}}) < -d \right] + \Pr_Y \left[ U(\beta_1 + z) \geq -d \right] \\ & \leq \Pr_{Y, \text{DPWideCI}} \left[ F_s(\tilde{\beta}_{1U}^{\text{DPWideTS}}) - q_U > d/2 - b - c \right] + \\ & \quad \Pr_Y \left[ U(\beta_1 + z) \geq -d \right] \\ & \leq \frac{R}{2\theta} \exp(-\varepsilon \cdot (d/2 - b - c) \cdot N/2) + \\ & \quad \left( 1 - \Phi \left( \frac{-d - \mu(z)}{\sigma(z)} \right) \right) + O \left( \frac{1}{n^2 \cdot \sigma^3(z)} \right) \end{aligned}$$

where  $b, c$  are defined as in Algorithm 6.2. The first term in the last line follows from Theorem 3.0.3 and the second term follows from Lemma 4.2.1. Setting this probability to  $\leq \alpha$  and solving for  $d$  and  $z$  gives us the desired result. We can run through a similar analysis for the event that  $\tilde{\beta}_{1L}^{\text{DPWideTS}} < \beta_1 - z - \theta$ .  $\square$

The width of the DPWideTSCUnion confidence interval is approximately twice the size of the convergence bound of the point estimator (Thm. 4.0.2), which we expect even in the non-private setting. However, there is an additional factor of 4 in the term corresponding to privacy noise  $(\ln(2R/\alpha\theta))$ . This can be improved using a more nuanced coverage analysis, as we will explore in the next section.

### 6.4 Tighter Confidence Interval

To improve the width of the confidence interval, we apply the more sophisticated approach from Drechsler et al. [27]. In particular, we call DPWideCI with the Union flag set to 0, so that  $q_L, q_U$  are computed using ComputeExpMechCITargets (Alg. 6.3).

---

#### Algorithm 6.3: ComputeExpMechCITargets

---

**Data:**  $\mathbf{s} = (s_1, \dots, s_N)$   
**Input:**  $\varepsilon \in \mathbb{R}_{>0}, \alpha \in (0, 1), [-R, R] \subset \mathbb{R}, \theta \in \mathbb{R}_{>0}$   
**for**  $t_L \in \mathbb{N}, 1 \leq t_L \leq N/2$  **do**  
     $Y_{t_L} = 1 - F_U(1 - 2(t_L - 1)/N) +$   
     $\sum_{m=t_L}^n F'_U(1 - 2m/N) \cdot \frac{R}{\theta} \exp(-(m - t_L) \cdot \varepsilon/2)$   
    //  $F_U, F'_U$  are the CDF and PDF of the null  
    U-statistic corresponding to  $\mathbf{s}$   
     $q_L = \max_{t_L \in \mathbb{N}, 1 \leq t_L \leq \lceil N/2 \rceil} \{t_L : Y_{t_L} \leq \alpha/2\}/N$   
**for**  $t_U \in \mathbb{N}, N/2 \leq t_U < N$  **do**  
     $Y_{t_U} = F_U(1 - 2t_U/N) + \sum_{m=1}^{t_U} F'_U(1 - 2m/N) \cdot$   
     $\frac{R}{\theta} \exp(-(t_U - m) \cdot \varepsilon/2)$   
     $q_U = \min_{t_U \in \mathbb{N}, \lceil N/2 \rceil \leq t_U < N} \{j : Y_{t_U} \leq \alpha/2\}/N$   
**return**  $q_L, q_U$

---

We offer a brief overview of the algorithm here: For a given  $t_L, t_U \in [N], \varepsilon \in \mathbb{R}_{>0}$ , let  $\tilde{L}_\alpha(\mathbf{s}, t_L) = \text{DPWide}(\mathbf{s}, \varepsilon/2, (t_L/N, \theta, -R, R))$  and  $\tilde{U}_\alpha(\mathbf{s}, t_U) = \text{DPWide}(\mathbf{s}, \varepsilon/2k, (t_U/N, \theta, -R, R))$ . As before, the goal is to control the probability that the interval  $[\tilde{L}_\alpha(\mathbf{s}, t_L) - \theta, \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta]$  fails to contain the true slope  $\beta_1$ . In particular, for  $\alpha \in (0, 1)$ , we would like to find the target ranks  $t_L$  and  $t_U$  closest to  $N/2$  such that

$$\begin{aligned} & \Pr_{\mathbf{s}, \text{DPWideCI}} \left[ \tilde{L}_\alpha(\mathbf{s}, t_L) - \theta > \beta_1 \right] \leq \alpha/2, \text{ and} \\ & \Pr_{\mathbf{s}, \text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \right] \leq \alpha/2 \end{aligned} \quad (5)$$

In Algorithm 6.3, we find these target ranks by first computing the probabilities above for all possible  $t_L$  and  $t_U$ 's, and then by numerically searching for the target ranks closest to  $N/2$  such that the probabilities above are both within  $\alpha/2$ . This search can be implemented more efficiently by noting that  $t_L$  is greater than or equal to  $N \cdot (1/2 - b - c)$  as defined in Algorithm 6.2, and similarly  $t_U$  is less than or equal to  $N \cdot (1/2 + b + c)$ .

As the outputs  $q_L, q_U$  of ComputeExpMechCITargets are  $\geq 1/2 - b - c$  and  $\leq 1/2 + b + c$ , where  $b, c$  are defined in DPWideCIUnion

algorithm, the width of the interval will always be less than or equal to that of the DPWideTSCUnion interval (Thm. 6.3.1).

**Theorem 6.4.1.** *Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1, and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$ . Let  $S$  be a set of unordered pairs of datapoints. For  $\alpha \in (0, 1)$ ,  $r_\alpha = 1/2$  (as a default, since it won't be used),  $\varepsilon, R, \theta > 0$ , and  $\beta_1 \in [-R + \theta, R - \theta]$  as in Assumption 3.0.2, let  $[\tilde{\beta}_{1L}^{\text{DPWideTS}}, \tilde{\beta}_{1U}^{\text{DPWideTS}}] = \text{DPTSCI}(\{x_i, y_i\}_{i=1}^n, \varepsilon, S, \text{DPWideCI}, (\alpha, r_\alpha, \theta, -R, R, \text{Union} = 0))$ . Then, the interval  $[\tilde{\beta}_{1L}^{\text{DPWideTS}}, \tilde{\beta}_{1U}^{\text{DPWideTS}}]$  is a  $1 - \alpha$ -confidence interval for the true slope  $\beta_1$  over the randomness in  $(x_i, y_i)_{i=1}^n$  and DPWideTSCI.*

The validity analysis for Alg. 6.3 (proof of Theorem 6.4.1) relies on characterizing the distribution of the rank of the population median in the dataset. Drechsler et al. used the fact that for i.i.d. data, the rank of the population median in the dataset follows a binomial distribution. In our setting, where the slopes  $\mathbf{s}$  computed by DPTSCI are not necessarily i.i.d, we instead characterize the rank of the population median (ie. the true slope  $\beta_1$ ) via the distribution of the corresponding U-statistic (Thm. 4.2.1).

To analyze this algorithm, we will first state a lemma that translates between the empirical distribution  $F_s$  to the distribution of the null U-statistic,  $F_U$ .

**Lemma 6.4.2.** *Let  $\mathbf{s} = (s_1, \dots, s_N) \in \mathbb{R}^N$  be a multiset of (not necessarily independent) slopes computed via the DPTSCI algorithm, where each  $s_j$  is drawn from a marginal distribution function that has true median  $\beta_1$ . Let  $F_s$  be the empirical distribution of the slopes, let  $U_0$  be the corresponding U-statistic (as defined in (3)), and let  $F_U, F'_U$  be the cdf and pdf, respectively, of  $U_0(\beta_1, (x_i, y_i)_{i=1}^n)$ . Then, for any  $m \in [N]$ ,*

$$\Pr \left[ F_s(\beta_1) = \frac{m}{N} \right] = F'_U \left( 1 - \frac{2m}{N} \right)$$

$$\Pr \left[ F_s(\beta_1) \leq \frac{m}{N} \right] = 1 - F_U \left( 1 - \frac{2m}{N} \right).$$

**PROOF.** We can rewrite  $F_s(\beta_1)$  as  $1/2 - U_0(\beta_1)/2$ , which directly gives that

$$\Pr \left[ F_s(\beta_1) = \frac{m}{N} \right] = \Pr \left[ U_0(\beta_1) = 1 - \frac{2m}{N} \right]$$

$$\Pr \left[ F_s(\beta_1) \leq \frac{m}{N} \right] = \Pr \left[ U_0(\beta_1) \geq 1 - \frac{2m}{N} \right].$$

□

Using the above lemma, we show the validity of the DPWideTSCI using ComputeExpMechCITargets.

