

GEOGRAPHIC SPINES IN THE 2020 CENSUS DISCLOSURE AVOIDANCE SYSTEM TOPDOWN ALGORITHM

John M. Abowd,[†] Robert Ashmead,^{†, ‡} Ryan Cumings-Menon,[†] Daniel Kifer,^{†, ◊}
Philip Leclerc,[†] Jeffrey Ocker,[†] Michael Ratcliffe,[†] Pavel Zhuravlev[†]

[†] U.S. Census Bureau

[‡] The Ohio Colleges of Medicine Government Resource Center

[◊] Penn State University

1. INTRODUCTION

The Census TopDown Algorithm (TDA) outputs microdata that satisfy either pure or zero-concentrated differential privacy (DP). The TDA begins by estimating the differentially private data histogram at the coarsest (highest) geographic level, or *geolevel* in a hierarchy, which is the U.S. (or the Commonwealth of Puerto Rico). Next, TDA estimates differentially private data histograms at progressively finer (lower) geographic granularity, subject to the constraint that these histograms are consistent with the estimates of next-higher (parent) geolevels. TDA processes the geolevels in a hierarchy given by, U.S., state, county, tract group, tract, block group, and block. *Geounits* are defined as the geographic entities in each of these geolevels. The definition of the geounits in this hierarchy is called the geographic *spine*.

TDA originally used the conventional geographic spine based on the Census Bureau Geography Division definitions of state, county, tract, block group, and block. Block groups, as defined by the Census Bureau's Geography Division, are the smallest geographic tabulation areas for the American Community Survey. Tracts, as defined by the Geography Division, are statistical tabulation areas used by decennial censuses and the American Community Survey. For both of these definitions, the tabulation geographies are designed to produce statistics on meaningful areas that can be usefully compared over time. Note that the geographic spine is a construct that is used internally in the TDA, and, even when the geographic spine used within the TDA does not correspond to this conventional spine, the statistical tabulations based on the TDA output define all geounits, including tracts and block groups, by Geography Division's standard definitions.

In order to ensure computational feasibility and enhance the accuracy of statistical tabulations, TDA created tract groups and redefined block groups in a consistent manner with the hierarchical structure of all geographic spines and the Geography Division's definitions of counties, tracts, and blocks. In particular, TDA used tract groups and redefined block groups to reduce the number of child geounits of parent geounits, called the *fanout* values.

The conventional spine, as defined by Geography Division, had two primary shortcomings when used within TDA. First, legally defined American Indian/Alaska Native/Native Hawaiian (AIAN) tribal areas are usually far from this spine, meaning that many on-spine geounits must be added to or subtracted from one another to compose these geographic areas. Being distant from the spine often results in query count estimates with greater mean squared error than equivalent geounits that are on-spine. Second, the conventional spine also places many other important legal, political or Census-designated entities far from the spine. These include minor civil divisions (MCDs) in regions that are both within strong-MCD states and outside of AIAN tribal areas, and incorporated places in regions that are either outside of the strong-MCD states or within AIAN areas. Collectively, we refer to these geographic entities as the *Place/MCD entities* (PMEs) in the remainder of the paper.

Date: August 18, 2021.

* The views expressed in this technical paper are those of the authors and not those of the U.S. Census Bureau.

To ameliorate the off-spine distance of AIAN tribal areas, TDA placed the state-level aggregate of all AIAN tribal areas on the spine. Then, TDA redefined each geounit at the state geolevel and below by the intersection of this geounit’s original definition and either the on-spine AIAN areas or their complement. This geographic hierarchy is called the *AIAN spine*. It was audited by the Geography Division for correctness in defining the AIAN tribal areas and their complements according to the final 2020 Census tabulation geographies.

This document describes several optimization heuristics that perform updates on the AIAN spine to enhance a few aspects of the spine, and we call the resulting geographic spine the *optimized spine*. First, the spine optimization methods redefine block groups and tract groups to bring a user specified set of *off-spine entities* (OSEs) closer to the spine. The current definition of OSEs used within the TDA includes both PMEs, and, to decrease the correlation between blocks with group quarters (GQs) and their nearby counterparts, for each tract and each combination of the seven major GQ types, the union of all blocks within the tract that contain GQs of each type in the GQ type combination. These redefinitions also ensure that fan-out values are not too high. After this is done, the second stage of the spine optimization algorithm reduces the variance of the final estimate by ensuring that fan-out values of the spine are also not too low, using a heuristic based on the variance matrix of the OLS estimator. For example, this decision rule results in parent geounits that only have one child being bypassed, the consistency with parent constraints require that the count estimates of the child are equal to those of the parent, so bypassing the parent geounit, or reallocating all of the privacy loss budget (PLB) from the parent to the child and then removing the parent, reduces the variance of the DP answers used to derive the final histogram estimate.

The heuristics used in these optimization routines are based on existing results from the DP literature, which are provided in Section 2. Afterward, Section 3 describes how geographic spines are represented here using matrices, and a summary of the remainder of the paper is also provided in this section. Afterward, the method used in the first stage is described Section 4. Section 5 describes the method used in the second stage and provides a result on the privacy guarantees of the TDA when an optimized spine is used. The next subsection outlines the notation used throughout this paper.

1.1. Notation. Throughout the paper we will denote matrices using capitalized font, and vectors using lower case bold font. Also, let the Kronecker product of the real matrices A, B be denoted by $A \otimes B$, and elementwise division, when these matrices are conformable, by $A \oslash B$ respectively. We will denote the elementwise absolute value of the real matrix A by $|A|$. A length N column vector with each element equal to $c \in \mathbb{R}^1$ will be denoted by \mathbf{c}_N , and, when there is little risk of confusion, we will omit the subscript N .

We will make use of several probability distributions, but two are worth pointing out explicitly, as their definitions are less standard. First, we will define the discrete Gaussian random variable so that its probability mass function, $f : \mathbb{Z} \rightarrow \mathbb{R}$, is given by $f(x) \propto \exp(-(x - \mu)^2 / (2\sigma^2))$, and denote the distribution of this random variable by $N_{\mathbb{Z}}(\mu, \sigma^2)$; see for example, [4]. Second, we will also define the discrete Laplace random variable so that its probability mass function, $f : \mathbb{Z} \rightarrow \mathbb{R}$, is given by $f(x) \propto \exp(-|x - \mu|/b)$, and denote the distribution of this random variable by $\text{Laplace}_{\mathbb{Z}}(\mu, \sigma^2)$; see for example, [8]. We also conform with the usual notation for the (continuous) Gaussian distribution and denote the distributions of length n column vectors with elements that are distributed as $N_{\mathbb{Z}}(\boldsymbol{\mu}_i, \mathbf{c}_i)$, $\text{Laplace}(\boldsymbol{\mu}_i, \mathbf{c}_i)$, and $\text{Laplace}_{\mathbb{Z}}(\boldsymbol{\mu}_i, \mathbf{c}_i)$, where $\boldsymbol{\mu} \in \mathbb{R}^n$ and $\mathbf{c} \in \mathbb{R}_+^n$, by $N_{\mathbb{Z}}(\boldsymbol{\mu}, \text{diag}(\mathbf{c}))$, $\text{Laplace}(\boldsymbol{\mu}, \text{diag}(\mathbf{c}))$, and $\text{Laplace}_{\mathbb{Z}}(\boldsymbol{\mu}, \text{diag}(\mathbf{c}))$ respectively.

2. DIFFERENTIAL PRIVACY

2.1. Privacy Definitions. The definitions of pure and approximate differential privacy are provided by [6, 7], and these definitions are also restated below. Both definitions can be viewed as a limit on the difference between the distribution of a mechanism’s output when the input is a given database and the distribution of the output when the input is a *neighboring database*. The specific notion of difference used in these definitions, along with their required upper bounds, is generally self evident, but more care is required in the case of the notion of neighboring database. This is because there are multiple definitions for this term that are commonly used, but the privacy semantic guarantees that these definitions imply are different from one another. For example, two databases are said to be *unbounded neighbors* if one database can be derived by adding *or* removing a record from the other database; likewise, two databases are said to be *bounded neighbors* if one database can be derived from the other by adding one record *and* removing one record [10].

In other words, the set of unbounded neighbors can be written as $\{x, x' \in \mathcal{X}^d \mid d_{\mathcal{H}}(x, x') = 2\}$, where \mathcal{X}^d is the set of databases with d records, and the set of bounded neighbors as $\{x, x' \mid d_{\mathcal{H}}(x, x') = 1\}$.

The definition of neighbor has important implications because the upper bounds provided in the privacy guarantees below can be translated into an upper bound on the power of any statistical test of the null hypothesis that the input database is x verse the alternative that it is a neighbor of x [5, 13]. For example, using bounded neighbors does not provide a theoretical bound on the accuracy of inferences on the number of records in the input database. However, in the case of tests with a null hypothesis that the database is x and an alternative hypothesis that it is a given bounded neighbor of x , formal privacy definitions that use bounded neighbors provide stronger limitations on the accuracy of privacy attackers' inferences. This can be shown for the privacy definitions below using the fact that a bounded neighbor of a given database is also an "unbounded neighbor of an unbounded neighbor" of the database.

The privacy guarantees provided by the TDA use a unique definition of neighbor that does not protect against certain inferences. Specifically, TDA does not protect each state's total population or the locations of each group quarter type. In other words, TDA outputs a database with state total populations that are identical to those of the input database, and, since at least one person must reside in each group quarter by the Census definition of group quarter, the population residing in each group quarter type in a given geounit is constrained to be at least the number of group quarters of that type within the geounit. For more detail on these two categories of data-dependent constraints imposed by TDA, as well as those that are data-independent, see [1].

For this reason, in the context of the TDA, two databases are said to be neighbors if one database can be derived from the other by adding one record to a given state and then removing one record from that same state, such that both databases also satisfy the group quarters invariant constraints. To emphasize this definition of neighbors in the presence of invariant constraints in our privacy definitions below, we will define the set of pairs of neighboring databases as $\{x, x' \in \mathcal{U} \mid d_{\mathcal{H}}(x, x') = 2\}$, where \mathcal{U} is a given universal set of databases. For example, this notation is a generalization of the definition of bounded neighbors, which used $\mathcal{U} = \mathcal{X}^d$. In the results throughout this paper that use these privacy definitions, we will denote the set of databases that satisfy these group quarter invariant constraints as \mathcal{G} and the set of databases with d_i records in each state i as \mathcal{X}^d . Using this notation, the definition of neighbors used by the TDA can be written as, $\{x, x' \in \mathcal{X}^d \cap \mathcal{G} \mid d_{\mathcal{H}}(x, x') = 2\}$.

