On Optimal Differentially Private Mechanisms for Count-Range Queries

Chen Zeng
University of Wisconsin-Madison
zeng@cs.wisc.edu

Jin-Yi Cai
University of Wisconsin-Madison
jyc@cs.wisc.edu

Pinyan Lu
Microsoft Research Asia
pinyanl@microsoft.com

Jeffrey F. Naughton
University of Wisconsin-Madison
naughton@cs.wisc.edu

ABSTRACT

While there is a large and growing body of literature on differentially private mechanisms for answering various classes of queries, to the best of our knowledge "count-range" queries have not been studied. These are a natural class of queries that ask "is the number of rows in a relation satisfying a given predicate between two integers θ_1 and θ_2?" Such queries can be viewed as a simple form of SQL "having" queries. We begin by developing a provably optimal differentially private mechansim for count-range queries for a single consumer. For count queries (in contrast to count-range queries), Ghosh et al. [9] have provided a differentially private mechanism that simultaneously maximizes utility for multiple consumers. This raises the question of whether such a mechanism exists for count-range queries. We prove that the answer is no — for count range queries, no such mechanism exists. However, perhaps surprisingly, we prove that such a mechanism does exist for "threshold" queries, which are simply count-range queries for which either $\theta_1 = 0$ or $\theta_2 = +\infty$. Furthermore, we prove that this mechanism is a two-approximation for general count-range queries.

1. INTRODUCTION

Recently, concomitant with the increasing ability to collect personal data, privacy has become a major concern. In response to this concern, the research community has devoted considerable attention to differentially private mechanisms for various classes of queries, including averages, sums, and counts. However, to the best of our knowledge, there is no published work on count-range queries

A count-range query tests if the number of rows satisfying a given predicate is within a specified range — that is, they ask "is the count within this range?" Count-range queries are a natural generalization of count queries, and correspond to a simple form of SQL "having" queries. An obvious differentially private mechanism for evaluating count-range queries is to count the number of rows satisfying the predicate, then to add Laplacian noise or geometric noise to the count, and to return *yes* if the noisy result is within the range and *no* otherwise. Our question in this paper is whether it is possible to do better. We answer in the affirmative, and give a different, optimal mechanism; but before doing so, we must first specify what "better" means.

Of course, privacy is just one aspect of the problem; utility also matters, as adding noise decreases accuracy. We measure the utility of a differentially private mechanism for count-range queries in terms of weighted errors. We adopt a model in which each information consumer provides an *error penalty function* that describes that consumer's perceived utility loss for a given error. For example, for a typical information consumer, errors that are in some sense "close" to the true answer may be less harmful than errors that are "farther" away.

However, different consumers may assign a different importance (weight) to the same error. In addition, each consumer may also have arbitrary side information about the data being queried. In an approach similar to that presented in [9] for count queries, we model a consumer's side information as a *prior distribution* over the number of rows satisfying the predicate of a count-range query. We combine a consumer's error penalty function and prior distribution to give a weighted error function. Therefore, returning to the issue of whether or not it is possible to do better than the naïve approach, the question becomes: given a privacy parameter, a consumer's weighted error penalty function and prior distribution, does adding geometric noise to the count and then checking the range minimize the consumer's weighted error? We show that the answer is "no", and propose a different, optimal differentially private mechanism for count-range queries.

With this result, we turn to consider a generalization in which the differentially private mechanism must serve multiple information consumers, each asking the same count-range query and each with their own weighted error function. A natural question is how to guarantee optimal utility for all such consumers. A naïve solution is to apply the single consumer mechanism separately for each consumer. However, this would result in the release of multiple randomizations of the query result, which would allow consumers to collude and reduce the effective noise in the answers. We seek a better alternative.

In the context of count queries (not count-range queries), [9, 10] showed that there is a more sophisticated differentially private mechanism that is both *collusion-resistant* and *simultaneously* optimal for every consumer. Their approach works by first perturbing the result of the count query, and then individually transforming that noisy result for each consumer. They proved that when the mechanism is the range-restricted geometric mechanism [9], the transformation guarantees optimal utility for every consumer.

Since count-range queries are a generalization of count queries, it is natural to ask if a similar approach works for count-range queries. We prove that the answer is no — in fact, we show that there is no differentially private mechanism that simultaneously maximizes every consumer's utility for count-range queries. On a more positive note, we prove the range-restricted geometric mechanism is an *approximate* universally utility maximizing mechanism for count-range queries, and that the weighted error for any consumer is at most twice that consumer's optimal weighted error.

Next, we consider threshold queries, a natural special case of count-range queries. Here, by "threshold queries" we mean queries that test if the number of rows satisfying a predicate is less/greater than a constant. That is, if a count-range query asks if the count is between two constants θ_1 and θ_2, threshold queries are just count-range queries for which either $\theta_1 = 0$ or $\theta_2 = +\infty$. Perhaps surprisingly, we show that with this apparently small change (requiring that one of the endpoints of the range in count-range query be zero or infinity), the range-restricted geometric mechanism guarantees optimal utility for every consumer while satisfying differential privacy.

The rest of this paper is organized as follows: Section 2 formulates the problem of guaranteeing differential privacy for count-range queries, and defines our utility model. Section 3 presents our results for count-range queries while Section 4 considers threshold queries. Section 5 discusses related work, while we conclude and discuss future directions in Section 6. Proofs not found in this submission are presented in the long version of our paper [1].

2. PRELIMINARIES

2.1 Count-Range Queries and Diff. Privacy

A *database* is a collection of rows. The domain of each row is a finite set D. The domain of a database of n rows is thus represented as D^n. In the rest of this paper, we shall use n to denote the number of rows in a database.