**PROOF.** For simplicity, consider the upper endpoint of the interval. Recall that for a given  $t_U \in [N]$ ,  $\tilde{U}_\alpha(\mathbf{s}, t_U) = \text{DPWide}(\mathbf{s}, \varepsilon/2k, (t_U/N, \theta, -R, R))$ , and  $F_s$  is the empirical distribution of the set of slopes  $\mathbf{s}$ . We will consider the probability that  $\tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1$  by splitting this event into two cases: first, when  $F_s(\beta_1) \leq t_U/N$ , and second, when  $F_s(\beta_1) > t_U/N$ .

$$\Pr_{\mathbf{s}, \text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \right]$$

$$= \sum_{m=1}^{t_U} \Pr_{\text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \mid F_s(\beta_1) = \frac{m}{N} \right]$$

$$\cdot \Pr_{\mathbf{s}} \left[ F_s(\beta_1) = \frac{m}{N} \right]$$

$$+ \sum_{m=t_U+1}^N \Pr_{\text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \mid F_s(\beta_1) = \frac{m}{N} \right]$$

$$\cdot \Pr_{\mathbf{s}} \left[ F_s(\beta_1) = \frac{m}{N} \right]$$

We can simplify the first sum using Lemma 6.4.2 and the utility of the widened exponential mechanism, Theorem 3.0.3:

$$\sum_{m=1}^{m=t_U} \Pr_{\text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \mid F_s(\beta_1) = \frac{m}{N} \right]$$

$$\cdot \Pr_{\mathbf{s}} [F_s(\beta_1) = m/N]$$

$$\leq \sum_{m=1}^{m=t_U} \Pr_{\text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) < \beta_1 \mid F_s(\beta_1) = \frac{m}{N} \right]$$

$$\cdot \Pr_{\mathbf{s}} [F_s(\beta_1) = m/N]$$

$$= \sum_{m=1}^{m=t_U} \Pr_{\text{DPWideCI}} \left[ F_s(\tilde{U}_\alpha(\mathbf{s}, t_U)) < m/N \right] \cdot F'_U \left( 1 - \frac{2m}{N} \right)$$

$$\leq \sum_{m=1}^{m=t_U} \Pr_{\text{DPWideCI}} \left[ \frac{t_U}{N} - F_s(\tilde{U}_\alpha(\mathbf{s}, t_U)) > \frac{t_U - m}{N} \right] \cdot F'_U \left( 1 - \frac{2m}{N} \right)$$

$$\leq \sum_{m=1}^{m=t_U} \frac{R}{\theta} \exp(-(t_U - m) \cdot \varepsilon/2) \cdot F'_U \left( 1 - \frac{2m}{N} \right)$$

For the second sum, we simply upper bound the first probability in the summation by 1 and use Lemma 6.4.2 to characterize the distribution of  $\mathbb{1}_{F_s(\beta_1)=m/N}$ .

$$\sum_{m=t_U+1}^{m=N} \Pr_{\text{DPWideCI}} \left[ \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \mid F_s(\beta_1) = \frac{m}{N} \right]$$

$$\cdot \Pr_{\mathbf{s}} \left[ F_s(\beta_1) = \frac{m}{N} \right]$$

$$\leq \sum_{m=t_U+1}^{m=N} \Pr_{\mathbf{s}} \left[ F_s(\beta_1) = \frac{m}{N} \right]$$

$$\leq F_U \left( 1 - \frac{2 \cdot t_U}{N} \right)$$

Therefore, we have that

$$\Pr_{\mathbf{s}, \text{DPWideCI}} \left( \tilde{U}_\alpha(\mathbf{s}, t_U) + \theta < \beta_1 \right)$$

$$\leq F_U \left( 1 - \frac{2 \cdot t_U}{N} \right) + \sum_{m=1}^{t_U} F'_U \left( 1 - \frac{2m}{N} \right) \cdot \frac{R}{\theta} \exp(-(t_U - m) \cdot \varepsilon/2)$$

A similar result holds for the other side of the interval. Then, validity of the interval follows directly from the selection of the target quantiles  $t_L, t_U$  (via ComputeExpMechCITargets) such that the interval has at least  $1 - \alpha$  coverage. □

## 7 Conclusion

In this work, we aimed to advance the usability of DP for a fundamental statistical task: simple linear regression. Our work provides

a deeper theoretical understanding of the privacy and accuracy guarantees of the DPTheilSen algorithms, which were found by Alabi et al. [2] to have strong empirical performance in practical (e.g. small dataset, high privacy) regimes. We provide finite-sample convergence bounds, offer insight into hyperparameter selection, and show how to produce differentially private confidence intervals, all under minimal assumptions.

This work’s focus on the one-dimensional setting is an intentional choice. Prior work demonstrated how computer science research has overlooked the importance of focusing on one-dimensional linear regression, and how existing solutions in higher-dimensions do not adequately translate to the one-dimensional setting [2]. Our work shows that though it may seem simple, analyzing the full suite of DPTheilSen algorithms in the one-dimensional setting is itself challenging and requires tailored analyses. Nevertheless, we hope our results serve as a stepping stone for future work that analyzes the optimality of these algorithms and extends the confidence intervals to multivariate settings.

By studying the DPTheilSen family of algorithms, this work provides usable theory for one of the most commonly used robust estimators, which is one of the most accurate algorithms for practical regimes in the private setting. We hope these results enhance the usability of DP estimators for linear regression and advance our theoretical toolkit for understanding robust, private regression.

## Acknowledgments

We thank Daniel Alabi, Audra McMillan, and Adam Smith for discussions that motivated this work. We also thank Cynthia Dwork and James Honaker for helpful conversations at an early stage of this work, and Ryan Cumings-Menon and others at the Fields Institute Privacy Workshop in Summer 2022 for helpful comparisons with related work on robust regression.

JS did much of this work at Harvard University and Columbia University, where she was supported by the Columbia Data Science Institute Fellowship. SV was supported by a Simons Investigator Award. Both authors were supported by Cooperative Agreement CB20ADR0160001 with the Census Bureau. The views expressed in this paper are those of the authors and not those of the U.S. Census Bureau or any other sponsor.

## References

[1] John M Abowd. 2018. The US Census Bureau adopts differential privacy. In *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*. 2867–2867.

[2] Daniel Alabi, Audra McMillan, Jayshree Sarathy, Adam Smith, and Salil Vadhan. 2022. Differentially Private Simple Linear Regression. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 184–204.

[3] Daniel Gbenga Alabi. 2022. *The Algorithmic Foundations of Private Computational Social Science*. Ph. D. Dissertation. Harvard University.

[4] Micah Altman, Alexandra Wood, David R O’Brien, and Urs Gasser. 2018. Practical approaches to big data privacy over time. *International Data Privacy Law* 8, 1 (2018), 29–51.

[5] Kareem Amin, Matthew Joseph, Mónica Ribero, and Sergei Vassilvitskii. 2023. Easy Differentially Private Linear Regression. In *The Eleventh International Conference on Learning Representations*.

[6] Hilal Asi, Jonathan Ullman, and Lydia Zakynthinou. 2023. From robustness to privacy and back. *arXiv preprint arXiv:2302.01855* (2023).

[7] Marco Avella-Medina. 2021. Privacy-preserving parametric inference: a case for robust statistics. *J. Amer. Statist. Assoc.* 116, 534 (2021), 969–983.

[8] Jordan Awan and Aleksandra Slavković. 2018. Differentially private uniformly most powerful tests for binomial data. *Advances in Neural Information Processing Systems* 31 (2018).

[9] Andrés F. Barrientos, J. Reiter, Ashwin Machanavajhala, and Yan Chen. 2017. Differentially Private Significance Tests for Regression Coefficients. *Journal of Computational and Graphical Statistics* 28 (2017), 440 – 453.

[10] Andrés F Barrientos, Aaron R Williams, Joshua Snoke, and Claire McKay Bowen. 2021. A Feasibility Study of Differentially Private Summary Statistics and Regression Analyses for Administrative Tax Data. *arXiv preprint arXiv:2110.12055* (2021).

[11] Raef Bassily, Adam Smith, and Abhradeep Thakurta. 2014. Private empirical risk minimization: Efficient algorithms and tight error bounds. In *2014 IEEE 55th annual symposium on foundations of computer science*. IEEE, 464–473.

[12] James Bennett, Stan Lanning, et al. 2007. The netflix prize. In *Proceedings of KDD cup and workshop*, Vol. 2007. New York, NY, USA., 35.

[13] Garrett Bernstein and Daniel R Sheldon. 2018. Differentially Private Bayesian Inference for Exponential Families. In *Advances in Neural Information Processing Systems*, S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett (Eds.), Vol. 31. Curran Associates, Inc. <https://proceedings.neurips.cc/paper/2018/file/08040837089cdf46631a10aca5258e16-Paper.pdf>

[14] Andrew C Berry. 1941. The accuracy of the Gaussian approximation to the sum of independent variates. *Transactions of the american mathematical society* 49, 1 (1941), 122–136.

[15] Joseph R Biden. 2023. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence. (2023).

[16] Thomas W. Brawner and J. Honaker. 2018. Bootstrap Inference and Differential Privacy: Standard Errors for Free.

[17] Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, and Lydia Zakynthinou. 2021. Covariance-aware private mean estimation without private covariance estimation. *Advances in Neural Information Processing Systems* 34 (2021), 7950–7964.

[18] T. Tony Cai, Yichen Wang, and Linjun Zhang. 2019. The Cost of Privacy: Optimal Rates of Convergence for Parameter Estimation with Differential Privacy. *CoRR* abs/1902.04495 (2019). <http://arxiv.org/abs/1902.04495>

[19] Silvia Casacuberta, Michael Shoemate, Salil Vadhan, and Connor Wagaman. 2022. Widespread Underestimation of Sensitivity in Differentially Private Libraries and How to Fix It. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 471–484.

[20] Louis HY Chen, Larry Goldstein, and Qi-Man Shao. 2011. *Normal approximation by Stein’s method*. Vol. 2. Springer.

[21] Raj Chetty and John N. Friedman. 2019. A Practical Method to Reduce Privacy Loss When Disclosing Statistics Based on Small Samples. *American Economic Review Papers and Proceedings* 109 (2019), 414–420.