Definition 1. (*Pure/Approximate Differential Privacy* [6, 7]) A randomized algorithm $\mathcal{M} : \mathcal{U} \rightarrow \mathcal{Y}$ satisfies approximate (ϵ, δ) -differential privacy if, for all $(x, x') \in \{x, x' \in \mathcal{U} \mid d_{\mathcal{H}}(x, x') = 2\}$ and all $E \subset \mathcal{Y}$, we have $P(\mathcal{M}(x) \in E) \leq \exp(\epsilon)P(\mathcal{M}(x') \in E) + \delta$. Also, we say a randomized algorithm satisfies pure ϵ -differential privacy if it satisfies $(\epsilon, 0)$ -differential privacy.

The definition of ρ -zero-concentrated DP (ρ -zCDP) [3, 4, 2] is provided below. We will primarily use ρ -zCDP as an intermediate privacy accounting tool when deriving an approximate DP mechanism; a result from [4], which is restated in the next subsection, provides a way to translate ρ -zCDP privacy guarantees to (ϵ, δ) -DP privacy guarantees.

Definition 2. (*Zero-Concentrated Differential Privacy (zCDP)* [2]) A randomized mechanism $\mathcal{M} : \mathcal{U} \rightarrow \mathcal{Y}$ is ρ -zero-concentrated differentially private (ρ -zCDP) if, for all $x, x' \in \{x, x' \in \mathcal{U} \mid d_{\mathcal{H}}(x, x') = 2\}$, all $\alpha \in (1, \infty)$, and all events $E \subset \mathcal{Y}$,

$$D_{\alpha}(\mathcal{M}(x) \parallel \mathcal{M}(x')) \leq \rho\alpha,$$

where $D_{\alpha}(P \parallel Q) = \log(\sum_{E \in \mathcal{Y}} P(E)^{\alpha} Q(E)^{(1-\alpha)}) / (\alpha - 1)$ is the Rényi divergence of order α between the distributions P and Q .

2.2. Privacy-Loss Accounting Results. A general pattern in our proofs that the TDA is DP will be to first establish that the DP primitive mechanism for each query i is either ϵ_i -DP or ρ_i -zCDP, and then use parallel and sequential composition to show that the combination of all of the DP primitive query answers used in the TDA are $\sum_i \epsilon_i$ -DP or $\sum_i \rho_i$ -zCDP. In the case of approximate DP, we will also require the final step of ensuring that $\sum_i \rho_i$ implies (ϵ, δ) -DP. This section contains these intermediate results that will be used in these proofs. The first two results will be used in the next subsection to show that each DP primitive mechanism satisfies $(\epsilon, 0)$ -DP or ρ -zCDP.

Lemma 1. (Theorem 3.2 [8]) Let $\Delta, \epsilon > 0$. Let $q : \mathcal{U} \rightarrow \mathbb{Z}$ satisfy $|q(x) - q(x')| \leq \Delta$ for all $x, x' \in \{x, x' \in \mathcal{U} \mid d_{\mathcal{H}}(x, x') = 2\}$. Define a randomized algorithm by $\mathcal{M}(x) = q(x) + Y$ where either $Y \sim \text{Laplace}_{\mathbb{Z}}(0, \Delta/\epsilon)$ or $Y \sim \text{Laplace}(0, \Delta/\epsilon)$. Then \mathcal{M} satisfies ϵ -DP.

Lemma 2. (Theorem 4 [3, 4]) Let $\Delta, \epsilon > 0$. Let $q : \mathcal{U} \rightarrow \mathbb{Z}$ satisfy $|q(x) - q(x')| \leq \Delta$ for all $x, x' \in \{x, x' \in \mathcal{U} \mid d_{\mathcal{H}}(x, x') = 2\}$. Define a randomized algorithm by $\mathcal{M}(x) = q(x) + Y$ where either $Y \sim \mathcal{N}_{\mathbb{Z}}(0, \Delta^2/(2\rho))$ or $Y \sim \mathcal{N}(0, \Delta^2/(2\rho))$. Then \mathcal{M} satisfies ρ -zCDP.

While providing a comprehensive compilation of the properties that are implied by a mechanism satisfying either (ϵ, δ) -DP or ρ -zCDP is beyond the scope of this paper, there are a few of these properties that we make use of below that are worth explicitly pointing out. First, these privacy guarantees share the property that they are invariant to post-processing. In other words, if $\mathcal{M} : \mathcal{U} \rightarrow \mathcal{Y}$ satisfies either of these privacy guarantees, then so does the mechanism $f \circ \mathcal{M}$, where $f : \mathcal{Y} \rightarrow \mathcal{Z}$. Second, if $\mathcal{M}_1(x)$ is ϵ_1 -DP (respectively, ρ_1 -zCDP) and $\mathcal{M}_2(x)$ is ϵ_2 -DP (ρ_2 -zCDP) then releasing the output of $\mathcal{M}_1(x)$ and $\mathcal{M}_2(x)$ simultaneously is itself $(\epsilon_1 + \epsilon_2)$ -DP ($(\rho_1 + \rho_2)$ -zCDP), which is called sequential composition. In some cases in which $\mathcal{M}_1(x)$ and $\mathcal{M}_2(x)$ only depend on disjoint subsets of the arbitrary dataset $x \in \mathcal{U}$, releasing the outputs of both of these mechanisms simultaneously is $(\max\{\epsilon_1, \epsilon_2\})$ -DP (respectively, $(\max\{\rho_1, \rho_2\})$ -zCDP), which is known as parallel composition. Specifically, the following lemma uses sequential and parallel composition to provide privacy guarantees for a mechanism that is defined by multiple univariate mechanisms described in Lemmas 1 and 2.

Lemma 3. (Theorem 14 [4], Proposition 1 [6], Theorem 3.2 [8]) Suppose $x, x' \in \mathcal{X}^d$ differ on a single entry, and let a randomized algorithm $\mathcal{M} : \mathcal{X}^d \rightarrow \mathcal{Y}^m$ be defined by $\mathcal{M}(x) = q(x) + \mathbf{y}$ where $q : \mathcal{X}^d \rightarrow \mathcal{Y}^m$ and \mathbf{y} is an m dimensional column vector of independent random variables. Then we have the following.

- (1) Let $b_1, \dots, b_m > 0$, $\epsilon > 0$, and $\sum_{j=1}^m \frac{|q_j(x) - q_j(x')|}{b_j} \leq \epsilon$. If, for all $j \in \{1, \dots, m\}$, either $\mathbf{y}_j \sim \text{Laplace}_{\mathbb{Z}}(0, b_j)$ or $\mathbf{y}_j \sim \text{Laplace}(0, b_j)$, then \mathcal{M} satisfies ϵ -DP.
- (2) Let $\sigma_1, \dots, \sigma_m > 0$, $\rho > 0$, and $\sum_{j=1}^m \frac{(q_j(x) - q_j(x'))^2}{\sigma_j^2} \leq 2\rho$. If, for all $j \in \{1, \dots, m\}$, either $\mathbf{y}_j \sim \mathcal{N}_{\mathbb{Z}}(0, \sigma_j^2)$ or $\mathbf{y}_j \sim \mathcal{N}(0, \sigma_j^2)$, then \mathcal{M} satisfies ρ -zCDP.

The next result provides a way to translate between an (ϵ, δ) -DP guarantee and a ρ -zCDP guarantee. Note that this result implicitly defines ρ in terms of ϵ, δ . After ρ is computed numerically using this result, the TDA scales the parameters denoted by σ^2 that are used within the DP primitive mechanisms to ensure that releasing a combination of all of these primitive mechanisms simultaneously satisfies (ϵ, δ) -DP. We refer the interested reader to [3, 4] for more detail on how the optimization problem below can be solved efficiently within the numerical method used to compute ρ .

Lemma 4. (Proposition 7 [3], Corollary 13 [4]) Let $\mathcal{M} : \mathcal{U} \rightarrow \mathcal{Y}$ be a randomized algorithm satisfying ρ -zCDP. Then \mathcal{M} is (ϵ, δ) -DP for any $\epsilon \geq 0$ and δ given by the unique solution of,

$$\inf_{\alpha \in (1, \infty)} \frac{\exp((\alpha - 1)(\alpha\rho - \epsilon))}{\alpha - 1} \left(1 - \frac{1}{\alpha}\right)^{\alpha}.$$

2.3. Linear Queries And Marginal Query Groups. The notation for each query $q(\cdot)$ in the preceding subsections is actually more general than required to describe the TDA. Specifically, the TDA only makes use of linear queries. We will define a *linear query* as a length n vector, and a linear query answer as the inner product of a linear query and the histogram cell counts. Since we only consider linear queries from this point forward, we will sometimes refer to a linear query as a *query* below. A *query matrix* is used to refer to linear queries that are vertically stacked on top of one another.

All elements of the linear queries used within the TDA have elements that are either zero and one, and they are defined so that each linear query answer provides an individual count for a marginal of the full histogram. It will be convenient to group the queries providing counts for the same marginal together, so we will define a *query group* as the linear queries that provide counts for the same marginal, vertically stacked on top of one another. For example, suppose the schema of the original database is CENRACE \times HISP \times VOTINGAGE, where CENRACE and HISP indicate which of the 63 Census race combinations, and which of the two hispanicity levels, the respondent identified as, respectively, and VOTINGAGE indicates if the

respondent is at least 18 years of age.¹ In this case the CENRACE \times VOTINGAGE query group is defined as the matrix

$$Q = I_{63} \otimes \mathbf{1}_2^\top \otimes I_2,$$

and right multiplying Q by the vector of histogram cell counts of a database provides the CENRACE \times VOTINGAGE query group answers. More generally, the query matrix of a given query group is defined as a matrix that can be written as a series of Kronecker products of identity matrices and row vectors of ones. Note that this definition encompasses cases in which each of these Kronecker factors are all either row vectors of ones or are all identity matrices.

One of the inputs of the TDA are either the proportions of PLB, when pure DP primitive mechanisms are used, or proportions of ρ , when approximate DP primitive mechanisms are used, to allocate to each query for a given geolevel. The following lemma uses this notational convention, while only considering either a single geounit, to provide the ϵ -DP and ρ -zCDP privacy guarantees of releasing the output of the primitive mechanisms of this geounit.² This will be used in the next section to provide the privacy guarantees of the TDA when either the conventional spine or the AIAN spine is used.