We will focus on a class of queries called *count-range queries*, where a count-range query consists of three parameters: a predicate p and two non-negative integers θ_1, θ_2 where ($\theta_1 < \theta_2$)[1]. Thus, we can characterize a count-range query by a triple $\langle p, \theta_1, \theta_2 \rangle$. Given a count-range query $\langle p, \theta_1, \theta_2 \rangle$ with predicate $p : D \rightarrow \{true, false\}$, the result of that count-range query is *yes* if the number of rows in a database that satisfy the predicate p is within the range $[\theta_1, \theta_2]$, and *no* otherwise. For ease of presentation, we define the *count* of a count-range query to be the number of rows satisfying the predicate of that query. When $\theta_1 = 0$ or $\theta_2 = +\infty$, the count-range query is a *threshold query*.

Our first goal is to propose a *differentially private* mechanism for count-range queries. In our context, a *mechanism* is a probabilistic function from D^n to some range R. Typical ranges include the real numbers, the integers, subranges of integers, and $\{$*yes, no*$\}$. For a mechanism X with a countable range R, we use $x_{\tau,r}$ to denote the probability of outputting $r \in R$ when the underlying database is τ. A mechanism X is called α-*differentially private* ($\alpha > 1$) if and only if for any pair of databases τ, τ' that differ by one row, $\forall r \in R$, $x_{\tau',r}/\alpha \leq x_{\tau,r} \leq \alpha x_{\tau',r}$. Two such databases τ and τ' are called *neighboring databases*.

We want to guarantee differential privacy for a count-range query. We formalize that problem next.

2.2 Diff. Private Mechanisms for Count-Range Queries

Because the result of a count-range query is either *yes* or *no*, given a differentially private mechanism X for a count-range query, let $x_{\tau,1}$ ($x_{\tau,0}$) be the probability of outputting *yes* (*no*) when the underlying database is $\tau \in D^n$. Because $x_{\tau,0} = 1 - x_{\tau,1}$, we can characterize a differentially private mechanism for a count-range query by $x_{\tau,1}$.

We assume that the probability that the result of a count-range query is *yes* is related to the count, the range, and the privacy parameter. More precisely, let μ_τ and $\mu_{\tau'}$ be the count of a count-range query over the databases τ and τ', respectively. Fixing the range and the privacy parameter, if $\mu_\tau = \mu_{\tau'}$, then we assume that $x_{\tau,1} = x_{\tau',1}$[2]. In the rest of this paper, unless otherwise specified, we assume that the range $[\theta_1, \theta_2]$ and the privacy parameter α are fixed. We call mechanisms satisfying our assumption *count-oriented* mechanisms.

DEFINITION 1. *(Count-oriented mechanism): A differentially private mechanism is* count-oriented *if and only if the output distributions produced by that mechanism on any pair of databases that have the same counts for a count-range query are identical.*

We introduce a function ϕ to characterize a *count-oriented* differentially private mechanism for a count-range query. Let $x_{\tau,1} = \phi(\mu)$ where μ is the count of that count-range query when the underlying database is τ. Of course, not every function ϕ can be used to define that probability. The following two basic properties on ϕ capture the requirement:

DEFINITION 2. *(Legal function): A function ϕ is a* legal function *if and only if for any integer μ,*

[1]We do not consider the case for $\theta_1 = \theta_2$ since a count-range query is equivalent to a count query in that case, which was considered in [9].

[2]The rationale of this assumption is discussed in the long version of our paper [1].

1. *for* $0 \leq \mu \leq n$, $0 \leq \phi(\mu) \leq 1$*;*
2. *for* $0 \leq \mu < n$, $\phi(\mu)/\alpha \leq \phi(\mu+1) \leq \alpha\phi(\mu)$ *and* $(1-\phi(\mu))/\alpha \leq 1-\phi(\mu+1) \leq \alpha(1-\phi(\mu))$.

The second property comes from the requirement of differential privacy that the ratio of the probabilities of outputting the same result (either *yes* or *no*) for any pair of neighboring databases must be bounded by the privacy parameter α. Thus, a legal function naturally corresponds to a count-oriented differentially private mechanism for a count-range query. Of course, there are many functions satisfying those two properties. Let Ω be the set of all legal functions: $\Omega = \{\phi \mid \phi \text{ is a legal function}\}$. Next, we propose a utility model to quantify the quality of a legal function. Our first goal in this paper is to find an optimal legal function that maximizes the utility of a consumer.

2.3 Utility Model

Because differentially private mechanisms are probabilistic, they commit errors. Thus, informally, the best differentially private mechanism should be the least likely to commit errors. Specifically, there are two types of errors in answering a count-range query:

1. False negative: the output is *no* but the correct answer is *yes*. The probability of a legal function ϕ to commit a false negative error when the count is μ is:
$$F^-_\phi(\mu) = 1-\phi(\mu),\ \theta_1 \leq \mu \leq \theta_2$$
2. False positive: the output is *yes* but the correct answer is *no*. The probability of a legal function ϕ to commit a false positive error when the count is μ is:
$$F^+_\phi(\mu) = \phi(\mu),\ 0 \leq \mu < \theta_1 \text{ or } \theta_2 < \mu \leq n$$

It is possible that different errors incur different utility losses for different consumers. Consider the following example: when the count is equal to θ_1, and the output is *no*, then that error is close to being correct in the sense that the correct answer will change from *yes* to *no* upon deleting even a single row that satisfies the predicate. Thus, that error may not severely impact utility. On the other hand, if the count is much larger than θ_2 and the output is *no*, the error might incur a large utility loss because it is far from being correct. Furthermore, each consumer may have a different tolerance on this type of errors. Therefore, we introduce an *error penalty function* ω for a consumer where $\omega(i)$ is the penalty to the error of a legal function when the count is i. The idea of error penalty function was proposed in [9, 10] for count queries, and we extend that idea to count-range queries. In both [9, 10], the error penalty functions are assumed to be monotone such that the error penalty function must be non-decreasing in the difference between the correct result of a count query and the output. In our work we do not require such property for ω, which provides greater flexibility in modeling a consumer's perceived utility loss for different errors.