[22] Raj Chetty, John N Friedman, Nathaniel Hendren, Maggie R Jones, and Sonya R Porter. 2018. *The opportunity atlas: Mapping the childhood roots of social mobility*. Technical Report. National Bureau of Economic Research.

[23] Simon Couch, Zeki Kazan, Kaiyan Shi, Andrew Bray, and Adam Groce. 2019. Differentially Private Nonparametric Hypothesis Testing. *arXiv preprint arXiv:1903.09364* (2019).

[24] Ryan Cumings-Menon. 2022. Differentially Private Estimation via Statistical Depth. *arXiv preprint arXiv:2207.12602* (2022).

[25] Irit Dinur and Kobbi Nissim. 2003. Revealing information while preserving privacy. In *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*. 202–210.

[26] Vito D’Orazio, J. Honaker, and G. King. 2015. Differential Privacy for Social Science Inference. *Alfred P. Sloan Foundation Economic Research Paper Series* (2015).

[27] Joerg Drechsler, Ira Globus-Harris, Audra McMillan, Jayshree Sarathy, and Adam Smith. 2022. Non-parametric differentially private confidence intervals for the median. *Journal of Survey Statistics and Methodology* 10 (2022), 804–829. Issue 3.

[28] Wenxin Du, Canyon Foot, Monica Moniot, Andrew Bray, and Adam Groce. 2020. Differentially Private Confidence Intervals. *arXiv arXiv:2001.02285* (2020).

[29] Cynthia Dwork. 2006. Differential Privacy. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II*. 1–12.

[30] Cynthia Dwork and Jing Lei. 2009. Differential privacy and robust statistics.. In *STOC*, Vol. 9. 371–380.

[31] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam D. Smith. 2006. Calibrating Noise to Sensitivity in Private Data Analysis. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*. 265–284.

[32] Cynthia Dwork, Kunal Talwar, Abhradeep Thakurta, and Li Zhang. 2014. Analyze gauss: optimal bounds for privacy-preserving principal component analysis. In *Symposium on the Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*. 11–20.

[33] Abdel H El-Shaarawi and Walter W Piegorsch. 2002. *Encyclopedia of environmental metrics*. Vol. 1. John Wiley & Sons.

[34] Carl-Gustav Esseen. 1942. On the Liapunov limit error in the theory of probability. *Ark. Mat. Astr. Fys.* 28 (1942), 1–19.

[35] Georgina Evans and Gary King. 2021. Statistically Valid Inferences from Differentially Private Data Releases, with Application to the Facebook URLs Dataset.

- Political Analysis* (2021–2021).
- [36] C. Ferrando, Shu-Fan Wang, and D. Sheldon. 2020. General-Purpose Differentially-Private Confidence Intervals. *ArXiv abs/2006.07749* (2020).
- [37] Marco Gaboardi, Ryan Rogers, and Or Sheffet. 2019. Locally Private Mean Estimation: Z-test and Tight Confidence Intervals. In *Proceedings of Machine Learning Research (Proceedings of Machine Learning Research, Vol. 89)*, Kamalika Chaudhuri and Masashi Sugiyama (Eds.). PMLR, 2545–2554.
- [38] Gonzalo M Garrido, Xiaoyuan Liu, Florian Matthes, and Dawn Song. 2023. Lessons Learned: Surveying the Practicality of Differential Privacy in the Industry. *Proceedings on Privacy Enhancing Technologies 2* (2023), 151–170.
- [39] Wassily Hoeffding. 1948. A class of statistics with asymptotically normal distribution. *Annals of Mathematical Statistics* 19 (1948), 293–325.
- [40] Samuel B Hopkins, Gautam Kamath, Mahbod Majid, and Shyam Narayanan. 2023. Robustness implies privacy in statistical estimation. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, 497–506.
- [41] V. Karwa and S. Vadhan. 2018. Finite Sample Differentially Private Confidence Intervals. In *ITCS*.
- [42] Maurice George Kendall. 1948. Rank correlation methods. (1948).
- [43] Alexander Knop and Thomas Steinke. 2022. Differentially Private Linear Regression via Medians. (2022).
- [44] Xiyang Liu, Prateek Jain, Weihao Kong, Sewoong Oh, and Arun Suggala. 2023. Label Robust and Differentially Private Linear Regression: Computational and Statistical Efficiency. In *Thirty-seventh Conference on Neural Information Processing Systems*.
- [45] Xiyang Liu, Weihao Kong, and Sewoong Oh. 2022. Differential privacy and robust statistics in high dimensions. In *Conference on Learning Theory*. PMLR, 1167–1246.
- [46] Frank McSherry and Kunal Talwar. 2007. Mechanism Design via Differential Privacy. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20–23, 2007, Providence, RI, USA, Proceedings*, 94–103.
- [47] Kelly Ramsay and Shoja’eddin Chenouri. 2021. Differentially private depth functions and their associated medians. *arXiv preprint arXiv:2101.02800* (2021).
- [48] Jayshree Sarathy, Sophia Song, Audrey Haque, Tania Schlatter, and Salil Vadhan. 2023. Don’t look at the data! how differential privacy reconfigures the practices of data science. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–19.
- [49] Pranab Kumar Sen. 1968. Estimates of the regression coefficient based on Kendall’s tau. *Journal of the American statistical association* 63, 324 (1968), 1379–1389.
- [50] Or Sheffet. 2017. Differentially Private Ordinary Least Squares. In *Proceedings of the 34th International Conference on Machine Learning, ICML 2017, Sydney, NSW, Australia, 6–11 August 2017*, 3105–3114. <http://proceedings.mlr.press/v70/sheffet17a.html>
- [51] Adam Smith. 2011. Privacy-preserving statistical estimation with optimal convergence rates. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, 813–822.
- [52] Henri Theil. 1950. A rank-invariant method of linear and polynomial regression analysis, 3; confidence regions for the parameters of polynomial regression equations. *Indagationes Mathematicae* 1, 2 (1950), 467–482.
- [53] Yu-Xiang Wang. 2018. Revisiting differentially private linear regression: optimal and adaptive prediction & estimation in unbounded domain. In *Proceedings of the Thirty-Fourth Conference on Uncertainty in Artificial Intelligence, UAI 2018, Monterey, California, USA, August 6–10, 2018*, 93–103.
- [54] Jun Zhang, Zhenjie Zhang, Xiaokui Xiao, Yin Yang, and Marianne Winslett. 2012. Functional Mechanism: Regression Analysis under Differential Privacy. *Proc. VLDB Endow.* 5, 11 (2012), 1364–1375.

## A Widened Exponential Mechanism (DPWide)

In this section, we provide more background on the *widened exponential mechanism* for quantile estimation designed by [2], which is a variant of the standard exponential mechanism [46] described below.

**Definition A.0.1** (Exponential Mechanism [46]). The exponential mechanism is defined with respect to a utility function  $u$ , which maps (data set, output) pairs to real values. Given dataset  $\mathbf{s}$  and range of possible outputs,  $[-R, R]$ , the exponential mechanism outputs  $r \in [-R, R]$  with probability density proportional to  $\exp\left(\frac{\varepsilon u(\mathbf{s}, r)}{2\Delta u}\right)$ , where  $\Delta(u) = \sup_{r \in [-R, R]} \sup_{\mathbf{s}, \mathbf{s}' } |u(\mathbf{s}, r) - u(\mathbf{s}', r)|$ . The exponential mechanism is  $\varepsilon$ -DP.

The standard instantiation of the exponential mechanism for quantile estimation (used, e.g., in [51]) uses a utility function that assigns a score to output  $r$  based on how far  $r$  is *in rank* from the desired quantile of  $\mathbf{s}$ . For all outputs  $r$  within the range  $[-R, R]$ , and for a target quantile  $q \in (0, 1)$ , the standard utility function is:

$$u(\mathbf{s}, r) = -\lfloor \#\text{below } r - n \cdot q \rfloor$$

where  $\#\text{below } r$  denotes the number of datapoints in  $\mathbf{s}$  that are less than or equal to  $r$  in value. Note that this utility function assigns the same utility score to every output  $r$  in the interval between two data points.

One issue with this mechanism is that when the output space is the real line and the data is highly concentrated, the mechanism may not place enough probability density near the target quantile. To mitigate this issue, [2] design a variation on the standard utility function. For widening parameter  $\theta > 0$ , and target quantile  $q \in (0, 1)$ , the widened utility function is:

$$u(\mathbf{s}, r) = -\lfloor \min_{w \in [r-\theta, r+\theta]} \#\text{below } w - n \cdot q \rfloor$$

This utility function provides a lower bound on the probability density the mechanism assigns around the target quantile.

Below, we prove the standard utility theorem for DPWide with widening hyperparameter  $\theta$  on a fixed dataset  $\mathbf{s}$ .

**PROOF OF THEOREM 3.0.3.** Let  $F_{\mathbf{s}}$  be the empirical distribution function for  $\mathbf{s}$ , and let  $F_{\mathbf{s}}^{-1}$  be the inverse empirical distribution function. The utility score of an output  $r \in [-R, R]$  is  $-\lfloor \min_{w \in [r-\theta, r+\theta]} N \cdot |F_{\mathbf{s}}(w) - q| \rfloor$ . Let  $r^* \in [\max(-R, r - \theta), \min(R, r + \theta)]$  be the value that maximizes the utility function for potential output value  $r$ . Therefore, we can rewrite the utility score of  $r$  as  $-\lfloor N |F_{\mathbf{s}}(r^*) - q| \rfloor$ .