Lemma 5. *If each $Q[i] \in \{Q[i]\}_{i=1}^q$ is a query group of dimension $m[i] \times n$ and the mechanism $\mathcal{M}(\mathbf{x})$, outputs $\{Q[i]\mathbf{x} + \mathbf{y}[i]\}_{i=1}^q$, where \mathbf{x} is a vector of the histogram counts for a database with d records and $\mathbf{y}[i]$ is a length $m[i]$ column vector of independent random variables, then we have the following.*

- (1) *If, for each $i \in \{1, \dots, q\}$, we have that $\mathbf{y}[i]$ is distributed as either $\mathbf{y}[i] \sim \text{Laplace}(0, \text{diag}(\mathbf{2}_{m[i]} / (\epsilon\alpha[i])))$ or $\mathbf{y}[i] \sim \text{Laplace}_{\mathbb{Z}}(0, \text{diag}(\mathbf{2}_{m[i]} / (\epsilon\alpha[i])))$, where $\sum_i \alpha[i] = 1$, then $\mathcal{M}(\cdot)$ is ϵ -DP.*
- (2) *If, for each $i \in \{1, \dots, q\}$, we have that $\mathbf{y}[i]$ is distributed as either $\mathbf{y}[i] \sim \text{N}(0, \text{diag}(\mathbf{1}_{m[i]} / (\rho\alpha[i])))$ or $\mathbf{y}[i] \sim \text{N}_{\mathbb{Z}}(0, \text{diag}(\mathbf{1}_{m[i]} / (\rho\alpha[i])))$, where $\sum_i \alpha[i] = 1$, then $\mathcal{M}(\cdot)$ is ρ -zCDP.*

Proof. Since, for each $i \in \{1, \dots, q\}$, only one element of each column of $Q[i]$ is nonzero, we will use Lemma 3 to leverage parallel composition to prove both cases. This reduces the problem to carrying out sequential composition of the set of mechanisms, $\{\mathcal{M}[i](\mathbf{x})\}_i^q$, where $\mathcal{M}[i](\mathbf{x}) := Q[i]\mathbf{x} + \mathbf{y}[i]$. In both cases, we will use the fact that $|Q[i]\mathbf{x} - Q[i]\mathbf{x}'|$, where \mathbf{x}, \mathbf{x}' are vectors of histogram cell counts of databases differing on a single entry, is a vector with at most two elements that are equal to one, with the remaining elements equal to zero.

In the first case, since $\sum_j |Q[i]_{j,\cdot}\mathbf{x} - Q[i]_{j,\cdot}\mathbf{x}'| \leq 2$, the first case in Lemma 3 implies $\mathcal{M}[i](\mathbf{x})$ is $\alpha[i]\epsilon$ -DP. Thus, using sequential composition, releasing the output of $\{\mathcal{M}[i](\mathbf{x})\}_i$ is $\sum_i \alpha[i]\epsilon = \epsilon$ -DP.

In the second case, since $\sum_j |Q[i]_{j,\cdot}\mathbf{x} - Q[i]_{j,\cdot}\mathbf{x}'|^2 \leq 2$, the second case in Lemma 3 implies $\mathcal{M}[i](\mathbf{x})$ is $\alpha[i]\rho$ -zCDP. Thus, using sequential composition, releasing the output of $\{\mathcal{M}[i](\mathbf{x})\}_i$ is $\sum_i \alpha[i]\rho = \rho$ -zCDP. \square

2.4. The Matrix Mechanism. This section will describe a class of random mechanisms known as matrix mechanisms in the context of linear queries composed of query groups [11]. Using the notation introduced in Lemma 5, we will assume that each of the errors of the i^{th} query group are random variables that are distributed as either $\mathbf{y}[i]_j \sim \text{Laplace}(0, 2/(\epsilon\alpha[i]))$, in the case of ϵ -DP, or $\mathbf{y}[i]_j \sim \text{N}(0, 1/(\rho\alpha[i]))$, in the case of ρ -zCDP, for every $j \in \{1, \dots, m[i]\}$, where $\alpha[i] \in \mathbb{R}_{++}$ satisfies $\sum_i \alpha[i] = 1$. Also, let the *workload* matrix $W \in \mathbb{R}^{m \times n}$ be defined as $W := \text{stack}(\{Q[i]\}_i^q)$, the errors vector as $\mathbf{y} := \text{stack}(\{\mathbf{y}[i]\}_i^q)$, the PLB or precision proportions vector as $\boldsymbol{\alpha} := \text{stack}(\{\alpha[i]\}_{m[i]}^q)$, and the response variable as $\mathbf{z} := W\mathbf{x} + \mathbf{y}$, which is also the vertically stacked output of the mechanism described in Lemma 5. We will assume that W has full column rank, which can be ensured by including the detailed cell query group in W (i.e.: the identity matrix).

For both of the distributions that we consider in this section, we can define an alternative response variable that is observationally equivalent to \mathbf{z} , but with homoskedastic errors. For example, in the case of ϵ -DP, we have $\mathbf{y} \sim \text{Laplace}(0, \text{diag}(\mathbf{2} \odot (\epsilon\boldsymbol{\alpha})))$, so we can define the rescaled errors as $\tilde{\mathbf{y}} := \text{diag}(\epsilon\boldsymbol{\alpha}/2)\mathbf{y}$, which are

¹While we are using attributes that are part of the census, note that this example, and the queries in this section, are simply described in the context of a hypothetical survey that does not use a geographic spine. The linear query notation introduced here will be extended in the next section to account for the presence of the geographic spine.

²Alternatively, for datasets that contain an attribute identifying each respondent's geounit for a given geolevel, this theorem can also be used to provide the privacy guarantees of releasing the output of all of the primitive DP mechanisms for the geolevel. However, depending on how the operation of bypassing geounits is defined, this can be less straightforward in the case of the optimized spine because there may be respondents in the dataset that are not included in any geounit in the geolevel. This alternative interpretation of the Lemma will be discussed in more detail in Sections 3, and the operation of bypassing geounits will be defined in 5.

distributed as $\tilde{\mathbf{y}} \sim \text{Laplace}(0, I)$, the rescaled workload as $\tilde{W} := \text{diag}(\epsilon\alpha/2)W$, and the rescaled response variable as $\tilde{\mathbf{z}} := \text{diag}(\epsilon\alpha/2)\mathbf{z} = \tilde{W}\mathbf{x} + \tilde{\mathbf{y}}$. In the case of ρ -DP, we have $\mathbf{y} \sim N(0, \text{diag}(\mathbf{1} \odot (\rho\alpha)))$, so we can define the rescaled errors as $\tilde{\mathbf{y}} := \text{diag}(\sqrt{\rho\alpha})\mathbf{y}$, which are distributed as $\tilde{\mathbf{y}} \sim N(0, I)$, the rescaled workload as $\tilde{W} := \text{diag}(\sqrt{\rho\alpha})W$, and the rescaled response variable as $\tilde{\mathbf{z}} := \text{diag}(\sqrt{\rho\alpha})\mathbf{z} = \tilde{W}\mathbf{x} + \tilde{\mathbf{y}}$.

One simple example of a matrix mechanism is a mechanism that releases the ordinary least squares estimates of $W\mathbf{x}$. Specifically, this can be done by first estimating \mathbf{x} as $\hat{\mathbf{x}} := \arg \min_{\mathbf{x}} \|\tilde{W}\mathbf{x} - \tilde{\mathbf{z}}\|_2^2 = (\tilde{W}^\top \tilde{W})^{-1} \tilde{W}^\top \tilde{\mathbf{z}}$, and then defining the output of the mechanism as $W\hat{\mathbf{x}}$. Note that in either the case of ϵ -DP or ρ -zCDP, the privacy guarantee of the final mechanism follows from the fact that a mechanism that released $\tilde{\mathbf{z}}$ would satisfy the same privacy guarantee, along with the invariance to post-processing property.

This simple mechanism can be generalized by making a distinction between the linear query answers provided as output and the linear queries used to estimate $\hat{\mathbf{x}}$. Specifically, we will define the *strategy* matrix $A \in \mathbb{R}^{p \times n}$ by $A := \text{stack}(\{R[i]\}_i^r)$, and the query group PLB or precision proportions by $\{\gamma[i]\}_i^r$. In the same manner as described above for W , we can define the rescaled strategy matrix as $\tilde{A} := \text{diag}(\epsilon\gamma/2)A$, when deriving an ϵ -DP mechanism, or $\tilde{A} := \text{diag}(\sqrt{\rho\gamma})A$, when deriving a ρ -zCDP mechanism. Likewise, the rescaled error vector and response variable can be defined as above so that $\tilde{\mathbf{z}} := \tilde{A}\mathbf{x} + \tilde{\mathbf{y}}$. The final output of this matrix mechanism is then given by this alternative estimate of the linear queries in the workload W , which are $W\hat{\mathbf{x}} = W(\tilde{A}^\top \tilde{A})^{-1} \tilde{A}^\top \tilde{\mathbf{z}}$.³

Note that the variance matrix of this output vector is given by,

$$\text{Var}(W\hat{\mathbf{x}}) = W(\tilde{A}^\top \tilde{A})^{-1} W^\top.$$

Prior works have focused on using this variance matrix to find strategies that provide a low expected sum of squared errors, which is given by $\text{Trace}(\text{Var}(W\hat{\mathbf{x}})) = \text{Trace}(W^\top W(\tilde{A}^\top \tilde{A})^{-1})$; see for example, [11, 12]. We use an alternative approach to motivate the heuristic used to bypass geounits in Section 5, after introducing how we represent the spine using matrices in the next section.

3. REPRESENTING LINEAR QUERIES ON THE SPINE

In this section we will describe how we represent the workload and the strategy matrices that include the linear queries for each geounit on the spine. To do so, we will first consider the case in which the same query groups are used in all such geounits, and generalize this notation afterward to the case in which the query matrix is dependent on the geolevel.

Let the workload of the linear queries for each geounit be denoted by $W \in \mathbb{R}^{m \times n}$, where $W = \text{stack}(\{Q[i]\}_i^q)$ and each $Q[i]$ is a query group matrix. We will also assign an integer to each block geounit for the purpose of ordering the blocks. Specifically, we will suppose that the blocks are ordered lexicographically so that blocks in the same state are adjacent to one another, within each state, blocks in the same county are adjacent, etc. For example, in the case of the conventional geographic spine, this can be achieved by sorting the blocks by their 15 digit Census GEOID, as the format of the GEOID is [2 digit state FIPS code][3 digit county FIPS code][6 digit Census tract code][4 digit Census block code]. We will also periodically refer to geounit $u \in \{1, \dots, U[l]\}$ in geolevel $l \in \{1, \dots, L\}$ as geounit (l, u) .