Following the model presented in [9] in their study of count queries, we also assume that each consumer has side information about the underlying database. We model that side information as a prior probability distribution ρ over the count, where $\rho(i)$ represents the probability that a consumer believes the count of the given threshold query to be i. That prior distribution represents the beliefs of that consumer, which might stem from other information sources, previous interactions with the database, introspection, or common sense. We emphasize that we are not introducing priors to weaken the definition of differential privacy; we use the standard definition of differential privacy, which makes no assumptions about the side information of an adversary, and use a prior only to discuss the utility of a legal function to a potential consumer. We model the utility of a legal function for a consumer in terms of her weighted error:

$$err(\phi)=\sum_{i=0}^{\theta_1-1}\omega(i)\rho(i)\phi(i)+\sum_{i=\theta_1}^{\theta_2}\omega(i)\rho(i)(1-\phi(i))+\sum_{i=\theta_2+1}^{n}\omega(i)\rho(i)\phi(i) \quad (1)$$

3. OPTIMAL DIFF. PRIVATE MECHANISMS FOR COUNT-RANGE QUERIES

In this section, we first propose an optimal differentially private mechanism for count-range queries, then consider the problem of serving multiple consumers. Ghosh et al. [9] showed that there is a mechanism for count queries that simultaneously maximizes every consumer's utility while guaranteeing differential privacy. Although count-range queries are a simple generalization of count queries, surprisingly, our results indicate that there is no such mechanism for count-range queries.

3.1 An Optimal Diff. Private Mechanism

First, we define the notion of an *optimal legal function* for a count-range query by a single consumer.

DEFINITION 3. *Given a consumer with error penalty function* ω *and a prior distribution* ρ*, a legal function* ϕ^* *is an* optimal legal function *for a count-range query by that consumer if and only if* $\forall\phi \in \Omega$*,*
$$err(\phi^*) \leq err(\phi)$$
where $err()$ *is the weighted error function defined in* (1).

A straightforward way to find an optimal legal function for a consumer is to treat each $\phi(i)$, $0 \leq i \leq n$, as a variable, and to solve the linear programming problem that minimizes her weighted error subject to the requirements of a legal function. This amounts to solving an optimization problem of $n+1$ variables. However, we will prove that for the design of an optimal legal function, it suffices to solve an optimization problem with two variables. First, we prove a theorem about the existence of an optimal legal function of a particular form. To better understand our results, we define two recurrence relations:

$$\psi_1(\mu+1) = \min\{\alpha\psi_1(\mu), \frac{\alpha-1+\psi_1(\mu)}{\alpha}\} \quad (2)$$

and

$$\psi_2(\mu+1) = \max\{\frac{1}{\alpha}\psi_2(\mu), 1-\alpha+\alpha\psi_2(\mu)\} \quad (3)$$

We will prove that an optimal legal function for a count-range query $\langle p, \theta_1, \theta_2\rangle$ can be characterized by the minimum of the two recurrence relations defined in (2) and (3).

THEOREM 1. *An optimal legal function ϕ^* for the count-range query $\langle p, \theta_1, \theta_2\rangle$ is of the following form:*

$$\phi^*(\mu) = \min\{\psi_1(\mu), \psi_2(\mu)\} \quad (4)$$

where ψ_1 and ψ_2 satisfy (2) *and* (3)*, respectively, and*

$$\begin{aligned} \psi_1(\theta_1) &\leq \psi_2(\theta_1) \\ \psi_1(\theta_2) &\geq \psi_2(\theta_2) \end{aligned} \quad (5)$$

As we will explain in more detail later, (2) actually characterizes a family of optimal legal functions for the threshold query $\langle p, \theta_1, +\infty\rangle$ while (3) does so for the threshold query $\langle p, 0, \theta_2\rangle$. Since a count-range query $\langle p, \theta_1, \theta_2\rangle$ can be expressed as the "and" of the two threshold queries $\langle p, \theta_1, +\infty\rangle$ and $\langle p, 0, \theta_2\rangle$, we expect that an optimal legal function for that count-range query should be closely related to those two recurrence relations, and Theorem 1 confirms this.