Next, let us upper bound the probability that the mechanism selects an output with score  $\leq -cN$ . The exponential mechanism assigns un-normalized probability density of at most  $\exp(-\varepsilon cN/2)$  to each of these outputs, and they span at most the interval  $[-R, R]$ . On the other hand, the exponential mechanism assigns un-normalized probability density of 1 to output values with score of zero, which we know exist in the range  $[-R, R]$  by Assumption 3.0.2. In particular, all outputs within  $\theta$  of  $F_{\mathbf{s}}^{-1}(q)$  have score of zero. Therefore, we have that

$$\begin{aligned} & \Pr_{\text{DPWide}(\mathbf{s}, \varepsilon, (q, -R, R, \theta))} \left( \tilde{q}^{\text{DPWide}} \notin [F_{\mathbf{s}}^{-1}(q - c), F_{\mathbf{s}}^{-1}(q + c)] \right) \\ &= \Pr_{\text{DPWide}(\mathbf{s}, \varepsilon, (q, -R, R, \theta))} \left( |F_{\mathbf{s}}(\tilde{q}^{\text{DPWide}^*}) - q| \geq c \right) \\ &= \Pr_{\text{DPWide}(\mathbf{s}, \varepsilon, (q, -R, R, \theta))} \left( N |F_{\mathbf{s}}(\tilde{q}^{\text{DPWide}^*}) - F_{\mathbf{s}}(\hat{q})| \geq cN \right) \\ &\leq \frac{2R \exp(-\varepsilon cN/2)}{2\theta \exp(-\varepsilon \cdot 0 \cdot N/2)} \\ &= \frac{R \exp(-\varepsilon cN/2)}{\theta} \end{aligned}$$

Since  $\tilde{q}^{\text{DPWide}}$  is at most  $\theta$  away from  $\tilde{q}^{\text{DPWide}^*}$ , we can expand the interval by  $\theta$  on each side and obtain the desired bound for  $\tilde{q}^{\text{DPWide}}$ .  $\square$

## B Finite-Sample Convergence of U-Statistic

In this section, we develop a finite-sample convergence bound for U-statistics (Definition 4.0.1) that will be a key component towards

proving the finite-sample convergence bound for DPWideTS. The bound is stated in Theorem 4.2.1. To develop this bound, we adapt the convergence bounds for linear statistics of i.i.d. mean-0 random variables [20] to work for U-statistics of independent, *non-identical* random variables.

We begin by analyzing the expectation and variance of the U-statistic in question.

### B.1 Expectation and Variance of U-statistic

Here, we consider the expectation and variance of  $U_z$  (Equation 2) in a very general form. These expressions are not fully evaluated in order to be as general as possible. They can be further characterized (as shown in Section C) based on features of the  $x$  values (number of ties, spacings, etc.) and the paired datapoints that are included within the set  $S$ .

**Lemma B.1.1.** *Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 and have variance  $\sigma_x^2$ , and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$  with variance  $\sigma_e^2$ . Let  $S$  be a set of unordered pairs of datapoints, let  $N = |S|$ , and let  $U_z$  be defined accordingly as in Definition 4.0.1, Equation (2). Let  $F_{diff}$  refer to the CDF of the difference in any two i.i.d. noise variables  $e_j, e_i$ , and let  $\Delta_{ij} = x_j - x_i$ . Then, we have that*

$$E_{e_1, \dots, e_n} [U_z] = \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign}(x_j - x_i) \cdot (1 - 2 \cdot F_{diff}(z \cdot \Delta_{ij}))$$

**PROOF.** Using the definition of  $F_{diff}$ , we can expand the expectation of  $U_z$  as follows.

$$\begin{aligned} E_{e_1, \dots, e_n} [U_z] &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} E_{e_i, e_j} [\text{sign}(x_j - x_i) \cdot \text{sign}(e_j - e_i - z \cdot \Delta_{ij})] \\ &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign}(x_j - x_i) \cdot (1 - 2 \cdot P_{e_j, e_i}(e_j - e_i < z \cdot \Delta_{ij})) \\ &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign}(x_j - x_i) \cdot (1 - 2 \cdot F_{diff}(z \cdot \Delta_{ij})) \end{aligned}$$

□

The next lemma bounds the variance of the U-statistic,  $U_z$ .

**Lemma B.1.2.** *Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 and have variance  $\sigma_x^2$ , and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$  with variance  $\sigma_e^2$ . Let  $S$  be a set of unordered pairs of datapoints, let  $N = |S|$ , and let  $U_z$  be defined accordingly as in Definition 4.0.1, Equation (2). Let  $B_{ij}(z) = \text{sign}(x_j - x_i) \cdot \text{sign}(e_j - e_i - z \cdot (x_j - x_i))$ . Then, we have that*

$$\begin{aligned} &\frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \\ &\leq \text{Var}_{e_1, \dots, e_n} [U_z] \end{aligned}$$

$$\leq \frac{1}{N} + \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z))$$

**PROOF.** We begin by rewriting the variance of  $U_z$  as a sum of covariances. Then, we can split up the sum based on the number of overlaps of datapoints  $i, j, s, t$  where  $\{i, j\}, \{s, t\} \in S$ .

$$\begin{aligned} &\text{Var}_{e_1, \dots, e_n} [U_z] \\ &= \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t}} \text{Cov}(B_{ij}(z) \cdot B_{st}(z)) \\ &= \frac{1}{N^2} \left( \sum_{\{i,j\} \in S, i < j} \text{Var}(B_{ij}(z)) + \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \right. \\ &\quad \left. + \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 0}} \text{Cov}(B_{ij}(z), B_{st}(z)) \right) \\ &\leq \frac{1}{N} + \left( \frac{1}{(N)^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \right) + 0 \end{aligned}$$

The first sum in the second line can be evaluated by noting that  $|S| = N$  and since  $\Pr_{e_i, e_j} [B_{ij} \in \{-1, 1\}] = 1$ ,  $\text{Var}(B_{ij}(z)) \leq 1$ . For the third sum, note that for  $|\{i, j\} \cap \{s, t\}| = 0$ ,  $B_{ij}(z)$  and  $B_{st}(z)$  are independent, so  $\text{Cov}(B_{ij}(z), B_{st}(z)) = 0$ . This leaves the second sum, which can be evaluated based on additional assumptions about the number of ties and spacings between  $x$  values, as in Lemma C.0.3. Note that since  $\text{Var}(B_{ij}(z)) \geq 0$ , we also have that

$$\text{Var}_{e_1, \dots, e_n} [U_z] \geq \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z))$$

which gives the desired result. □

Using Lemma B.1.2, we will evaluate the variance of the null U-statistic,  $U_0$ .

**Corollary B.1.3.** *Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 and have variance  $\sigma_x^2$ , and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution  $F_e$  with variance  $\sigma_e^2$ . Let  $S$  be a set of unordered pairs of datapoints, let  $N = |S|$ , and let  $U_0$  be defined accordingly as in Definition 4.0.1, Equation (3). Then, we have that*

$$\begin{aligned} &\text{Var}_{e_1, \dots, e_n} [U_0] \\ &= \frac{1}{N} + \left( \frac{1}{3 \cdot N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{sign}(x_j - x_i) \cdot \text{sign}(x_t - x_s) \right) \end{aligned}$$

**PROOF.** For any  $\{i, j\} \in S$ ,  $i < j$ , let  $B_{ij}(0) = \text{sign}(x_j - x_i) \cdot \text{sign}(e_j - e_i)$ . First, note that  $\text{Var}[B_{ij}(0)] = 1$  and  $\text{Cov}(B_{ij}(0), B_{st}(0))$

can be expanded as follows.

$$\begin{aligned} & \text{Cov}(B_{ij}(0), B_{st}(0)) \\ &= \mathbb{E}_{e_i, e_j, e_s, e_t} [B_{ij}(0) \cdot B_{st}(0)] - \mathbb{E}_{e_i, e_j} [B_{ij}(0)] \cdot \mathbb{E}_{e_s, e_t} [B_{st}(0)] \\ &= \text{sign}(x_j - x_i) \cdot \text{sign}(x_t - x_s) \cdot \left( \mathbb{E} [\text{sign}(e_j - e_i) \cdot \text{sign}(e_t - e_s)] \right. \\ & \quad \left. - \mathbb{E} [\text{sign}(e_j - e_i)] \cdot \mathbb{E} [\text{sign}(e_t - e_s)] \right) \end{aligned}$$

It can be shown that for all  $\{i, j\} \in S, i < j$  and  $\{s, t\} \in S, s < t$  such that  $|\{i, j\} \cap \{s, t\}| = 1$ , we have that  $\mathbb{E}[\text{sign}(e_j - e_i) \cdot \text{sign}(e_t - e_s)] = 1/3$  [42]. In addition, by the symmetric, mean-0 nature of  $F_e$ , we have that  $\mathbb{E}[\text{sign}(e_j - e_i)] = \mathbb{E}[\text{sign}(e_t - e_s)] = 0$ . Plugging these into the characterization of  $\text{Var}[U_z]$  from Lemma B.1.2 gives the desired result.

$$\begin{aligned} & \text{Var}_{e_1, \dots, e_n} [U_0] \\ &= \frac{1}{N^2} \left( \sum_{\{i, j\} \in S, i < j} \text{Var}(B_{ij}(0)) \right) + \\ & \quad \left( \frac{1}{N^2} \sum_{\substack{\{i, j\} \in S, i < j \\ \{s, t\} \in S, s < t \\ |\{i, j\} \cap \{s, t\}| = 1}} \text{Cov}(B_{ij}(0), B_{st}(0)) \right) \\ &= \frac{1}{N} + \left( \frac{1}{3 \cdot N^2} \sum_{\substack{\{i, j\} \in S, i < j \\ \{s, t\} \in S, s < t \\ |\{i, j\} \cap \{s, t\}| = 1}} \text{sign}(x_j - x_i) \cdot \text{sign}(x_t - x_s) \right) \end{aligned}$$

□

## B.2 Berry-Esseen-type bound for U-statistic

Now, we move onto developing the finite-sample convergence bound for independent, non-identical U-statistics, shown in Theorem 4.2.1. First, we state a standard Berry-Esseen theorem for independent, mean-0, (not necessarily identical) statistics.