We will also let $b[l, u]$ denote the number of block level descendants of geounit (l, u) . For example, since all blocks are descendants of the US geounit, there a total of $b[1, 1]$ blocks. Let $\mathbf{x} \in \mathbb{Z}_+^{nb[1, 1]}$ be a vector of histogram cell counts over all blocks in the US, ordered in the manner described in the preceding paragraph, which we will refer to as the true histogram cell counts below. Using this notation, we can express the query answers to the query matrix W for the US geounit in terms of these block level cell counts as $(\mathbf{1}_{b[1, 1]}^\top \otimes W)\mathbf{x}$. Likewise, the query answers for all of the block geounits is $(I_{b[1, 1]} \otimes W)\mathbf{x}$. More generally, this notation allows us to express the workload over all geolevels as sums of block level cell counts. Specifically, a possible workload is

³All of the results and discussion in this paper are also straightforward to extend to the more general case in which the workloads and strategy matrices are not required to be vertically stacked query group matrices. The most obvious generalization would be to cases in which one also assigned a weight to each query in the workload matrix. Allowing for this generalization, or removing the requirement that these matrices are vertically stacked query groups entirely, is also straightforward, and this would not alter the theorem and observation provided in Section 5.

$$V := B \otimes W \in \mathbb{R}_+^{M \times N},$$

where $M := m \sum_l U[l]$, $N := nb[1, 1]$, and,

$$(1) \quad B := \begin{bmatrix} B[1] \\ B[2] \\ \vdots \\ B[L-1] \\ B[L] \end{bmatrix} = \begin{bmatrix} \mathbf{1}_{b[1,1]}^\top \\ \text{block_diag}(\{\mathbf{1}_{b[2,u]}^\top\}_{u=1}^{U[2]}) \\ \vdots \\ \text{block_diag}(\{\mathbf{1}_{b[L-1,u]}^\top\}_{u=1}^{U[L-1]}) \\ I_{b[1,1]} \end{bmatrix}.$$

As a summary of this notation, an example of $B \otimes W$ is shown in Figure 1.

While we will use this definition for the workload over all geolevels when describing a heuristic used in the spine optimization routines below, it is not actually quite general enough to capture all possible workloads that a user may specify in the TDA. This is because the TDA also allows users to specify distinct strategy matrices in each geolevel, but the notation above assumes that the strategy matrix in each geolevel is W . For this reason, we will also use an alternative definition for the strategy matrix that is general enough to encompass all possible workloads used by TDA in our results that establish privacy guarantees. To do so, let $W[l] \in \{W[l]\}_{l=1}^L$ denote the workload in geolevel l . Using this notation, the workload used within the TDA can be defined as,

$$(2) \quad V := \begin{bmatrix} B[1] \otimes W[1] \\ B[2] \otimes W[2] \\ \vdots \\ B[L-1] \otimes W[L-1] \\ B[L] \otimes W[L] \end{bmatrix}.$$

The following theorem uses the notation established so far to show that the TDA is either ϵ -DP or ρ -zCDP, depending on whether a pure or approximate DP primitive mechanism is used, when either the conventional spine or the AIAN spine is used. The fact that geounits can be bypassed in the case of the optimized spine requires some modifications to this proof, which are described in Section 5. Note that, as in the proof below, the TDA takes the positive values in the set $\{\beta[l]\}_{l=1}^L$ as input, which define either the PLB proportions, in the case of pure DP, or the precision proportions, in the case of zCDP, for each geolevel.

Note that in the case of the conventional spine and the AIAN spine, there is no distinction between the workload matrix and the strategy matrix, as the TDA does not currently alter the per-geounit workloads $\{W[l]\}_l$, or the matrix representation of the spine B , in these cases prior to calling the primitive mechanisms.

Theorem 1. *Suppose the primitive mechanism $\mathcal{M}(\mathbf{x})$ outputs $\{(B[l] \otimes W[l])\mathbf{x} + \mathbf{y}[l]\}_{l=1}^L$, where each $W[l]$ is defined by vertically stacking the query group matrices $\{Q[i, l]\}_{i=1}^{q[l]}$ with $Q[i, l]$ of dimension $m[i, l] \times n$, \mathbf{x} is the true histogram cell counts, and $\mathbf{y}[l]$ is a vector of independent random variables.*

Also, let $\{\beta[l]\}_{l=1}^L$ be defined so that $\beta[l] \in \mathbb{R}_{++}$ and $\sum_l \beta[l]$. Likewise, for each geolevel $l \in \{1, \dots, L\}$, let each $\alpha[i, l] \in \{\alpha[i, l]\}_{i=1}^{q[l]}$, be defined so that $\alpha[i, l] \in \mathbb{R}_{++}$ and $\sum_i \alpha[i, l] = 1$, and let $\boldsymbol{\alpha}[l] := \text{stack}(\{\boldsymbol{\alpha}[i, l]_{m[i, l]}\}_i)$. Then we have the following.

- (1) *If $\mathbf{y}[l]$ is distributed as either $\mathbf{y}[l] \sim \text{Laplace}(\mathbf{0}, \text{diag}(\mathbf{2} \odot (\epsilon\beta[l]\boldsymbol{\alpha}[l])))$ or $\mathbf{y}[l] \sim \text{Laplace}_{\mathbb{Z}}(\mathbf{0}, \text{diag}(\mathbf{2} \odot (\epsilon\beta[l]\boldsymbol{\alpha}[l])))$, then both $\mathcal{M}(\cdot)$ and the TDA are ϵ -DP with respect to the neighbor definition $\{x, x' \in \mathcal{X}^d \cap \mathcal{G} \mid d_{\mathcal{H}}(x, x') = 2\}$.*
- (2) *If $\mathbf{y}[l]$ is distributed as either $\mathbf{y}[l] \sim \text{N}(\mathbf{0}, \text{diag}(\mathbf{1} \odot (\rho\beta[l]\boldsymbol{\alpha}[l])))$ or $\mathbf{y}[l] \sim \text{N}_{\mathbb{Z}}(\mathbf{0}, \text{diag}(\mathbf{1} \odot (\rho\beta[l]\boldsymbol{\alpha}[l])))$, then both $\mathcal{M}(\cdot)$ and the TDA are ρ -zCDP with respect to the neighbor definition $\{x, x' \in \mathcal{X}^d \cap \mathcal{G} \mid d_{\mathcal{H}}(x, x') = 2\}$.*

Proof. Note that for each fixed l , we have

$$B[l] \otimes W[l] = B[l] \otimes \text{stack}(\{Q[i, l]\}_i) = \text{stack}(\{B[l] \otimes Q[i, l]\}_i).$$

Block 2

FIGURE 1. An example of $B \otimes W$ is given above. In this example, B is given by $\text{vertical_stack}(\mathbf{1}_2^\top, I_2)$, which corresponds to the case in which there is one US geounit with two block geolevel child geounits. Each geounit contains a 2×2 histogram, and the linear queries in W are given by a total sum query ($\mathbf{1}_2^\top \otimes \mathbf{1}_2^\top$), the marginal query groups for each attribute ($I_2 \otimes \mathbf{1}_2^\top$ and $\mathbf{1}_2^\top \otimes I_2$), and the detailed cell query group ($I_2 \otimes I_2$). For each of the geounits, the total sum query is highlighted in green, the marginal query groups are highlighted in light and dark red, and the detailed cell query group is unhighlighted.

Since each $B[l] \otimes Q[i, l]$ satisfies the definition of a query group matrix, Lemma 5 implies that releasing the output of \mathcal{M}_l , with output defined as $(B[l] \otimes W[l])\mathbf{x} + \mathbf{y}[l]$ is $(\beta[l]\epsilon)$ -DP in the first case and $(\beta[l]\rho)$ -zCDP in the second case. Thus, sequential composition implies that the DP primitive mechanism $\mathcal{M}(\cdot)$ is $\sum_i \beta[l]\epsilon = \epsilon$ -DP in the first case and $\sum_i \beta[l]\rho = \rho$ -zCDP in the second case. Since both ρ -zCDP and ϵ -DP guarantees are invariant to post-processing, the TDA satisfies the same privacy guarantee as the primitive mechanisms. \square

In order to describe the spine optimization routines, we will require a distinction between the workload and the strategy matrix. Specifically, this strategy will maintain the same per-geounit queries $\{W\}_{i=1}^q$ and the same per-geounit proportions $\{\alpha[i, l]\}_{i, l}$ as the initial inputs. However, the strategy matrix will alter the matrix representation of the spine as well as the PLB or precision proportions allocated to each geounit. We will denote the matrix representation of this alternative spine as $A = \text{stack}(\{A[l]\}_l^L)$, which we require to satisfy the following properties. First, we will constrain our attention to spines that include all blocks, so A must have the same number of columns as B , which is $b(1, 1)$, and we require the lowest geolevel to be defined as these blocks, so $A[L] := I_{b(1, 1)}$. Second, the spine must include a US geounit, so we have $A[1] = \mathbf{1}_{b(1, 1)}^\top$. Third, the spine must include the same number of geolevels and be hierarchical, so, for geolevel $l \in \{1, \dots, L - 1\}$, we require each row of $A[l]$ to be equal to the sum of a subset of the rows of $A[l + 1]$. Since bypassing geounits will result in geounits within the same geolevel having different PLB or precision proportions, we will also use $\gamma[l, u]$ to denote the geolevel PLB or precision proportion for each geounit (l, u) , and $\boldsymbol{\gamma}$ to denote a vector composed of these values, using the same lexicographic ordering of the geounits described above. We will continue to use $\{\beta[l]\}_l^L$ to denote the per-geolevel PLB or precision proportions of the initial spine, and use $\boldsymbol{\beta}$ to denote the vector $\text{stack}(\{\beta[l]_{U[l]}\}_l^L)$.