By Theorem 1, when searching for an optimal legal function, it suffices to consider legal functions satisfying (4), which is an optimization problem consisting of two variables. That is, if we fix $\psi_1(0) = \beta_1$, then ψ_1 is well-defined because (2) is a first-order linear recurrence relation. More precisely, we can rewrite (2) as:

$$\psi_1(\mu+1) = \begin{cases} \alpha\psi_1(\mu) & \text{if } \psi_1(\mu) \leq 1/(\alpha+1) \\ (\alpha-1+\psi_1(\mu))/\alpha & \text{otherwise.} \end{cases}$$

For any integer μ $(0 \leq \mu \leq n)$, if $\beta_1 \in [0, 1/(\alpha^{n-1}(\alpha+1)))$, then

$$\psi_1(\mu) = \alpha^\mu \beta_1$$

and if $\beta_1 \in [1/(\alpha+1), 1]$, then

$$\psi_1(\mu) = 1 - \frac{1-\beta_1}{\alpha^\mu}$$

and if $\beta_1 \in [1/(\alpha^{n-1}(\alpha+1)), 1/(\alpha+1))$, let k be the unique integer between 1 and $n-1$, such that if $\beta_1 \in [1/(\alpha^k(\alpha+1)), \alpha/(\alpha^k(\alpha+1)))$, then

$$\psi_1(\mu) = \begin{cases} \alpha^\mu \beta_1 & \text{if } 0 \leq \mu \leq k \\ 1 - \frac{1-\beta_1\alpha^k}{\alpha^{\mu-k}} & \text{otherwise.} \end{cases}$$

Therefore, we divide the range $[0, 1]$ into $n+1$ subintervals, where $\psi_1(\mu)$ is linear in β_1 when β_1 is in a subinterval. Similarly, we can show ψ_2 is also well-defined by fixing $\psi_2(0) = \beta_2$.

Hence, the weighed error of ϕ can be written as $err(\phi) = err(\beta_1, \beta_2)$, where $err(\beta_1, \beta_2)$ is a piecewise multilinear function in β_1, β_2. To compute the minimum of $err(\beta_1, \beta_2)$, we can compute the minimum of $err(\beta_1, \beta_2)$ on each 2-dimensional subinterval, which is trivial, and then compare those local minima to get the global minimum. Let that global minimum be $err(\beta_1^*, \beta_2^*)$. Then, an optimal legal function ϕ^* is of the following form:

$$\phi^*(\mu) = \min\{\psi_1^*(\mu), \psi_2^*(\mu)\}$$

where $\psi_1^*(0) = \beta_1^*, \psi_2^*(0) = \beta_2^*$, and ψ_1^* and ψ_2^* satisfy the (2) and (3), respectively.

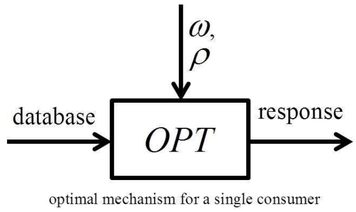

Figure 1: Consumer Dependent Optimal Mechanism

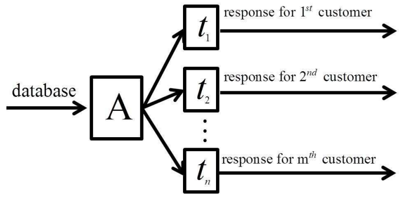

Figure 2: Serving Multiple Consumers with a Single Mechanism

3.2 Multiple Consumers

While we have given an optimal solution for the single consumer case, the situation where there are multiple consumers, each with their own error penalty functions and prior distributions, is more complex. Our main question is whether there is a single optimal function that works for multiple consumers. In this section, we consider a scenario in which multiple consumers ask the same count-range query. Our goal is to enforce differential privacy for multiple consumers while simultaneously guaranteeing optimal utility for every consumer.

A naïve application of our single consumer mechanism to multiple consumers is to invoke the optimal α-differentially private mechanism for each consumer separately. However, that naïve application allows colluding consumers to combine their noisy results and reduce the noise, and thus infer the real result more accurately. It is well-known that in such a situation the database has to operate under a more stringent privacy parameter to satisfy the utility requirements of the consumers. More precisely, suppose that there are m consumers, and the database guarantees α_i-differential privacy for the i^{th} consumer. By the composition property of differential privacy [7], we can only guarantee α-differential privacy for those m consumers provided $\prod_{i=1}^m \alpha_i \leq \alpha$, and thus, $\alpha_i \ll \alpha$. As a result, the weighted error of each consumer is actually larger than that of the optimal α-differentially private mechanism for each consumer.

The problem with collusion arises because the true answer

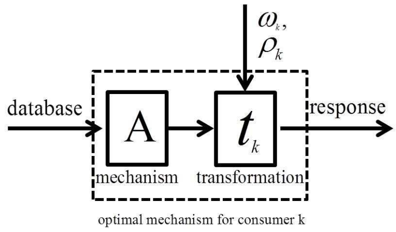

Figure 3: Decomposition of the Optimal Mechanism for a Consumer

is randomized and released multiple times. To avoid that problem, we observe that if the true query result is randomized only once, and every consumer receives the same noisy result, then the problem goes away. However, if the true query result is only randomized once, the differentially private mechanism cannot be optimal for every consumer unless they have the same error penalty function and prior distribution. That apparent paradox is resolved by assuming that the database can individually further transform the intermediate noisy output (which is the same for every consumer), and that transformation is deliberately calibrated to the consumer's parameters — her error penalty function and prior distribution — such that the combination of the differentially private mechanism and that transformation maximizes that consumer's utility.

To illustrate that idea, for a single consumer, the optimal mechanism depends on her error penalty function and prior distribution as shown in Figure 1. When serving multiple consumers, instead of invoking each consumer's optimal mechanism, the database employs a common mechanism A for every consumer to produce an intermediate noisy result, and then for each consumer, individually transforms that intermediate noisy result for each consumer to produce the output (*yes,no*) for that consumer. This is shown in Figure 2. Therefore, that approach actually decomposes a consumer's optimal mechanism into two parts, a consumer independent mechanism A, and a consumer dependent transformation as shown in Figure 3. For each consumer, if that decomposition is "lossless", then the mechanism A indirectly guarantees optimal utility for that consumer. We inquire whether there exists such a common mechanism A. In the rest of this paper, we shall refer to the consumer independent mechanism A as the "deployed mechanism." In our context, a transformation is a probabilistic reinterpretation of the intermediate noisy output produced by A. This is defined in Definition 4.