**Theorem B.2.1** (Berry-Esseen bound for independent mean-0 r.v.s [14, 34]). *Let  $\zeta_1, \dots, \zeta_n$  be independent random variables with  $\mathbb{E}[\zeta_i] = 0$ ,  $\mathbb{E}[\zeta_i^2] > 0$ , and  $\mathbb{E}[|\zeta_i|^3] = \rho_i^3 < \infty$ , for  $i \in [n]$ . Let  $\sum_{i=1}^n \text{Var}(\zeta_i) = 1$  and  $\rho^3 = \sum_{i=1}^n \rho_i^3$ . Let  $W = \sum_{i=1}^n \zeta_i$  and  $\Phi$  be the standard normal cdf. Then,*

$$\sup_{t \in \mathbb{R}} |\Pr(W \leq t) - \Phi(t)| \leq C \cdot \rho^3$$

where  $C > 0$  is a universal constant.

Now, to prove Theorem 4.2.1, we begin by stating an inequality presented by [20] that bounds the difference between the cumulative distributions of a non-linear function  $T$  and a linear approximation function  $W$ . Note that this inequality, stated below in Lemma B.2.2, does not require i.i.d random variables, but the subsequent theorems in [20] that rely on this bound do require identical marginals.

**Lemma B.2.2** ([20]). *Let  $\zeta_1, \dots, \zeta_n$  be independent random variables satisfying  $\mathbb{E}[\zeta_i] = 0$ ,  $\mathbb{E}[\zeta_i^2] > 0$ , and  $\mathbb{E}[|\zeta_i|^3] < \infty$  for  $i \in [n]$ . Let  $\sum_{i=1}^n \text{Var}(\zeta_i) = 1$ ,  $W = \sum_{i=1}^n \zeta_i$ , and  $T = W + \Delta$  for some  $\Delta :=$*

$\Delta(\zeta_1, \dots, \zeta_n)$ . For each  $i \in [n]$ , let  $\Delta_i$  be a random variable such that  $\zeta_i$  and  $(W - \zeta_i, \Delta_i)$  are independent. Then, for all  $t \in \mathbb{R}$ ,

$$\begin{aligned} & |\Pr(T \leq t) - P(W \leq t)| \leq 2 \sum_{i=1}^n \mathbb{E}[\zeta_i^2] \mathbb{1}_{|\zeta_i| > 1} + \\ & 2 \sum_{i=1}^n \mathbb{E}[|\zeta_i|^3] \mathbb{1}_{|\zeta_i| \leq 1} + \mathbb{E}[|W\Delta|] + \sum_{i=1}^n \mathbb{E}[|\zeta_i(\Delta - \Delta_i)|]. \end{aligned}$$

Using the inequality above in Lemma B.2.2, along with a standard Berry-Esseen theorem (Theorem B.2.1) to replace  $\Pr[W \leq t]$  with  $\Phi(t)$ , Chen et al. [20] develop a Berry-Esseen bound for non-linear statistics of i.i.d. mean-0 random variables. We will adapt this bound for non-identical yet independent, mean-0 random variables to match the setting of our U-statistic,  $U_z$ .

To do so, we first state some definitions that allow us to rewrite  $U_z$  as the sum of a linear approximation function  $W$  and a remainder  $\Delta$ . These include defining the variables  $\Psi_1, \dots, \Psi_n$  and  $\zeta_1, \dots, \zeta_n$ . To help parse the notation in the following lemma, note that each  $\Psi_i$  is conditioned on the corresponding noise variable  $e_i$ , so  $\Psi_1, \dots, \Psi_n$  are independent. In addition, note that the expectation  $\mu_\Psi$  and variance  $\sigma_\Psi$  of the sum of the  $\Psi_i$ 's can be related to the expectation and variance of  $U_z$  (as shown in Lemma B.2.4). The linear approximation function  $W$  is the sum of  $\zeta_i, i \in [n]$ , which are normalized versions of the  $\Psi_i$  random variables.

**Lemma B.2.3.** *Let  $S$  be a set of unordered pairs of datapoints from  $(x_i, y_i)_{i=1}^n$ , where  $|S| = N = nk/2$ . For  $\{i, j\} \in S, i < j$ , let  $a_{ij} = \text{sign}(x_j - x_i)$ ,  $b_{ij} = \text{sign}(e_j - e_i)$ ,  $c_{ij}(z) = \text{sign}(e_j - e_i - z \cdot (x_j - x_i))$ , and  $B'_{ij} = \mathbb{E}_{e'} [\text{sign}(e' - e_i - z \cdot (x_j - x_i)) | e_i]$  where  $e'$  is a fresh draw from the distribution  $F_e$ . Then, for  $i \in [n]$ , let*

$$\Psi_i = \frac{1}{k} \sum_{j: \{i, j\} \in S} a_{ij} \cdot B'_{ij} \text{ and } \zeta_i = \frac{\Psi_i - \mu_i}{\sigma_\Psi \cdot n}$$

where  $\mu_i = \mathbb{E}_{e_1, \dots, e_n} [\Psi_i]$  and  $\sigma_i^2 = \text{Var}_{e_1, \dots, e_n} [\Psi_i]$ . In addition, let  $\mu_\Psi = \sum_{i=1}^n \mu_i/n$  and  $\sigma_\Psi^2 = \sum_{i=1}^n \sigma_i^2/n^2$ . Now, we define the following:

$$\tilde{h}(i, j) = a_{ij} \cdot c_{ij} - \frac{1}{2} \cdot \Psi_i - \frac{1}{2} \cdot \Psi_j$$

$$\Delta = \frac{1}{2 \cdot \sigma_\Psi \cdot N} \sum_{\{i, j\} \in S} \tilde{h}(i, j) \text{ and } \Delta_l = \frac{1}{2 \cdot \sigma_\Psi \cdot N} \sum_{\substack{\{i, j\} \in S \\ i, j \neq l}} \tilde{h}(i, j)$$

Finally, let  $W = \sum_{i=1}^n \zeta_i$ . Then, we claim the following.

- (1)  $\zeta_1, \dots, \zeta_n$  are independent
- (2)  $W + \Delta = (U_z - \mu_\Psi) / (\sigma_\Psi)$
- (3) For each  $l \in [n]$ ,  $\zeta_l$  is independent of  $(W - \zeta_l, \Delta_l)$ .

**PROOF.** First, note that each  $\zeta_i$  conditions on the corresponding noise variable  $e_i$ , and the only randomness in each  $\zeta_i$  is a fresh draw  $e'$  from the distribution  $F_e$ , so  $\zeta_1, \dots, \zeta_n$  are independent.

Next, using the definitions of  $\Psi_i$  and  $\tilde{h}(i, j, z)$ , we can expand  $W + \Delta$  as follows. In particular, note that the  $\Psi_i$  and  $\Psi_j$  variables cancel out, so we are left with sums of  $a_{ij}c_{ij}$  and  $\mu_i$ .

$$\begin{aligned} & W + \Delta \\ &= \sum_{i=1}^n \zeta_i + \frac{1}{\sigma_\Psi \cdot N} \sum_{\{i, j\} \in S} \tilde{h}(i, j) \end{aligned}$$



$$\begin{aligned}
 &= \frac{1}{\sigma_\Psi \cdot n} \sum_{i=1}^n (\Psi_i - \mu_i) + \frac{1}{2 \cdot \sigma_\Psi \cdot N} \sum_{\{i,j\} \in S} \left( a_{ij} c_{ij} - \frac{1}{2} \cdot \Psi_i - \frac{1}{2} \cdot \Psi_j \right) \\
 &= \frac{1}{2 \cdot \sigma_\Psi \cdot N} \sum_{\{i,j\} \in S} a_{ij} c_{ij} - \frac{1}{\sigma_\Psi \cdot n} \sum_{i=1}^n \mu_i \\
 &\quad + \frac{1}{\sigma_\Psi \cdot n} \sum_{i=1}^n \Psi_i - \frac{1}{4 \cdot \sigma_\Psi \cdot N} \sum_{\{i,j\} \in S} (\Psi_i + \Psi_j) \\
 &= \frac{1}{\sigma_\Psi \cdot N} \sum_{\{i,j\} \in S, i < j} a_{ij} c_{ij} - \frac{1}{\sigma_\Psi \cdot n} \sum_{i=1}^n \mu_i \\
 &= \frac{U_z - \mu_\Psi}{\sigma_\Psi}
 \end{aligned}$$

Finally, note that for each  $l \in [n]$ , the random variables  $W - \zeta_l$  and  $\Delta_l$  are functions of  $\zeta_j, j \neq l$ . As  $\zeta_1, \dots, \zeta_n$  are independent of each other, this means that  $\zeta_l$  is independent of  $(W - \zeta_l, \Delta_l)$ .  $\square$

Below, we relate the quantities  $\mu_\Psi$  and  $\sigma_\Psi^2$  to  $\mu(z)$  and  $\sigma^2(z)$ , the expectation and variance of  $U_z$ .