Using the terminology from Section 2.4, we will introduce the rescaling vector $r \in \mathbb{R}_+^{m \sum_l U[l]}$ and the strategy matrix \tilde{S} , for later use in Section 5, as,

$$\tilde{S} := \text{diag}(r)(A \otimes W) = (\text{diag}(\gamma) \otimes \text{diag}(\alpha\epsilon))(A \otimes W) = (\text{diag}(\gamma)A) \otimes (\text{diag}(\alpha\epsilon)W),$$

in the case in which a pure ϵ -DP primitive Laplace mechanism is used and,

$$\tilde{S} := \text{diag}(r)(A \otimes W) = (\text{diag}(\sqrt{\gamma}) \otimes \text{diag}(\sqrt{\alpha\rho}))(A \otimes W) = (\text{diag}(\sqrt{\gamma})A) \otimes (\text{diag}(\sqrt{\alpha\rho})W),$$

in the case in which a ρ -zCDP primitive Gaussian mechanism is used. Also, let the stacked DP primitive mechanism answers be defined as $\tilde{\mathbf{z}} := \tilde{S}\mathbf{x} + \tilde{\mathbf{y}}$, where $\tilde{\mathbf{y}} = \text{diag}(r)\mathbf{y}$, $\mathbf{y} = \text{stack}(\{\mathbf{y}[\mathbf{l}]\}_{\mathbf{l}=1}^L\}$, and $\{\mathbf{y}[\mathbf{l}]\}_{\mathbf{l}=1}^L$ is defined as in the previous theorem. Then the OLS estimate for this strategy matrix can be expressed as,

$$(3) \quad \hat{\mathbf{x}} = (\tilde{S}^\top \tilde{S})^{-1} \tilde{S} \tilde{\mathbf{z}},$$

and the variance matrix of the output of the matrix mechanism is given by,

$$(4) \quad \text{Var}(V\hat{\mathbf{x}}) = V(\tilde{S}^\top \tilde{S})^{-1} V^\top.$$

3.1. Summary. There are two stages of the spine optimization routines, and each are described in the next two sections. The first stage takes the AIAN spine as input and then applies a method that is described in Section 4. This section introduces the OSE distance (OSD), which, for each OSE, is defined as the number of on-spine geounits that must be added or subtracted from one another in order to derive the OSE. We believe that defining geounits to minimize a function (such as the maximum or the mean) of the OSD values is a non-convex optimization problem, so Section 4 also provides a computationally efficient heuristic that reduces the OSD by redefining block groups and, when they are included on the spine, tract groups.

The output of the first stage is then updated again using a method that is described in Section 5. Specifically, this section provides a result that describes when bypassing a geounit on the spine results in every expected squared error of matrix mechanism either decreasing or remaining unchanged. Afterward, an algorithm is provided that uses this result to motivate a decision rule for when to bypass a geounit. The use of this decision rule within the TDA should also be regarded as a heuristic for two reasons. First, the output of the TDA is not defined using ordinary least squares, so this decision rule is not based on the actual variance matrix of the output of the TDA. Second, the TDA uses the random noise drawn from either of the discrete distributions, $\text{Laplace}_{\mathbb{Z}}(0, b)$ or $\text{N}_{\mathbb{Z}}(0, \sigma^2)$, rather than their continuous counterparts, $\text{Laplace}(0, b)$ and $\text{N}(0, \sigma^2)$, which are the distributions that motivate this decision rule. The TDA uses the discrete distributions $\text{Laplace}_{\mathbb{Z}}(0, b)$ and $\text{N}_{\mathbb{Z}}(0, \sigma^2)$ rather than $\text{Laplace}(0, b)$ and $\text{N}(0, \sigma^2)$ in part because they provide lower variance, and this same fact implies that using these distributions instead would alter the decision rule. However, this difference is primarily relevant when the PLB or precision allocated to a particular query of a geolevel is very large. For example, even when $\sigma^2 = 1$, using $\text{N}_{\mathbb{Z}}(0, \sigma^2)$, rather than $\text{N}(0, \sigma^2)$, provides a decrease in the variance of less than $3 \cdot 10^{-7}$, and when $\sigma^2 = 2$, this decrease in variance is less than $3 \cdot 10^{-15}$.⁴ For this reason, in most practical cases, this second departure from the TDA is unlikely to be as important as the first.

As described in Section 2.4, the norm in the literature on the matrix mechanism is to minimize the expected sum of squared error [11, 12]. In our independent experiments, this alternative decision rule resulted in many more geounits being bypassed, which resulted in a low expected sum of squared error objective function, but with high values for some individual expected squared errors. This problem persisted even after accounting for the disproportionate number of terms in this sum from the block level geounits by assigning each geolevel a PLB or precision proportion that was proportional to the inverse of the number of geounits in the geolevel. In contrast, the approach that we use is more conservative, in the sense that the input spine is only changed when doing so would either decrease or not changed the expected squared error of each query of the OLS estimate. This objective function aligns more closely with our goal when setting geolevel PLB or precision proportions, which is to ensure that the final query estimates for each geolevel satisfies a certain accuracy criterion. The only paper that we are aware of that takes a similar approach is [14].

⁴These values were estimated numerically in Mathematica with 100 digits of precision.

4. BRINGING OFF-SPINE ENTITIES CLOSER TO THE SPINE

This section describes how to redefine block groups and tract groups to bring OSEs closer to the spine. This is done by using a heuristic based on an objective function called the *off-spine entity distance* (OSED), which returns the minimum number of geounits that must be added or subtracted from one another to derive an OSE.⁵ This heuristic generally results in a reduction in the variance of estimates for these geographic regions, particularly when sufficient PLB or precision proportion is allocated to the geolevels that are being redefined.

Before moving onto defining a systematic way in which the OSEDs can be found for each OSE, we will define some additional notation. Specifically, let the set of OSEs be denoted by \mathcal{K} , an arbitrary encoding of the geographic spine by g , and the set of geounits that are children of geounit u of geolevel l by $J[l, u]$. Also, let $\{C_k(u)\}_{k \in \mathcal{K}}$, where $C_k : \mathbb{N}_+ \rightarrow \{0, 1\}$ denote a set of functions such that $C_k(u) = 1$ when the OSE $k \in \mathcal{K}$ contains the block geounit u and zero otherwise.

We will begin by choosing $k \in \mathcal{K}$ and finding the OSEDs for both k as well as its complement, which we will denote by k' , under the assumption that the only geolevel is the block geolevel. In this case, each block would contribute $c[k, L, u] := C_k(u)$ to the OSED of OSE k . Likewise, each block would contribute $c[k', L, u] := 1 - C_k(u)$ to the OSED of the complement of k .

If the block-group geolevel is added at this point, we could compose the intersection of a single block group and k in one of two ways. First, we could add all of the blocks to one another that are both inside of entity k and inside of the block group. This would result in the block-group u contributing $\sum_{v \in J(L-1, u)} c[k, l, v]$ to the OSED of k . On the other hand, we could also take all of the geographic extent that the block group occupies and then subtract off the geographic region of the blocks in the complement of k . This would result in this block group contributing $1 + \sum_{v \in J(L-1, u)} c[k', l, v]$ to the OSED of k . Note that an additional one is added in this case because of the additional step of subtracting the complement of k in the block group from the block group itself. Since OSED is defined as the *minimum* number of geounits that must be added or subtracted to one another to define an entity, we will choose the option that results in a smaller value. Since similar derivations can be carried out for the complement of k , by symmetry, we have,

$$(5) \quad c[k, L-1, u] := \min \left\{ \sum_{v \in J(L-1, u)} c[k, l, v], 1 + \sum_{v \in J(L-1, u)} c[k', l, v] \right\}$$

$$(6) \quad c[k', L-1, u] := \min \left\{ \sum_{v \in J(L-1, u)} c[k', l, v], 1 + \sum_{v \in J(L-1, u)} c[k, l, v] \right\}.$$

Note that (5) and (6) provide a closed form solution for $\{(c[k, L-1, u], c[k', L-1, u])\}_u$ in terms of $\{(c[k, L, u], c[k', L, u])\}_u$. Similar logic can be repeated to derive the following recursive system of equations.

$$(7) \quad c[k, l-1, u] := \min \left\{ \sum_{v \in J(l-1, u)} c[k, l, v], 1 + \sum_{v \in J(l-1, u)} c[k', l, v] \right\}$$

$$(8) \quad c[k', l-1, u] := \min \left\{ \sum_{v \in J(l-1, u)} c[k', l, v], 1 + \sum_{v \in J(l-1, u)} c[k, l, v] \right\}$$

Since all entities are assumed to be contained within the US, the final OSED for entity k can be found by applying these recursions to the root geounit and defining this OSED as $c[k, 1, 1]$. Afterward, our final

⁵Our use of the term “off-spine entities” refers to geographic entities that may be off of the spine, but we do not assume that each OSE has a geographic extent that differs from each (on-spine) geounit. An implication of this definition of OSED is that, when the geographic extent of an OSE is identical to a geounit on the spine, its OSED is equal to one.

objective function is defined by a reduce operation, such as a function that returns the mean or maximum OSED. This is summarized in Algorithm 1.

Algorithm 1: OSEDs_Reduced($g, \mathcal{K}, \{C_k(\cdot)\}_k, h(\cdot), L$)

```

for  $k \in \mathcal{K}$  do
  for  $u \in \text{Geounits\_in\_Geolevel}(L, g)$  do
     $c[k, L, u] \leftarrow C_k(u)$ 
     $c[k', L, u] \leftarrow 1 - C_k(u)$ 
  for  $l \in \{L - 1, L - 2, \dots, 1\}$  do
    for  $u \in \text{Geounits\_in\_Geolevel}(l, g)$  do
       $x \leftarrow \sum_{v \in \text{Children}(u, l, g)} c[k, l + 1, v]$ 
       $y \leftarrow \sum_{v \in \text{Children}(u, l, g)} c[k', l + 1, v]$ 
       $c[k, l, u] \leftarrow \min \{x, y + 1\}$ 
       $c[k', l, u] \leftarrow \min \{y, x + 1\}$ 
return  $h(\{c[k, 1, 1]\}_{k \in \mathcal{K}})$ 

```

In the most general setting, in which the OSEs are not necessarily disjoint, formulating an algorithm that redefines block groups and tract groups in order to minimize the OSEDs with a polynomial time complexity appears to be a difficult problem because of the similarity of this optimization problem to a covering problem. For this reason, Algorithm 2 describes a greedy approach to approximate the optimal redefinitions of tract groups in a computationally tractable manner. In contrast, block groups are redefined by combining blocks within a given tract, and within the same intersection of the OSEs. As described in the code below, each redefined block group is composed of up to $\sqrt{n} + \text{fanout_cutoff}$ blocks, where n is the blocks in the redefined block group's parent tract and fanout_cutoff is a user choice parameter. This choice is motivated by the fact that the smallest maximum fanout value among a given tract and its child geounits is $\lceil \sqrt{n} \rceil$, where $\lceil \cdot \rceil$ denotes the ceiling function. For example, for a tract with 100 block geounit descendants, redefining its children by 10 redefined block group child geounits, each with 10 block child geounits, would result in the lowest possible maximum fanout of 10 among these 11 geounits, so the redefined block groups within this tract would contain no more than $10 + \text{fanout_cutoff}$ blocks in this case. Note that a similar approach, is used to define the maximum number of tracts within a tract group in Algorithm 2.