DEFINITION 4. *(Transformation): For a deployed differentially private mechanism $A : D^n \rightarrow R$, a* transformation $\mathbf{t}$ *for a count-range query is a probabilistic function from R to $\{yes\}$. For a countable range R, t_r denotes the probability that the database reinterprets the outcome $r \in R$ of the mechanism A to yes.*

It suffices to only consider the probability of mapping an intermediate noisy result r to *yes* since $1 - t_r$ naturally corresponds to the probability of reinterpretting the outcome r to *no*. To output a noisy result for a count-range query by a consumer, let $\mathbf{t}$ be a transformation for a particular consumer, and r be the intermediate noisy result produced by the deployed mechanism A. Then the database flips a biased coin with probability t_r to output *yes*, and $1 - t_r$ to output *no*. Note that the output range of the deployed mechanism A does not necessarily correspond to $\{yes,no\}$ as the transformation will eventually remap the noisy output of A to that range. Furthermore, only the deployed mechanism A needs to be differentially private since the transformation receives the noisy output from A, which has already been differentially private.

Given a deployed differentially private mechanism A, and a transformation $\mathbf{t}$, the combination of A and $\mathbf{t}$ induces a new mechanism X for count-range queries, where the probability of returning *yes* for a database τ is: $x_\tau = \sum_{r \in R} a_{\tau,r} t_r$. Since A is differentially private, X is also differentially private by linearity. In accordance with the literature [3, 13], we say a mechanism X can be *derived* from the deployed mechanism A if there is a transformation $\mathbf{t}$ such that $X = A \circ \mathbf{t}$. Since X is actually a vector, we shall denote it by $\mathbf{x}$.

Since $\mathbf{x}$ is a differentially private mechanism for count-range queries, for the design of an optimal differentially private mechanism for count-range queries, we shall assume that $\mathbf{x}$ is count-oriented. To guarantee that, we require that the deployed differentially private mechanism is also count-oriented, and thus, we can characterize the domain of that mechanism by $\{0, \ldots, n\}$ instead of D^n. After that restriction, the induced mechanism $\mathbf{x}$ naturally corresponds to a legal function. We say the induced mechanism $\mathbf{x}$ is optimal for a consumer if and only if $\mathbf{x}$ minimizes that consumer's weighted error.

For each consumer, if the decomposition of her optimal mechanism is "lossless" in the sense that there is a transformation such that the induced mechanism of the deployed mechanism and that transformation is also optimal for her, then the deployed mechanism indirectly guarantees optimal utility for that consumer. Such a mechanism is called a *universally utility maximizing mechanism.*

DEFINITION 5. *(Universally utility maximizing differentially private mechanism): A differentially private mechanism A is* universally utility maximizing *if and only if for each consumer k, there is a transformation $\mathbf{t}_k$ such that the induced differentially private mechanism $\mathbf{x}_k$ is optimal for that consumer k.*

If we can find such a mechanism, then the database can utilize that mechanism to randomize the count only once to produce an intermediate noisy result, and then store that intermediate noisy result. For every consumer, the database uses a transformation tailored for that consumer to randomize the stored intermediate noisy output. That "double-randomization" approach rules out the privacy threat of colluding consumers as even if they successfully cancel out the noise, the result is the intermediate noisy result, which is still differentially private. Furthermore, by carefully selecting a transformation for each consumer, the induced mechanism of the universally utility maximizing mechanism and that transformation guarantees optimal utility for that consumer, which provides a strong utility guarantee. Ghosh et al. [9] showed that the range-restricted mechanism is universally utility maximizing for count queries when the error penalty function is monotone, and is of the following form:

DEFINITION 6. *(Range-restricted geometric mechanism [9]): For a given privacy parameter α and a count query Q, $\forall \tau \in D^n$, let μ be the correct result of Q over τ. The range-restricted geometric mechanism outputs $Z(\mu)$ where $Z(\mu)$ is a random variable with the following distribution for each integer z:*

$$\Pr[Z(\mu) = z] = \begin{cases} \frac{\alpha}{\alpha+1}\alpha^{-|z-\mu|} & \text{if } z \in \{0, n\} \\ \frac{\alpha-1}{\alpha+1}\alpha^{-|z-\mu|} & \text{if } 0 < z < n \\ 0 & \text{otherwise.} \end{cases} \quad (6)$$

Since count-range queries are a natural generalization of count queries, one may expect that the range-restricted geometric mechanism is also universally utility maximizing for count-range queries. However, we will prove that this is not so. More surprisingly, our results indicate that there is no differentially private mechanism that is universally utility maximizing for count range queries, as stated in Theorem 2.

THEOREM 2. *There is no universally utility maximizing differentially private mechanism for count-range queries.*

Note that Theorem 2 not only deals with count-oriented mechanisms, but also considers other differentially private mechanisms. To give an intuition for why Theorem 2 holds, let us first examine why the range-restricted geometric mechanism is not universally utility maximizing for count-range queries.