**Lemma B.2.4.** *Let  $S$  be the set of unordered pairs of datapoints from  $(x_i, y_i)_{i=1}^n$ , and let  $N = |S|$ . Let  $\mu_\Psi, \sigma_\Psi$  be defined as in Lemma B.2.2. In addition, let  $U_z$  be defined as in (2), namely  $\mu(z) = \mathbb{E}_{e_1, \dots, e_n} [U_z]$ , and  $\sigma^2(z) = \text{Var}_{e_1, \dots, e_n} [U_z]$ . Then,*

$$\mu_\Psi = \mu(z) \text{ and } \sigma_\Psi^2 = \sigma^2(z) + \Theta(1/N)$$

**PROOF.** First, we show that  $\mu_\Psi(z)$  can be rewritten as  $\mu(z)$ . Let  $B_{ij} = E_{e'} [e_j - e_i - z(x_j - x_i) \mid e_i]$  and  $B'_{ij} = E_{e'} [e' - e_i - z(x_j - x_i) \mid e_i]$ , where  $e'$  is a fresh draw of the random variable  $e$ . Note that as  $e_j$  and  $e'$  are identical random variables, both of which are independent from  $e_i, B_{ij} = B'_{ij}$ . Then, we have that

$$\begin{aligned}
 \mu_\Psi &= \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{e_1, \dots, e_n} [\Psi_i] \\
 &= \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{e_1, \dots, e_n} \left[ \frac{1}{k} \sum_{j: \{i,j\} \in S} a_{ij} \cdot B'_{ij} \right] \\
 &= \frac{2}{nk} \sum_{\{i,j\} \in S, i < j} a_{ij} \cdot B_{ij} \\
 &= \mathbb{E}_{e_1, \dots, e_n} [U_z] \\
 &= \mu(z)
 \end{aligned}$$

Next, for  $\sigma(z)$ , we know from Lemma B.1.2 that

$$\begin{aligned}
 &\frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \\
 &\leq \sigma^2(z) \\
 &\leq \frac{1}{N} + \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}(z), B_{st}(z))
 \end{aligned}$$

In addition, note that  $\text{Cov}(B'_{ij}, B'_{st}) = \text{Cov}(B_{ij}, B_{st})$ . To see this, notice that  $e'$  is identical to  $e_j$ , and both are independent from the other random variables  $e_i, e_s, e_t, e''$ , so  $e', e_j$  are interchangeable in this expression. Similarly,  $e''$  is identical to  $e_t$ , and both are

independent from  $e_i, e_j, e', e_s$ , so  $e''$  and  $e_t$  are interchangeable in this expression.

Then, note that we can rewrite  $\sigma_\Psi$  as follows.

$$\begin{aligned}
 \sigma_\Psi^2 &= \frac{1}{n^2} \sum_{i=1}^n \text{Var}[\Psi_i] \\
 &= \frac{1}{n^2} \sum_{i=1}^n \left( \frac{1}{k^2} \sum_{\substack{j: \{i,j\} \in S \\ t: \{i,t\} \in S}} \text{Cov}(B'_{ij}, B'_{it}) \right) \\
 &= \frac{1}{n^2 k^2} \sum_{i=1}^n \left( \sum_{j: \{i,j\} \in S} \text{Cov}(B'_{ij}, B'_{ij}) + \sum_{\substack{j: \{i,j\} \in S \\ t: \{i,t\} \in S, t \neq j}} \text{Cov}(B'_{ij}, B'_{it}) \right) \\
 &= \frac{2}{n^2 k^2} \sum_{\{i,j\} \in S, i < j} \text{Cov}(B'_{ij}, B'_{ij}) + \frac{4}{n^2 k^2} \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S, s < t \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B'_{ij}, B'_{st}) \\
 &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{Cov}(B'_{ij}, B'_{ij}) + \frac{1}{N^2} \cdot \sum_{\substack{\{i,j\} \in S, i < j \\ \{s,t\} \in S \\ |\{i,j\} \cap \{s,t\}| = 1}} \text{Cov}(B_{ij}, B_{st}) \\
 &= \sigma^2(z) + \Theta\left(\frac{1}{N}\right)
 \end{aligned}$$

As we can see, this gives the desired result.  $\square$

Next, we use bounds for  $\mathbb{E}[\Delta^2]$  and  $\mathbb{E}[(\Delta - \Delta_l)^2]$  shown by Chen et al. [20]. The proof is lengthy so it is omitted here.

**Lemma B.2.5** ([20]). *Let  $\Delta, \Delta_l$  and  $\zeta_l$  (for  $l \in [n]$ ) be defined as in Lemma B.2.3. In addition, for  $U_z$  as defined in (2), let  $\sigma^2(z) = \text{Var}_{e_1, \dots, e_n} [U_z]$ , and let  $\sigma_\Psi^2 = \sum_{l=1}^n \text{Var}[\Psi_l]/n^2$ . Then,*

$$\mathbb{E}[\Delta^2] \leq \frac{\sigma^2(z)}{2(n-1) \cdot \sigma_\Psi^2} \text{ and } \mathbb{E}[(\Delta - \Delta_l)^2] \leq \frac{2\sigma^2(z)}{2n(n-1) \cdot \sigma_\Psi^2}$$

The above lemma allows us to bound the right side of the inequality in Lemma B.2.2.

**Lemma B.2.6.** *Let  $W, \Delta, \Delta_l$ , and  $\zeta_l$  (for  $l \in [n]$ ) be defined as in Lemma B.2.3, where  $\rho^3 = \sum_{l=1}^n \mathbb{E}[|\zeta_l|^3]$ . Let  $\gamma$  be defined as follows.*

$$\begin{aligned}
 \gamma &= C \cdot \rho^3 + 2 \sum_{l=1}^n \mathbb{E}[\zeta_l^2] \mathbb{1}_{|\zeta_l| > 1} + 2 \sum_{l=1}^n \mathbb{E}[|\zeta_l|^3] \mathbb{1}_{|\zeta_l| \leq 1} + \\
 &\quad \mathbb{E}[|W\Delta|] + \sum_{l=1}^n \mathbb{E}[|\zeta_l(\Delta - \Delta_l)|]
 \end{aligned}$$

where  $C > 0$  is a universal constant. In addition, let  $\sigma^2(z) = \text{Var}_{e_1, \dots, e_n} [U_z]$ , where  $U_z$  is defined in (2). Then, for sufficiently large  $n, \gamma = O(1/(n^2 \sigma^3(z)))$ .

**PROOF.** First, note that  $|\Psi_i - \mu_i| \leq 2$  for all  $i \in [n]$ , because this term consists of a product and expectation of signs. Therefore, we have that

$$|\zeta_i| = \left| \frac{\Psi_i - \mu_i}{2 \cdot \sigma_\Psi \cdot n} \right| \leq \frac{1}{\sigma_\Psi \cdot n}, \quad \rho^3 = \sum_{i=1}^n \mathbb{E}[|\zeta_i|^3] \leq \frac{1}{\sigma_\Psi^3 \cdot n^2}$$

Note that  $\sigma_\Psi = \Theta(1/\sqrt{n})$ , so  $\zeta_i = \Theta(1/\sqrt{n})$ . Thus, for sufficiently large  $n$ , we have that

$$\sum_{i=1}^n \mathbb{E}[\zeta_i^2] \cdot \mathbb{1}_{|\zeta_i| > 1} + 2 \sum_{i=1}^n \mathbb{E}[|\zeta_i|^3] \cdot \mathbb{1}_{|\zeta_i| \leq 1} = 0 + \rho^3 \leq \frac{1}{\sigma_\Psi^3 \cdot n^2}$$

Next, note that  $\mathbb{E}[W] = \mathbb{E}[\sum_{i=1}^n \zeta_i] = 0$ . Therefore,

$$\mathbb{E}[W^2] = \text{Var}[W] = \frac{1}{4 \cdot \sigma_\Psi^2 \cdot n^2} \sum_{i \in [n]} \sigma_i^2 = O\left(\frac{n^2 \sigma_\Psi^2}{\sigma_\Psi^2 n^2}\right) = O(1)$$

Using this and the fact from Lemma B.2.5 that  $\mathbb{E}[\Delta^2] = O(\sigma^2(z)/n \cdot \sigma_\Psi^2)$ , we have that

$$\begin{aligned} \mathbb{E}[|W\Delta|] &\leq \mathbb{E}[|W||\Delta|] \\ &\leq \sqrt{\mathbb{E}[|W|^2] \cdot \mathbb{E}[|\Delta|^2]} \\ &= \sqrt{\mathbb{E}[W^2] \cdot \mathbb{E}[\Delta^2]} \\ &= \sqrt{\mathbb{E}[W^2] \cdot \mathbb{E}[\Delta^2]} \\ &= O\left(\frac{\sigma(z)}{\sqrt{n} \cdot \sigma_\Psi}\right) \end{aligned}$$