This algorithm also uses $\mathbf{x} \preceq_{\text{lexicographic}} \mathbf{y}$, where $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, to denote the lexicographic less than or equal to partial ordering, which is defined as \perp when $\mathbf{x} \neq \mathbf{y}$ and the first index i for which \mathbf{x}_i and \mathbf{y}_i differ satisfies $\mathbf{x}_i > \mathbf{y}_i$, and \top otherwise.

Note that Algorithm 2 does not alter the PLB or precision proportions of the input spine, which is the AIAN spine. The next section describes the Algorithm used to update these proportions, along with the spine that is output from Algorithm 2, in the second spine optimization stage.

5. A PARETO FRONTIER OF GEOUNIT DEFINITIONS

This section uses a matrix mechanism to provide a decision rule for when it is best to bypass a geounit. To do so, we will constrain our attention to DP primitive mechanisms that use noise drawn from the continuous distributions $N(\cdot)$ and $\text{Laplace}(\cdot)$. We will also suppose that the matrix B is the matrix representation of the spine that is used as input of this method. In the case of the TDA, this spine is formed using the output of Algorithm 2.

It is also worth explicitly stating how we define the operation of bypassing a parent geounit. We define the operation of bypassing a parent geounit with c children, each with equal PLB or precision proportions, by, 1) creating c geounits in the geolevel of the parent, each with a geolevel proportion given by the sum of proportion allocated to the parent and one of the children, 2) defining the single child of each of these c new geounits by one of the children, 3) removing the old parent geounit, 4) redefining the geolevel proportion of each child to be zero. Thus, even though we call this operation “bypassing a parent,” this operation actually moves the geolevel PLB or precision proportion to a higher geolevel. This ensures that this operation does not change the total number of geolevels, and since the TDA fixes the final estimates in a top-down manner, so that the consistency with parent constraints are satisfied, this also ensures that the entire share of the geolevel PLB or precision allocations are used in cases in which a parent geounit has only one child geounit. While this is the definition of this operation used within the TDA, the decision rules developed in this section

Algorithm 2: `Redefine_Block_Groups_and_Tract_Groups($g, \mathcal{K}, \{C_k(\cdot)\}_k$)`

```

// Within each tract, redefine block groups by combining groups of
 $\sqrt{n} + \text{fanout\_cutoff}$  blocks in the intersections of the same OSEs, where  $n$  is the
number of blocks in the tract.
// Initialize tract groups so that they each have one child Tract.
current_OSEDs  $\leftarrow$  OSEDs_Reduced( $g, \mathcal{K}, \{C_k(\cdot)\}_k, \text{Sort\_Descending}(\cdot)$ )
for  $i \in \{1, \dots\}$  do
   $g\_changed \leftarrow \perp$ 
  for county  $\in$  Counties( $g$ ) do
     $n \leftarrow$  Number_of_tracts_in_county(county)
    for  $u, v \in$  Children(county) do
      if  $\text{Card}(\text{Children}(u) \cup \text{Children}(v)) > \sqrt{n} + \text{fanout\_cutoff}$  then
         $\perp$  continue
       $g' \leftarrow$  Combine_Siblings( $u, v, g$ )
      test_OSEDs  $\leftarrow$  OSEDs_Reduced( $g', \mathcal{K}, \{C_k(\cdot)\}_k, \text{Sort\_Descending}(\cdot)$ )
      if test_OSEDs  $\preceq_{\text{lexicographic}}$  current_OSEDs then
         $g \leftarrow g'$ 
        current_OSEDs  $\leftarrow$  test_OSEDs
         $g\_changed \leftarrow \top$ 
    if not  $g\_changed$  then
       $\perp$  break
return  $g$ 

```

only depend on properties of $\tilde{S}^\top \tilde{S}$, and using this definition of the bypass operation impacts this matrix in the same way as simply reallocating the geolevel PLB or precision proportion of the parent geounit to the children. For this reason, we motivate the decision rules described in this section on this simpler definition of the bypass operation.

Using the notation from 3, recall that the expected squared errors of the output of the matrix mechanism with the strategy matrix \tilde{S} are given by the diagonal of $\text{Var}(V\hat{\mathbf{x}})$, as defined in (4). The next result describes a case in which each of these expected squared errors can be decreased, or remain unchanged, by bypassing a parent. In cases in which the initial PLB proportion of a parent and its children are equal, this result simply implies that accuracy can be improved by bypassing over the parent geounit when it has less than or equal to three child geounits. The decision rule that used for the case in which ρ -zCDP primitive Gaussian mechanisms are used will be discussed after the proof.

Theorem 2. *Suppose ϵ -DP primitive Laplace mechanisms are used and that the per-geolevel query strategies and query PLB proportions are the same in each geolevel. Also suppose that the geolevel PLB allocated to each of the c children of geounit $(l, 1)$ are equal (ie: $\gamma[l+1, u] = \gamma[l+1, v]$ for all $u, v \in \{1, \dots, c\}$). If $\gamma[l+1, 1] \geq (c-1)\gamma[l, 1]/2$, then, for any W and $\{\alpha[i]\}_i$, reallocating the PLB assigned to geounit $(l, 1)$ to its children will either decrease or leave unchanged each of the diagonal elements of $\text{Var}(V\hat{\mathbf{x}})$.*

Proof. Let $\{\gamma_0[l, u]\}_{l,u}$ and $\{\gamma_1[l, u]\}_{l,u}$ denote the geounit PLB proportions before and after reallocation, respectively. Likewise, let $\hat{\mathbf{x}}_0$ and $\hat{\mathbf{x}}_1$ denote the OLS estimate before and after reallocation, respectively. Also, for the symmetric matrices $C, D \in \mathbb{R}^{n \times n}$ we will use $C \leq D$ to denote the condition that $C - D$ is negative semidefinite and $C \leq 0$ to denote the condition that C is negative semidefinite. The variance matrix of the OLS estimate before (respectively, after) bypassing geounit $(l, 1)$ is proportional to,

$$\begin{aligned}
\text{Var}(\hat{\mathbf{x}}_i) &= ((\text{diag}(\boldsymbol{\gamma}_i)A \otimes W)^\top (\text{diag}(\boldsymbol{\gamma}_i)A \otimes W))^{-1} \\
&= ((A^\top \text{diag}(\boldsymbol{\gamma}_i) \otimes W^\top) (\text{diag}(\boldsymbol{\gamma}_i)A \otimes W))^{-1} \\
&= ((A^\top \text{diag}(\boldsymbol{\gamma}_i^2)A) \otimes (W^\top W))^{-1} \\
&= (A^\top \text{diag}(\boldsymbol{\gamma}_i^2)A)^{-1} \otimes (W^\top W)^{-1},
\end{aligned}$$

where $i = 0$ (respectively, $i = 1$). We will prove the sufficient condition that $\text{Var}(\hat{\mathbf{x}}_1) \leq \text{Var}(\hat{\mathbf{x}}_0)$. Given the variance matrix of the OLS estimator above, this condition is equivalent to,

$$\begin{aligned} \text{Var}(\hat{\mathbf{x}}_1) < \text{Var}(\hat{\mathbf{x}}_0) &\iff \\ (A^\top \text{diag}(\gamma_1^2)A)^{-1} \otimes (W^\top W)^{-1} &\leq (A^\top \text{diag}(\gamma_0^2)A)^{-1} \otimes (W^\top W)^{-1} \iff \\ ((A^\top \text{diag}(\gamma_1^2)A)^{-1} - (A^\top \text{diag}(\gamma_0^2)A)^{-1}) &\otimes (W^\top W)^{-1} \leq 0. \end{aligned}$$

Since we assume that $W^\top W$ is positive definite, this condition holds if and only if,

$$\begin{aligned} ((A^\top \text{diag}(\gamma_1^2)A)^{-1} - (A^\top \text{diag}(\gamma_0^2)A)^{-1}) &\leq 0 \iff \\ (A^\top \text{diag}(\gamma_1^2)A)^{-1} &\leq (A^\top \text{diag}(\gamma_0^2)A)^{-1} \iff \\ A^\top \text{diag}(\gamma_1^2)A &\geq A^\top \text{diag}(\gamma_0^2)A \iff \\ A^\top \text{diag}(\gamma_1^2 - \gamma_0^2)A &\geq 0 \end{aligned}$$

Note that the only elements of γ_1 that are not equal to γ_0 can be defined in terms of γ_0 by $\gamma_1[l+1, u] = \gamma_0[l+1, u] + \gamma_0[l, 1]$ for all $u \in \{1, \dots, c\}$ and $\gamma_1[l, 1] = 0$. Thus, $A^\top \text{diag}(\gamma_0^2 - \gamma_1^2)A$ is a block matrix with a single block that is nonzero. Let $n[u] := b[l+1, u]$ for $u \in \{1, \dots, c\}$. This block is of dimension $b[l, 1] \times b[l, 1]$, and is given by,

$$D := \begin{bmatrix} 2\gamma_0[l+1, 1]\gamma_0[l, 1]\mathbf{1}_{n[1]}\mathbf{1}_{n[1]}^\top & -\gamma_0[l, 1]^2\mathbf{1}_{n[1]}\mathbf{1}_{n[2]}^\top & -\gamma_0[l, 1]^2\mathbf{1}_{n[1]}\mathbf{1}_{n[3]}^\top & \cdots \\ -\gamma_0[l, 1]^2\mathbf{1}_{n[2]}\mathbf{1}_{n[1]}^\top & 2\gamma_0[l+1, 2]\gamma_0[l, 1]\mathbf{1}_{n[2]}\mathbf{1}_{n[2]}^\top & -\gamma_0[l, 1]^2\mathbf{1}_{n[2]}\mathbf{1}_{n[3]}^\top & \\ -\gamma_0[l, 1]^2\mathbf{1}_{n[3]}\mathbf{1}_{n[1]}^\top & -\gamma_0[l, 1]^2\mathbf{1}_{n[3]}\mathbf{1}_{n[2]}^\top & 2\gamma_0[l+1, 3]\gamma_0[l, 1]\mathbf{1}_{n[3]}\mathbf{1}_{n[3]}^\top & \\ \vdots & & & \ddots \end{bmatrix}.$$