3.2.1 Discussion on Range-restricted Geometric Mechanism

Let us consider a special case where the size of the database $n = 3$, and the bounds for the count-range query are $\theta_1 = 1$ and $\theta_2 = 2$. In this case we can represent the optimal differentially private mechanism for the count-range query as a vector $(z_0, z_1, z_2, z_3)^t$, where z_i $(0 \leq i \leq 3)$ is the probability of outputting *yes* when the count is i. We can prove that when a consumer posing this query has a uniform error penalty function and a uniform prior distribution, the *only* optimal differentially private mechanism for that consumer is

$$\hat{\mathbf{x}} = (\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t$$

We can prove that the range-restricted geometric mechanism can not derive $\hat{\mathbf{x}}$, and thus is not universally utility maximizing. We can also understand why the range-restricted geometric mechanism is not universally utility maximizing for count-range queries from a more intuitive perspective: by Theorem 1, an optimal legal function for count-range queries can be rewritten into the following form:

$$\phi^*(\mu) = \begin{cases} \psi_1(\mu) & \text{if } 0 \leq \mu \leq \gamma \\ \psi_2(\mu) & \text{if } \gamma < \mu \leq n \end{cases}$$

where γ is an integer between θ_1 and θ_2.

Let $\mathbf{r}_1 = (\psi_1(0), \ldots, \psi_1(n))^t$ and $\mathbf{r}_2 = (\psi_2(0), \ldots, \psi_2(n))^t$. As proved later in Section 4, there exists a transformation $\mathbf{t}_1$ such that the induced mechanism of the range-restricted geometric mechanism M and that transformation is $\mathbf{r}_1$, where $M \circ \mathbf{t}_1 = \mathbf{r}_1$. There also exists a transformation $\mathbf{t}_2$ such that $M \circ \mathbf{t}_2 = \mathbf{r}_2$. Therefore, intuitively, the database should pick $\mathbf{t}_1$ to transform the noisy count produced by the range-restricted geometric mechanism if the count μ does not exceed γ, and $\mathbf{t}_2$ otherwise. However, the decision of which transformation to employ depends on the correct count μ. If that decision is deterministic, then it is a violation of differential privacy since no deterministic algorithm satisfies differential privacy [5]. Therefore, that decision has to be randomized to accommodate the privacy requirement. As a result, the database will inevitably commit errors in picking the correct transformation because of the randomized nature, and thus, the combination of the range-restricted geometric mechanism and the transformation can not yield an optimal differentially private mechanism for a consumer.

3.2.2 Count-Oriented Mechanisms

Let us first assume that some universally utility maximizing mechanism exists that is a function of count. Again, we start with the special case where $n = 3$, $\theta_1 = 1$ and $\theta_2 = 2$. For a consumer with a uniform error penalty function and a uniform prior distribution, the only optimal differentially private mechanism for that consumer is:

$$\hat{\mathbf{x}} = (\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t.$$

Next, we reassign the probability mass of the uniform prior distribution such that the prior distribution ρ satisfies:

$$\rho(0)/\rho(1) = \alpha^2, \rho(2)/\rho(1) = \alpha, \rho(3) = \rho(2)$$

We can prove that for a consumer with a uniform error penalty function and such a prior distribution ρ, the *only* optimal differentially private mechanism is:

$$\hat{\mathbf{y}} = (\frac{1}{(\alpha+1)\alpha}, \frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t$$

We characterize a differentially private mechanism A as a matrix of size $4 \times m$, where the output range of A is $\{1, \ldots, m\}$ whose elements satisfy $1/\alpha \leq a_{i,j}/a_{i+1,j} \leq \alpha$. We prove that there is no universally utility maximizing mechanism by showing that no matrix satisfying differential privacy can derive both $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$. We start by investigating the properties of A.

LEMMA 1. *Let $B = \begin{bmatrix} \mathbf{p}^t \\ \mathbf{q}^t \end{bmatrix} = \begin{bmatrix} p_1 & p_2 & \ldots & p_m \\ q_1 & q_2 & \ldots & q_m \end{bmatrix}$ be any $2 \times m$ matrix, where $\mathbf{p}$ and $\mathbf{q}$ are two probability vectors: $0 \leq p_j, q_j \leq 1$ and $\sum_j p_j = \sum_j q_j = 1$. Suppose they further satisfy the privacy constraints $1/\alpha \leq p_j/q_j \leq \alpha$, and for some $\mathbf{t}$, with $0 \leq t_j \leq 1$, $B \circ \mathbf{t} = (\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1})^t$. Then, all privacy constraints are tight: For all $1 \leq j \leq m$, either $p_j/q_j = \alpha$, or $p_j/q_j = 1/\alpha$. Furthermore, $t_j = 0$ in the former case, and $t_j = 1$ in the latter case.*

PROOF. If for some j, $p_j/q_j > 1/\alpha$ and the corresponding $t_j \neq 0$, then $p_j t_j > q_j t_j/\alpha$. Since for every other j', $p_{j'}/q_{j'} \geq 1/\alpha$, we get $\mathbf{p} \circ \mathbf{t} > \mathbf{q} \circ \mathbf{t}/\alpha$, a contradiction. Hence for all $1 \leq j \leq m$, $p_j/q_j = 1/\alpha$ or $t_j = 0$.

Now consider $\mathbf{t}' = \mathbf{1} - \mathbf{t}$, where $\mathbf{1}$ is the vector of all ones. Note that $\mathbf{p} \circ \mathbf{t}' = 1 - \mathbf{p} \circ \mathbf{t} = \frac{\alpha}{\alpha+1}$, and $\mathbf{q} \circ \mathbf{t}' = 1 - \mathbf{q} \circ \mathbf{t} = \frac{1}{\alpha+1}$. Switching the roles of $\mathbf{p}$ and $\mathbf{q}$, we have for all $1 \leq j \leq m$, $p_j/q_j = \alpha$ or $t_j = 1$.