Similarly, using the fact from Lemma B.2.5 that  $\mathbb{E}[(\Delta - \Delta_l)^2] = O(\sigma^2(z)/n^2 \cdot \sigma_\Psi^2)$ , we have that

$$\begin{aligned} \sum_{l \in [n]} \mathbb{E}[|\zeta_l \cdot (\Delta - \Delta_l)|] &\leq \sum_{l \in [n]} \sqrt{\mathbb{E}[\zeta_l^2] \cdot \mathbb{E}[(\Delta - \Delta_l)^2]} \\ &= \sum_{l \in [n]} \sqrt{\frac{\sigma_l^2}{n^2 \cdot \sigma_\Psi^2} \cdot O\left(\frac{\sigma^2(z)}{n^2 \cdot \sigma_\Psi^2}\right)} \\ &= O\left(\frac{\sigma(z)}{n^2 \cdot \sigma_\Psi^2}\right) \cdot \sum_{l \in [n]} \sigma_l \\ &= O\left(\frac{\sigma(z)}{n^2 \cdot \sigma_\Psi^2}\right) \cdot O(n) \\ &= O\left(\frac{\sigma(z)}{n \cdot \sigma_\Psi^2}\right) \end{aligned}$$

where the second to last line follows from noting that  $\sigma_l \in (0, 1]$ . This gives us that

$$\gamma = O\left(\frac{1}{n^2 \cdot \sigma_\Psi^3}\right) + O\left(\frac{\sigma(z)}{\sqrt{n} \cdot \sigma_\Psi}\right) + O\left(\frac{\sigma(z)}{n \cdot \sigma_\Psi^2}\right) = O\left(\frac{1}{n^2 \cdot \sigma^3(z)}\right)$$

where the second step follows from noting that  $\sigma_\Psi < 1$  for sufficiently large  $n$ , and by replacing  $\sigma_\Psi$  with  $\sigma(z)$  via Lemma B.2.4.  $\square$

Below, we put all the above lemmas together to restate and prove the finite-sample convergence of the distribution of the U-statistic to the standard normal distribution.

**Theorem 4.2.1.** *Let  $x_1, \dots, x_n$  satisfy Assumption 1.1.1 (ie. not all equal) and let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$  and each  $e_i$  is sampled i.i.d from a continuous, symmetric, mean-0 distribution. Let  $S$  be a set of unordered pairs of datapoints, and let  $U_z$  be defined with respect to  $S$  as in (2). Let  $\mu(z) = \mathbb{E}_{e_1, \dots, e_n}[U_z]$ , and  $\sigma^2(z) = \text{Var}_{e_1, \dots, e_n}[U_z]$ .*

Then, for sufficiently large  $n$ ,

$$\sup_{t \in \mathbb{R}} \left| \Pr\left[\frac{U_z - \mu(z)}{\sigma(z)} \leq t\right] - \Phi(t) \right| = O\left(\frac{1}{n^2 \cdot \sigma^3(z)}\right)$$

where  $\Phi$  is the cdf of a standard normal distribution.

**PROOF.** Recall from Lemma B.2.3 the following definitions: for  $a_{ij} = \text{sign}(x_j - x_i)$  and  $B'_{ij} = \mathbb{E}_{e'}[\text{sign}(e' - e_i - z \cdot (x_j - x_i)) \mid e_i]$ , where  $e'$  is a fresh draw of the random variable  $e$ , we let

$$\Psi_i = \frac{1}{k} \sum_{j: \{i, j\} \in S} a_{ij} \cdot B'_{ij} \text{ and } \zeta_i = \frac{\Psi_i - \mu_i}{\sigma_\Psi \cdot n}$$

where  $\mu_i = \mathbb{E}_{e_1, \dots, e_n}[\Psi_i]$ ,  $\sigma_i = \text{Var}_{e_1, \dots, e_n}[\Psi_i]$ , and  $\sigma_\Psi^2 = \sum_{i=1}^n \sigma_i^2/n^2$ . From these definitions, it can be shown that  $\mathbb{E}[\zeta_i] = 0$ ,  $\mathbb{E}[\zeta_i^2] > 0$ ,  $\mathbb{E}[|\zeta_i|^3] < \infty$ , and  $\sum_{i=1}^n \text{Var}[\zeta_i] = 1$ . In addition, Lemma B.2.4 shows that for  $\mu_\Psi = \sum_{i=1}^n \mu_i/n$ ,

$$\mu(z) = \mu_\Psi, \quad \sigma^2(z) = \sigma_\Psi^2 + \Theta(1/N),$$

where  $N = |S|$ . By Lemma B.2.3, we therefore have that

$$\frac{U_z - \mu(z)}{\sigma(z)} = W + \Delta,$$

and for each  $i \in [n]$ ,  $\zeta_i$  is independent of  $(W - \zeta_i, \Delta_i)$ . Then, putting together Lemma B.2.2 and Lemma B.2.6 gives the desired result.  $\square$

## C Evaluating DPWideTS Bound for Special Case

We consider the special setting where the x-values are evenly split between the endpoints of an interval of length  $\Delta_x$ . The DPWideTS algorithm computes  $N = \lfloor n/2 \rfloor \cdot \lceil n/2 \rceil$  slopes. This section evaluates the bound from Theorem 4.0.2 for this special setting.

To do so, we first solve for the expectation and variance of the U-statistic for this case so that we can plug these values into the general convergence bound. We rely on the following approximation of the normal CDF.

**Lemma C.0.1** (Normal CDF approximation). *Let  $F(\cdot)$  be the cumulative distribution function for a Gaussian with mean  $\beta_1$  and variance  $\sigma^2$ . For all  $y$  such that  $|y - \beta_1|/\sigma$  is sufficiently small, we have that*

$$F(y) = \frac{1}{2} + \frac{y - \beta_1}{\sigma\sqrt{2\pi}} + O\left(\frac{(y - \beta_1)^3}{\sigma^3}\right)$$

**PROOF.** For any  $y \in \mathbb{R}$ , the distribution function  $F(y)$  is defined as follows.

$$F(y) = \frac{1}{2} \left( 1 + \text{erf}\left(\frac{y - \beta_1}{\sigma\sqrt{2}}\right) \right)$$

The error function  $\text{erf}(z)$  can be rewritten using a power series expansion. For  $z$  close to 0, we have:

$$\begin{aligned} \text{erf}(z) &= \frac{2}{\sqrt{\pi}} \int_0^z e^{-t^2} dt \\ &= \frac{2}{\sqrt{\pi}} \int_0^z \left( 1 - t^2 + \frac{t^4}{2!} + \dots \right) dt \\ &= \frac{2}{\sqrt{\pi}} \left( z - \frac{z^3}{3} + \dots \right) \\ &= \frac{2}{\sqrt{\pi}} z + O(z^3) \end{aligned}$$

Setting  $z = (y - \beta_1)/(\sigma\sqrt{2})$ , we have that when  $z$  is close to 0,

$$\begin{aligned} F(y) &= \frac{1}{2} \left( 1 + \frac{\sqrt{2}(y - \beta_1)}{\sqrt{\pi}\sigma} + O\left(\frac{(y - \beta_1)^3}{\sigma^3}\right) \right) \\ &= \frac{1}{2} + \frac{y - \beta_1}{\sigma\sqrt{2\pi}} + O\left(\frac{(y - \beta_1)^3}{\sigma^3}\right) \end{aligned}$$

which gives us the desired result.  $\square$

Now, we can evaluate the expectation and variance of  $U_z$  for this special setting.

**Lemma C.0.2.** *Suppose that  $x_1, \dots, x_n$  be at two endpoints of an interval of size  $\Delta_x$  such that they satisfy Assumption 5.0.1, and let  $e_1, \dots, e_n$  be drawn i.i.d from  $F_e = \mathcal{N}(0, \sigma_e^2)$  according to Assumption 5.0.2. Let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$ . Let  $S$  be the set of unordered pairs of datapoints, and let  $U_z$  be defined accordingly as in (2). Then, we have that for sufficiently small  $z \cdot \Delta_x/\sigma_e$ ,*

$$\mathbb{E}_{e_1, \dots, e_n} [U_z] = \frac{-z \cdot \Delta_x}{\sqrt{\pi}\sigma_e} + O\left(\frac{z^3 \cdot \Delta_x^3}{\sigma_e^3}\right)$$

**PROOF.** First, let  $F_{\text{diff}}$  refer to the CDF of the difference in any two i.i.d. noise variables  $e_j, e_i$ . In addition, let  $N = |S|$ . Then, we have from Lemma B.1.1 that

$$\mathbb{E}_{e_1, \dots, e_n} [U_z] = \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \text{sign}(\Delta_x) \cdot (1 - 2 \cdot F_{\text{diff}}(z \cdot \Delta_x))$$