This matrix only has c unique columns, and the vectors $\{t_i\}_i^c$, where $t_i := (\mathbf{0}_{a[i]}^\top, \mathbf{1}_{n[i]}^\top/n[i], \mathbf{0}_{b[i]}^\top)^\top$, $a[i] := \sum_{j=1}^{i-1} n[j]$ and $a[i] := \sum_{j=i+1}^c n[j]$, for $i \in \{1, \dots, c\}$, provide an orthogonal basis for the span of these columns. Let $T := \text{horizontal_stack}(\{t_i\}_i)$. Thus,

$$\begin{aligned} D \geq 0 &\iff TDT^\top \geq 0 \iff \\ \begin{bmatrix} 2\gamma_0[l+1, 1]\gamma_0[l, 1] & -\gamma_0[l, 1]^2 & -\gamma_0[l, 1]^2 & \cdots \\ -\gamma_0[l, 1]^2 & 2\gamma_0[l+1, 2]\gamma_0[l, 1] & -\gamma_0[l, 1]^2 & \\ -\gamma_0[l, 1]^2 & -\gamma_0[l, 1]^2 & 2\gamma_0[l+1, 3]\gamma_0[l, 1] & \\ \vdots & & & \ddots \end{bmatrix} &\geq 0 \iff \\ \text{diag}(\mathbf{1}_r(2\gamma_0[l+1, 1]\gamma_0[l, 1] + \gamma_0[l, 1]^2)) - \mathbf{1}_r\mathbf{1}_r^\top \gamma_0[l, 1]^2 &\geq 0. \end{aligned}$$

Since $\gamma_0[l, u] \geq 0$ for all l, u , the eigenvector corresponding to the smallest eigenvalue is $\mathbf{1}_r$, so this matrix is positive semidefinite when,

$$2\gamma_0[l+1, 1]\gamma_0[l, 1] \geq (c-1)\gamma_0[l, 1]^2.$$

Since $(l, 1)$ was not bypassed in our initial PLB allocation, $\gamma_0[l, 1] \neq 0$, so we have,

$$\gamma_0[l+1, 1] \geq (c-1)\gamma_0[l, 1]/2.$$

□

Remark 1. Consider two cases in which the only query in W is a total population query. First, if the parent is not bypassed, we could construct unbiased estimates of the total population of the parent by either observing the DP answer for the parent directly, which has a variance of $2/\gamma[l, 1]^2$, or by summing the DP answers of the children together, which has a variance of $2c/\gamma[l + 1, 1]^2$. The mean with inverse variance weighting provides the linear combination of these estimates with the lowest possible variance of $2c/(\gamma[l, 1]^2 + \gamma[l + 1, 1]^2)$ in this case. Second, if we did bypass the parent, we could estimate the total population query for the parent by summing the total population of the children, which would have a variance of $2c/(\gamma[l + 1, 1] + \gamma[l, 1])^2$ in this case. The theorem above can be viewed as a statement that limiting our attention to a single total population query, and to only the parent and its children, in this way is without loss of generality, at least for the purpose of finding the cases in which bypassing the parent does not increase the expected error for any query in any geounit. This is because $2c/(\gamma[l, 1]^2 + \gamma[l + 1, 1]^2) \geq 2c/(\gamma[l + 1, 1] + \gamma[l, 1])^2$ if and only if $\gamma[l + 1, 1] \geq (c - 1)\gamma[l, 1]/2$, which is the same requirement given in the statement of the theorem. \square

Remark 2. This theorem may be of independent interest in the DP literature because other authors have already considered strategy matrices that have a hierarchical structure that is analogous to the matrix representation of the spine A above, and this result can be used to narrow the search space of the set of hierarchical strategy matrices considered when choosing a strategy matrix with this property [9, 11]. For example, when using the OLS approach described by [9] with PLB proportions that are the same for each level of the hierarchy and with the children of each non-leaf node defined by either two or three sub-intervals of the range of the parent node, this result implies that the expected squared error of an arbitrary linear query can be reduced by increasing the number of sub-intervals used to define these child nodes. \square

One can use a similar technique to show that, in the case in which ρ -zCDP primitive Gaussian mechanisms are used to define \mathbf{y} , bypassing a parent will increase at least one diagonal element of $\text{Var}(V\hat{\mathbf{x}})$ whenever the parent has two or more children, and the diagonal elements of $\text{Var}(V\hat{\mathbf{x}})$ will remain unchanged whenever the parent has only one child. In part for this reason, our decision rule for the case in which ρ -zCDP primitive Gaussian mechanisms are used is simply to bypass parent geounits with only one child. However, given the top-down manner in which the TDA fixes estimates to ensure consistency with the estimates of the parent geounits, the estimates of a child geounit are fixed by those of the parent geounit whenever the parent only has one child geounit. Thus, we need not solely rely on the change in the diagonal elements of $\text{Var}(V\hat{\mathbf{x}})$ to motivate the decision rule for this case; an alternative motivation is provided in the following observation. Note that the decision rule provided in Theorem 2 results in at least the same number of geounits being bypassed, since, whenever $c = 1$, the condition in the statement of the theorem becomes $\gamma[l + 1, 1] \geq 0$, and we require each $\gamma[l, u]$ to be non-negative.

Observation 1. *The DP primitive mechanism answers for each child geounit that does not have a sibling geounit are not used. Thus, the variance of the DP primitive mechanisms output that are actually used to construct the final estimates in the TDA can be decreased by bypassing all parent geounits with only one child.*

Algorithm 3 summarizes how both of these decision rules are used within the spine optimization routines of the TDA. Note that this algorithm starts at the block group geolevel rather than the US, which ensures that no remaining geounits can be bypassed after only one pass over the spine.

Algorithm 3: Move_Spine_to_Pareto_Frontier($B, \{\beta[l, u]\}_{l,u}, \text{pure_DP} \in \{\top, \perp\}$)

```

for  $l \in \{L - 1, L - 2, \dots, 1\}$  do
  for parent in geolevel  $l$  do
     $\beta_{\text{child}} \leftarrow \min_{u \in \text{Children}(\text{parent})} \beta[l + 1, u]$ 
     $\beta_{\text{parent}} \leftarrow \beta[l, \text{parent}]$ 
     $c \leftarrow \text{Card}(\text{Children}(\text{parent}))$ 
    if  $\text{pure\_DP} \wedge \beta_{\text{child}} \geq (c - 1)\beta_{\text{parent}}/2$  then
       $B, \{\beta[l, u]\}_{l,u} \leftarrow \text{Bypass\_Parent\_Geounit}(\text{parent}, B, \{\beta[l, u]\}_{l,u})$ 
    else if  $c = 1$  then
       $B, \{\beta[l, u]\}_{l,u} \leftarrow \text{Bypass\_Parent\_Geounit}(\text{parent}, B, \{\beta[l, u]\}_{l,u})$ 
return  $B, \{\beta[l, u]\}_{l,u}$ 

```

5.1. The impact of Spine Optimization on the Privacy Guarantees of TDA. Note that the using the TDA with the spine that is output from Algorithm 2 does not alter the privacy guarantees of the TDA because the same arguments used in the proof of Theorem 1 apply in this case as well. However, this cannot be said for the spine that is output from Algorithm 3 when at least one geounit is bypassed. The following theorem generalizes the argument used in 1 to show that using the spine output from Algorithm 3 within the TDA does not impact the privacy guarantees.

Theorem 3. *Suppose the primitive mechanism $\mathcal{M}(\mathbf{x})$ outputs $\{(A[l]_{u,\cdot} \otimes W[l])\mathbf{x} + \mathbf{y}[l, u]\}_{l,u}$, where each $A[l] \in \{0, 1\}^{U[l] \times b[1,1]}$ is the matrix representation of geolevel $l \in \{1, \dots, L\}$ of the spine output from the spine optimization routines described in Sections 4 and 5, each $W[l]$ is defined by vertically stacking the query group matrices $\{Q[i, l]\}_{i=1}^{q[l]}$ with $Q[i, l]$ of dimension $m[i, l] \times n$, \mathbf{x} is the true histogram cell counts, and $\mathbf{y}[l, u]$ is a vector of either independent random variables or has all elements equal to ∞ .*

Also, let the input geolevel PLB or precision proportions $\{\beta[l]\}_l$ be defined so that $\beta[l] \in \mathbb{R}_{++}$ and $\sum_l \beta[l]$, and let $\{\gamma[l, u]\}_{l,u}$ denote the resulting geolevel PLB or precision proportions that is output from the spine optimization routines. Likewise, for each geolevel $l \in \{1, \dots, L\}$, let each $\alpha[i, l] \in \{\alpha[i, l]\}_{i=1}^{q[l]}$, be defined so that $\alpha[i, l] \in \mathbb{R}_{++}$ and $\sum_i \alpha[i, l] = 1$, and let $\boldsymbol{\alpha}[l] := \text{stack}(\{\boldsymbol{\alpha}[i, l]_{m[i,l]}\}_i)$. Then we have the following.