Since clearly $t_j = 0$ and $t_j = 1$ cannot hold simultaneously, we conclude that for all $1 \leq j \leq m$, either $p_j/q_j = \alpha$ or $1/\alpha$. In the former case, clearly $p_j/q_j \neq 1/\alpha$, and hence $t_j = 0$. Similarly when $p_j/q_j = 1/\alpha$, we have $t_j = 1$. $\square$

COROLLARY 1. *If a $4 \times m$ matrix A can derive both $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$, then all the privacy constraints must be tight: $\forall i, j$, where $0 \leq i < 3$, $1 \leq j \leq m$*

$$a_{i,j}/a_{i+1,j} = \alpha \ \ or \ \ a_{i,j}/a_{i+1,j} = 1/\alpha$$

Next, we will prove that in fact no such matrix exists.

LEMMA 2. *No matrix A can derive both $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$.*

PROOF. Let $A \circ \mathbf{t} = \hat{\mathbf{x}}$, and $A \circ \mathbf{t}' = \hat{\mathbf{y}}$. By Lemma 1 and Corollary 1, without loss of generality (by renaming the columns of A), we may assume that $\exists k (1 \leq k < m)$ such that $\forall j (1 \leq j \leq k)$, $a_{0,j}/a_{1,j} = 1/\alpha$ and $t_j = 1$, and $\forall j (k < j \leq m)$, $a_{0,j}/a_{1,j} = \alpha$ and $t_j = 0$. Note that since each row of A sums to 1, we must have $1 \leq k < m$.

Among $\{1, \ldots, k\}$, we may further assume without loss of generality that $\exists \ell (0 \leq \ell < k)$, such that $\forall j (1 \leq j \leq \ell)$, $a_{1,j}/a_{2,j} = 1/\alpha$, and $\forall j (\ell < j \leq k)$, $a_{1,j}/a_{2,j} = \alpha$. (Here either range is guaranteed to be non-empty.)

Then,

$$\frac{\alpha}{\alpha+1} = \mathbf{a}_1 \circ \mathbf{t} = \frac{1}{\alpha} \sum_{j=1}^{\ell} a_{2,j} + \alpha \sum_{j=\ell+1}^{k} a_{2,j}$$

$$\frac{\alpha}{\alpha+1} = \mathbf{a}_2 \circ \mathbf{t} = \sum_{j=1}^{\ell} a_{2,j} + \sum_{j=\ell+1}^{k} a_{2,j}$$

It follows that

$$\sum_{j=1}^{\ell} a_{2,j} = \frac{\alpha^2}{(\alpha+1)^2}$$

From $A \circ \mathbf{t}' = \hat{\mathbf{y}}$, and

$$\mathbf{a}_0 \circ \mathbf{t}' = \frac{1}{\alpha} \mathbf{a}_1 \circ \mathbf{t}'$$

we have $\forall j > k$, $t'_j = 0$. This is because for any $j > k$, $a_{0,j} = \alpha a_{1,j} > a_{1,j}/\alpha$. From

$$\mathbf{a}_1 \circ \mathbf{t}' = \frac{1}{\alpha} \mathbf{a}_2 \circ \mathbf{t}'$$

we have $\forall j (\ell < j \leq k)$, $t'_j = 0$, by the same reasoning. Therefore,

$$\frac{\alpha}{\alpha+1} = \mathbf{a}_2 \circ \mathbf{t}' \leq \sum_{j=0}^{\ell} a_{2,j} = \frac{\alpha^2}{(\alpha+1)^2}$$

a contradiction.

Hence, there is no matrix A that can derive both $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$ while guaranteeing differential privacy. $\square$

Therefore, for the special case $n = 3$, $\theta_1 = 1$ and $\theta_2 = 2$, there is no universally utility maximizing mechanism that is count-oriented for count-range queries. For the general case, we can prove that there are consumers whose only optimal differentially private mechanisms, when expressed as vectors of length $n+1$, contain $\hat{\mathbf{x}}$, and $\hat{\mathbf{y}}$ respectively, as a subsequence. More precisely, let $k = (\theta_1 + \theta_2 - 1)/2$ if $\theta_1 + \theta_2$ is odd, and $k = (\theta_1 + \theta_2)/2$ otherwise.

LEMMA 3. *There exists a consumer whose only optimal differentially private mechanism is:*

$$\mathbf{x} = (x_0, \ldots, x_n)^t$$

where for all i, $0 \leq i \leq k$, $x_i = 1/(\alpha^{k-1-i}(\alpha+1))$, and for all j, $k+1 \leq j \leq n$, $x_j = 1/(\alpha^{j-k-2}(\alpha+1))$, and a consumer whose only optimal differentially private mechanism is:

$$\mathbf{y} = (y_0, \ldots, y_n)^t$$

where for all i, $0 \leq i \leq k$, $y_i = 1/(\alpha^{k-i}(\alpha+1))$, and for all j, $k+1 \leq j \leq n$, $y_j = 1/(\alpha^{j-k-2}(\alpha+1))$.

By Lemma 3, in particular,

$$(x_{k-1}, x_k, x_{k+1}, x_{k+2})^t = \hat{\mathbf{x}}$$
$$(y_{k-1}, y_k, y_{k+1}, y_{k+2})^t = \hat{\mathbf{y}}$$

Therefore, if there is a matrix A that can derive both $\mathbf{x}$ and $\mathbf{y}$, then the submatrix $(\mathbf{a}_{k-1}, \mathbf{a}_k, \mathbf{a}_{k+1}, \mathbf{a}_{k+2})^t$ can derive both $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$, which is in contradiction to Lemma 2.