Next, note that for our special case (assumptions 5.0.1 and 5.0.2),  $\text{sign}(\Delta_x) = 1$  and  $F_{\text{diff}}$  is the CDF of the difference between two i.i.d noise variables from a  $\mathcal{N}(0, \sigma_e^2)$  distribution. Therefore, using a Taylor approximation of the normal cdf from Lemma C.0.1, we have that for sufficiently small  $z \cdot \Delta_x/\sigma_e$ ,

$$\begin{aligned} \mathbb{E}_{e_1, \dots, e_n} [U_z] &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} (1 - 2 \cdot F_{\text{diff}}(z \cdot \Delta_x)) \\ &= \frac{1}{N} \sum_{\{i,j\} \in S, i < j} \left( 1 - 2 \left( \frac{1}{2} + \frac{z\Delta_x}{2\sqrt{\pi}\sigma_e} + O\left(\frac{z^3 \Delta_x^3}{\sigma_e^3}\right) \right) \right) \\ &= \frac{-z \cdot \Delta_x}{\sqrt{\pi}\sigma_e} + O\left(\frac{z^3 \cdot \Delta_x^3}{\sigma_e^3}\right) \end{aligned}$$

which gives the desired result.  $\square$

**Lemma C.0.3.** *Suppose that  $x_1, \dots, x_n$  be at two endpoints of an interval of size  $\Delta_x$  such that they satisfy Assumption 5.0.1, and let  $e_1, \dots, e_n$  be drawn i.i.d from  $F_e = \mathcal{N}(0, \sigma_e^2)$  according to Assumption 5.0.2. Let  $y_1, \dots, y_n$  be the corresponding response variables under the model  $y_i = \beta_0 + \beta_1 x_i + e_i$ , where  $\beta_0, \beta_1 \in \mathbb{R}$ . Let  $S$  be the set of unordered pairs of datapoints, and let  $U_z$  be defined accordingly as in (2). Then, for sufficiently small  $z \cdot \Delta_x/\sigma_e$ ,*

$$\text{Var}_{e_1, \dots, e_n} [U_z] = \frac{4}{3n} + O\left(\frac{z \cdot \Delta_x}{n \cdot \sigma_e}\right) + O\left(\frac{1}{n^2}\right)$$

**PROOF.** Let  $B_{ij}(z) = \text{sign}(\Delta_x) \cdot c_{ij}(z)$ , where  $c_{ij} = \text{sign}(e_j - e_i - z \cdot \Delta_x)$ . Starting with the result from Lemma B.1.2, we have that

$$\text{Var}_{e_1, \dots, e_n} [U_z] \leq \left( \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S \\ \{s,t\} \in S \\ |\{i,j\} \cap \{s,t\}|=1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \right) + \frac{1}{N}$$

Note that under our additional assumptions 5.0.1 and 5.0.2,  $\text{sign}(\Delta_x) = 1$  and  $N = \lfloor n/2 \rfloor \cdot \lceil n/2 \rceil$ .

Next, for  $|\{i, j\} \cap \{s, t\}| = 1$  (and supposing  $i = s$ ), we have that

$$\begin{aligned} \text{Cov}(B_{ij}(z), B_{st}(z)) &\leq \mathbb{E}_{e_1, \dots, e_n} [B_{ij}(z) \cdot B_{st}(z)] \\ &= \mathbb{E}_{e_i, e_j, e_t} [c_{ij}(z) \cdot c_{it}(z)] \\ &= \mathbb{E}_{e_i} [\mathbb{E}_{e_j, e_t} [c_{ij}(z) \cdot c_{it}(z) \mid e_i]] \\ &= \mathbb{E}_{e_i} [\mathbb{E}_{e_j} [c_{ij}(z) \mid e_i] \cdot \mathbb{E}_{e_t} [c_{it}(z) \mid e_i]] \\ &= \mathbb{E}_{e_i} [(1 - 2 \cdot F_e(e_i + z \cdot \Delta_x))^2] \end{aligned}$$

The same expression follows for the case where  $j = t$  instead of  $i = s$ . Note that  $F_e$  is the cumulative distribution function for  $e_i, i \in [n]$ , which by Assumption 5.0.2 is  $\mathcal{N}(0, \sigma_e^2)$ .

Setting  $w = z\Delta_x$ , let  $g(w) = \mathbb{E}_{e_i} [(1 - 2 \cdot F_e(e_i + w))^2]$ . Now, we can rewrite  $e_i$  as  $F_e^{-1}(U)$ , where  $U$  is a uniform  $[0, 1]$  random variable, and then compute  $g(0)$  as follows.

$$\begin{aligned} g(w) &= \mathbb{E}_U \left[ (1 - 2 \cdot F_e(F_e^{-1}(U) + w))^2 \right] \\ g(0) &= \mathbb{E}_U \left[ (1 - 2 \cdot F_e(F_e^{-1}(U)))^2 \right] = \mathbb{E}_U \left[ (1 - 2 \cdot U)^2 \right] = 1/3 \end{aligned}$$

Next, we know that for any constant  $c > 0$ , if  $|g'(w)| \leq c$  for all  $w \in \mathbb{R}$ , then

$$g(w) \in (g(0) - cw, g(0) + cw)$$

To bound  $g'(w)$ , we can first express it as follows.

$$\begin{aligned} g'(w) &= \mathbb{E}_U \left[ 2 \cdot (1 - 2 \cdot F_e(F_e^{-1}(U) + w)) \cdot (-2 \cdot F'_e(F_e^{-1}(U) + w)) \right] \\ &= \mathbb{E}_U \left[ -4 \cdot (1 - 2 \cdot F_e(F_e^{-1}(U) + w)) \cdot \frac{1}{\sigma_e \cdot \sqrt{2\pi}} \cdot \exp\left(\frac{-(F_e^{-1}(U) + w)^2}{2\sigma_e^2}\right) \right] \end{aligned}$$

where the second line follows by noting that  $F'_e$  is a pdf of a  $\mathcal{N}(0, \sigma_e^2)$  random variable. As a cumulative distribution function,  $F_e(\cdot)$  is between 0 and 1. In addition, we can see that the exp factor is between 0 and 1. Therefore, we have that

$$|g'(w)| \leq 4 \cdot \frac{1}{\sigma_e \cdot \sqrt{2\pi}} = O\left(\frac{1}{\sigma_e}\right), \text{ so } g(w) = g(0) + O\left(\frac{w}{\sigma_e}\right)$$

Finally, the number of terms that share one datapoint, ie.  $\#\{i, j\} \in S, \{s, t\} \in S \text{ s.t. } |\{i, j\} \cap \{s, t\}| = 1$ , divided by the  $N^2$  factor, is less than or equal to

$$\frac{2 \cdot (n/2)^2 \cdot (n/2 - 1)}{(n/2)^4} = \frac{4(n-2)}{n^2}$$

Putting this all together, we have that for  $w = z\Delta_x$ , the following holds.

$$\text{Var}_{e_1, \dots, e_n} [U(\delta_n, (x_i, y_i)_{i=1}^n)]$$

$$\begin{aligned}
&\leq \left( \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S \\ \{s,t\} \in S \\ |\{i,j\} \cap \{s,t\}|=1}} \text{Cov}(B_{ij}(z), B_{st}(z)) \right) + \frac{1}{N} \\
&\leq \left( \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S \\ \{s,t\} \in S \\ |\{i,j\} \cap \{s,t\}|=1}} E_{e_i} \left[ (1 - 2 \cdot F_e(e_i + z \cdot \Delta_x))^2 \right] \right) + \frac{1}{N} \\
&= \left( \frac{1}{N^2} \sum_{\substack{\{i,j\} \in S \\ \{s,t\} \in S \\ |\{i,j\} \cap \{s,t\}|=1}} g(w) \right) + \frac{1}{N} \\
&\leq \frac{1}{(n/2)^4} \cdot 2 \cdot (n/2)^2 \cdot (n/2 - 1) \cdot \left( \frac{1}{3} + O\left(\frac{w}{\sigma_e}\right) \right) + \frac{1}{(n/2)^2} \\
&= \frac{4(n-2)}{n^2} \left( \frac{1}{3} + O\left(\frac{w}{\sigma_e}\right) \right) + O\left(\frac{1}{n^2}\right) \\
&\leq \frac{4}{3n} + O\left(\frac{z \cdot \Delta_x}{n \cdot \sigma_e}\right) + O\left(\frac{1}{n^2}\right)
\end{aligned}$$

□

## D Confidence Intervals

First, we will prove the coverage validity of the non-private Theil-Sen confidence interval [49] stated in Lemma 6.1.2.

PROOF OF LEMMA 6.1.2. We will consider the upper limit of the interval,  $\hat{\beta}_{1U}$ , for simplicity. First, note that

$$\begin{aligned}
U(\hat{\beta}_{1U}) &= 1 - 2F_s(\hat{\beta}_{1U}) = 1 - 2F_s(F_s^{-1}(1/2 + b)) \\
&= -2b = \Phi^{-1}(\alpha_1/8) \cdot \sigma(0)
\end{aligned}$$

Next, we rely on the fact that if  $\beta_1 > \hat{\beta}_{1U}$ ,  $U(\beta_1) < U(\hat{\beta}_{1U})$ . Therefore, we can use the distribution of  $U(\beta_1)$  and its convergence to a standard normal via Theorem 4.2.1 to evaluate the probability that  $\beta_1 > \hat{\beta}_{1U}$ .

$$\begin{aligned}
\Pr_s \left[ \beta_1 > \hat{\beta}_{1U} \right] &= \Pr_s \left[ U(\beta_1) < U(\hat{\beta}_{1U}) \right] \\
&\leq \Phi \left( \frac{U(\hat{\beta}_{1U})}{\sigma(0)} \right) + O\left(\frac{1}{n^2 \cdot \sigma^3(0)}\right) \\
&= \Phi \left( \frac{\Phi^{-1}(\alpha_1/8) \cdot \sigma(0)}{\sigma(0)} \right) + O\left(\frac{1}{n^2 \cdot \sigma^3(0)}\right) \\
&= \alpha_1/8 + O\left(\frac{1}{n^2 \cdot \sigma^3(0)}\right) \\
&= \alpha_1/8 + O\left(\frac{1}{\sqrt{n}}\right) \\
&\leq \alpha_1/2
\end{aligned}$$

where the second to last line holds follows from Corollary B.1.3 and the last line holds for  $n \geq c/\alpha_1^2$ . We can go through a similar argument for  $\hat{\beta}_{1L}$ , which gives the desired result. □