- (1) *If $\mathbf{y}[l, u] = \infty$ when $\gamma[l, u] = 0$, and is distributed as either $\mathbf{y}[l, u] \sim \text{Laplace}(\mathbf{0}, \text{diag}(\mathbf{2} \odot (\epsilon \gamma[l, u] \boldsymbol{\alpha}[l])))$ or $\mathbf{y}[l, u] \sim \text{Laplace}_{\mathbb{Z}}(\mathbf{0}, \text{diag}(\mathbf{2} \odot (\epsilon \gamma[l, u] \boldsymbol{\alpha}[l])))$, when $\gamma[l, u] > 0$, then both $\mathcal{M}(\cdot)$ and the TDA are ϵ -DP with respect to the neighbor definition $\{x, x' \in \mathcal{X}^d \cap \mathcal{G} \mid d_{\mathcal{H}}(x, x') = 2\}$.*
- (2) *If $\mathbf{y}[l, u] = \infty$ when $\gamma[l, u] = 0$, and is distributed as either $\mathbf{y}[l, u] \sim \mathcal{N}(\mathbf{0}, \text{diag}(\mathbf{1} \odot (\rho \gamma[l, u] \boldsymbol{\alpha}[l])))$ or $\mathbf{y}[l, u] \sim \mathcal{N}_{\mathbb{Z}}(\mathbf{0}, \text{diag}(\mathbf{1} \odot (\rho \gamma[l, u] \boldsymbol{\alpha}[l])))$, when $\gamma[l, u] > 0$, then both $\mathcal{M}(\cdot)$ and the TDA are ρ -zCDP with respect to the neighbor definition $\{x, x' \in \mathcal{X}^d \cap \mathcal{G} \mid d_{\mathcal{H}}(x, x') = 2\}$.*

Proof. For $x \in \mathcal{X}^d \cap \mathcal{G}$, let the set of datasets $x' \in \mathcal{X}^d \cap \mathcal{G}$ that differ from x on a single entry be denoted by $\mathcal{N}(x)$. Also, let $T[l] := \{u \in \mathbb{Z}_{++} \mid u < U[l] \wedge \gamma[l, u] > 0\}$. Note that the output of all of the DP primitive mechanisms is observationally equivalent the set of finite output elements, or $\{(A[l]_{u,\cdot} \otimes W[l])\mathbf{x} + \mathbf{y}[l, u]\}_{l,u \in T[l]}$, because, independently of the data, the remaining DP primitive answers are infinite with probability one. Thus, without loss of generality, we can restrict our attention to this alternative mechanism. Let $\widehat{A}[l] := A[l]_{T[l],\cdot}$, and $\widehat{\gamma}[l] := \text{stack}(\{\gamma[l, u]\}_{l,u \in T[l]})$, so the strategy matrix for this alternative mechanism can be written as,

$$D := \text{stack}(\{\widehat{A}[l] \otimes W[l]\}_l).$$

In the case of the first result of the theorem, the noise for this mechanism is distributed as either $\hat{\mathbf{y}} \sim \text{Laplace}(\mathbf{0}, \text{diag}(\hat{\mathbf{b}}))$ or $\hat{\mathbf{y}} \sim \text{Laplace}_{\mathbb{Z}}(\mathbf{0}, \text{diag}(\hat{\mathbf{b}}))$, where $\hat{\mathbf{b}} := \text{stack}(\{\hat{\mathbf{b}}[l]\}_l)$ and $\mathbf{b}[l] := \mathbf{2} \odot (\epsilon(\widehat{\gamma}[l] \otimes \boldsymbol{\alpha}[l]))$. Thus, we will show the following condition, which, by the first result in Lemma 3, is a sufficient condition,

$$(9) \quad \max_{x \in \mathcal{X}^d \cap \mathcal{G}, x' \in \mathcal{N}(x)} \sum_i \left| D_{i,\cdot} (x - x') / \hat{\mathbf{b}}_i \right| \leq \epsilon.$$

Starting from the left hand side of this inequality, we have,

$$(10) \quad \begin{aligned} \max_{x \in \mathcal{X}^d \cap \mathcal{G}, x' \in \mathcal{N}(x)} \sum_i \left| \left(\text{diag}(\mathbf{1} \odot \hat{\mathbf{b}}) D \right)_{i,\cdot} (x - x') \right| &\leq 2 \max_j \sum_i \left(\text{diag}(\mathbf{1} \odot \hat{\mathbf{b}}) D \right)_{i,j} = \\ &= 2 \max_j \sum_i \text{stack} \left(\left(\text{diag}(\epsilon(\widehat{\gamma}[l] \otimes \boldsymbol{\alpha}[l]) / 2) (\widehat{A}[l] \otimes W[l]) \right)_l \right)_{i,j} = \\ &= \epsilon \max_j \sum_l \sum_i \left(\text{diag}(\widehat{\gamma}[l]) \widehat{A}[l] \otimes \text{diag}(\boldsymbol{\alpha}[l]) W[l] \right)_{i,j}. \end{aligned}$$

Note that each of the row sums of $\text{diag}(\boldsymbol{\alpha}[l]) W[l]$ (i.e.: the elements of the vector $W[l]^\top \text{diag}(\boldsymbol{\alpha}[l]) \mathbf{1} = W[l]^\top \boldsymbol{\alpha}[l]$) are equal to 1 because $\sum_k Q[i, l]_{k,\cdot} = \mathbf{1}^\top$ and $\sum_k \alpha[k, l] = 1$. Thus, since each column j of $\text{diag}(\widehat{\gamma}[l]) \widehat{A}[l]$ contains at most one nonzero value, we have,

$$\begin{aligned} & \epsilon \max_j \sum_l \sum_i \left((\text{diag}(\hat{\gamma}[l]) \hat{A}[l]) \otimes (\text{diag}(\alpha[l]) W[l]) \right)_{i,j} = \\ & \epsilon \max_j \sum_l \sum_i \left(\text{diag}(\hat{\gamma}[l]) \hat{A}[l] \right)_{i,j} = \epsilon \max_j \sum_i \left(\text{diag}(\hat{\gamma}) \hat{A} \right)_{i,j}, \end{aligned}$$

where $\hat{\gamma} := \text{stack}(\{\hat{\gamma}[l]\}_l)$. Note that $\sum_i \left(\text{diag}(\hat{\gamma}) \hat{A} \right)_{i,j}$ is equal to the sum of the geolevel PLB proportions along a path from the US geounit to the block geounit j . Since the bypass operation used within Algorithm 3 does not change this sum, and its initial value is $\sum_l \beta[l] = 1$, we have

$$\epsilon \max_j \sum_i \left(\text{diag}(\hat{\gamma}) \hat{A} \right)_{i,j} = \epsilon \sum_l \beta[l] = \epsilon,$$

which implies inequality (9).

Similar logic also implies the second result of the theorem. Specifically, in this case we can use the second result of Lemma 3, and the fact that for each $x \in \mathcal{X}^d \cap \mathcal{G}$ and $x' \in N(x)$ we have $(D_{i,\cdot}(x-x'))^2 = |D_{i,\cdot}(x-x')|$, to derive the sufficient condition,

$$(11) \quad \max_{x \in \mathcal{X}^d, x' \in N(x)} \sum_i |D_{i,\cdot}(x-x')| / \hat{\sigma}_i^2 \leq 2\rho,$$

where $\hat{\sigma}^2 := \text{stack}(\{\hat{\sigma}^2[l]\}_l)$ and $\hat{\sigma}^2[l] := \mathbf{1} \odot (\rho(\hat{\gamma}[l] \otimes \alpha[l]))$. This inequality follows from,

$$(12) \quad \begin{aligned} & \max_{x \in \mathcal{X}^d \cap \mathcal{G}, x' \in N(x)} \sum_i |D_{i,\cdot}(x-x')| / \hat{\sigma}_i^2 \leq 2 \max_j \sum_i (\text{diag}(\mathbf{1} \odot \hat{\sigma}^2) D)_{i,j} = \\ & 2\rho \max_j \sum_i (\text{diag}(\hat{\gamma}[l] \otimes \alpha[l]) D)_{i,j}. \end{aligned}$$

Since this last value is equal to the value of (10) multiplied by $2\rho/\epsilon$, and the logic above implies the value of (10) is equal to ϵ , we have,

$$2\rho \max_j \sum_i (\text{diag}(\hat{\gamma}[l] \otimes \alpha[l]) D)_{i,j} = \epsilon \cdot (2\rho/\epsilon) = 2\rho,$$

which implies the sufficient condition (11). \square

6. CONCLUSION

This document describes both stages of the spine optimization routines used in the TDA. The first stage brings OSEs closer to the spine by redefining block groups and tract groups, and the second stage bypasses geounits with low-fanouts using a decision rule that is motivated by the expected squared errors of the ordinary least squares estimator. This final section also provides a result that spine optimization does not alter the privacy guarantees of the TDA.

REFERENCES

- [1] John Abowd, Daniel Kifer, Brett Moran, Robert Ashmead, Philip Leclerc, William Sexton, Simson Garfinkel, and Ashwin Machanavajjhala. Census topdown: Differentially private data, incremental schemas, and consistency with public knowledge. Technical report, Technical report, US Census Bureau, 2019.
- [2] Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In *Theory of Cryptography Conference*, pages 635–658. Springer, 2016.
- [3] Clément L Canonne, Gautam Kamath, and Thomas Steinke. The discrete gaussian for differential privacy. In H. Larochelle, M. Ranzato, R. Hadsell, M. F. Balcan, and H. Lin, editors, *Advances in Neural Information Processing Systems*, volume 33, pages 15676–15688. Curran Associates, Inc., 2020.
- [4] Clément L. Canonne, Gautam Kamath, and Thomas Steinke. The discrete gaussian for differential privacy. Technical report, 2021. arXiv extended version arXiv:2012.00135.

- [5] Jinshuo Dong, Aaron Roth, and Weijie J Su. Gaussian differential privacy. *arXiv preprint arXiv:1905.02383*, 2019.
- [6] Cynthia Dwork, Krishnaram Kenthapadi, Frank McSherry, Ilya Mironov, and Moni Naor. Our data, ourselves: Privacy via distributed noise generation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 486–503. Springer, 2006.
- [7] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.
- [8] Arpita Ghosh, Tim Roughgarden, and Mukund Sundararajan. Universally utility-maximizing privacy mechanisms. *SIAM Journal on Computing*, 41(6):1673–1693, 2012.
- [9] Michael Hay, Vibhor Rastogi, Gerome Miklau, and Dan Suciu. Boosting the accuracy of differentially private histograms through consistency. *Proceedings of the VLDB Endowment*, 3(1), 2010.
- [10] Daniel Kifer and Ashwin Machanavajjhala. No free lunch in data privacy. In *Proceedings of the 2011 ACM SIGMOD International Conference on Management of data*, pages 193–204, 2011.
- [11] Chao Li, Michael Hay, Vibhor Rastogi, Gerome Miklau, and Andrew McGregor. Optimizing linear counting queries under differential privacy. In *Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 123–134, 2010.
- [12] Ryan McKenna, Gerome Miklau, Michael Hay, and Ashwin Machanavajjhala. Optimizing error of high-dimensional statistical queries under differential privacy. *Proceedings of the VLDB Endowment*, 11(10):1206–1219, 2018.
- [13] Larry Wasserman and Shuheng Zhou. A statistical framework for differential privacy. *Journal of the American Statistical Association*, 105(489):375–389, 2010.
- [14] Yingtai Xiao, Zeyu Ding, Yuxin Wang, Danfeng Zhang, and Daniel Kifer. Optimizing fitness-for-use of differentially private linear queries. *arXiv preprint arXiv:2012.00135*, 2020.