COROLLARY 2. *No matrix A satisfying differential privacy can derive both $\mathbf{x}$ and $\mathbf{y}$.*

3.2.3 Other Mechanisms

So far, we have only considered count-oriented mechanisms. For any arbitrary mechanism that may depend on the database and not merely the count, we construct $n+1$ instances of databases, $\tau_0, \ldots, \tau_n$ where the count for a count-range query is i in the database τ_i, and τ_i, τ_{i+1} are neighboring databases. Therefore, we can still characterize the optimal mechanism, when restricted to these $n+1$ databases, for a consumer by a vector $(z_0, \ldots, z_n)^t$ where z_i is the probability of outputting *yes* when the underlying database is τ_i, and the mechanism as a matrix A of size $(n+1) \times m$ where the i^{th} row corresponds to the database τ_i, which is identical to that of count-oriented mechanisms. By differential privacy, $a_{i+1,j}/\alpha \leq a_{i,j} \leq \alpha a_{i+1,j}$. By Lemma 3, there are consumers whose only optimal mechanism is $\mathbf{x}$ and $\mathbf{y}$.

By Corollary 2, no matrix can derive both $\mathbf{x}$ and $\mathbf{y}$. Therefore, there is no universally utility maximizing mechanism for count-range queries.

3.3 A Non-Existence Result

So far, we have proved that there is no universally utility maximizing mechanism for count-range queries. However, the requirements of a universally utility maximizing mechanism actually limit the behavior of a database: the database can only produce an intermediate noisy output, and then transform that intermediate noisy output for each consumer. Going beyond any such restriction, we can prove that no matter what mechanism is deployed by a database to produce the noisy results for multiple consumers, as long as that mechanism is differentially private, that mechanism can not maximize every consumer's utility.

THEOREM 3. *There is no differentially private mechanism that maximizes every consumer's utility for a count-range query.*

Proof Sketch: We start by considering a special case where $n = 3$, and $\theta_1 = 1$, $\theta_2 = 2$. We have already shown that there are two consumers whose only optimal differentially private mechanisms are:

$$\hat{\mathbf{x}} = (\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t$$
$$\hat{\mathbf{y}} = (\frac{1}{(\alpha+1)\alpha}, \frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t$$

For ease of presentation, we shall define the consumer whose optimal mechanism is $\hat{\mathbf{x}}$ as the first consumer, and the other one as the second consumer. Then $\forall \tau \in D^n$, $i, j = 0, 1$, let $t_{\tau,i,j}$ be the probability of outputting i for the first consumer, and j for the second consumer. First, we prove the case where the mechanism is count-oriented. This will be generalized later. Therefore, we can characterize the output distribution for $\mu = 0, 1, 2$ by three 2×2 matrices:

	0	1	0	1	0	1
0	$t_{0,0,0}$	$t_{0,0,1}$	$t_{1,0,0}$	$t_{1,0,1}$	$t_{2,0,0}$	$t_{2,0,1}$
1	$t_{0,1,0}$	$t_{0,1,1}$	$t_{1,1,0}$	$t_{1,1,1}$	$t_{2,1,0}$	$t_{2,1,1}$

By the requirement of differential privacy, $\forall \mu = 0, 1$, and $i, j = 0, 1$, $t_{\mu+1,i,j}/\alpha \leq t_{\mu,i,j} \leq \alpha t_{\mu+1,i,j}$. If that mechanism maximizes both consumers' utility, then the marginal distribution in each matrix for each consumer constitutes her optimal mechanism. Let $t_{\mu,1,1} = t_\mu$, and thus, the mechanism is:

	0	1	0	1	0	1
0	$t_0 + \frac{\alpha-1}{\alpha}$,	$\frac{1}{(\alpha+1)\alpha} - t_0$	t_1,	$\frac{1}{\alpha+1} - t_1$	$t_2 - \frac{\alpha-1}{\alpha+1}$,	$\frac{\alpha}{\alpha+1} - t_2$
1	$\frac{1}{\alpha+1} - t_0$,	t_0	$\frac{\alpha}{\alpha+1} - t_1$,	t_1	$\frac{\alpha}{\alpha+1} - t_2$,	t_2

By differential privacy, $t_1 \leq \alpha t_0$, and

$$\frac{1}{\alpha+1} - t_1 \leq \alpha(\frac{1}{\alpha(\alpha+1)} - t_0)$$

Thus, $\alpha t_0 \leq t_1$. Therefore $t_1 = \alpha t_0$. Similarly, we can prove that $t_2 = \alpha t_1$. By differential privacy,

$$t_0 + \frac{\alpha-1}{\alpha} \leq \alpha t_1 = \alpha^2 t_0$$

Then, $t_0 \geq 1/(\alpha(\alpha+1))$. By differential privacy,

$$\frac{\alpha}{\alpha+1} - t_1 \leq \alpha(\frac{\alpha}{\alpha+1} - t_2)$$

Since $t_2 = \alpha^2 t_0$ and $t_1 = \alpha t_0$, $t_0 \leq 1/(\alpha+1)^2$. We have thus obtained a contradiction. Therefore, no such mechanism maximizes both consumers' utility when $n = 3$, $\theta_1 = 1$ and $\theta_2 = 2$.

For the more general case, the proof is similar to that of Corollary 2 and Theorem 2, and we omit the details here. □

As discussed in [3], the universally utility maximizing mechanism only exists for a limited class of queries. Brenner et al. characterized the necessary conditions on the queries that admit universally utility maximizing mechanism. The basic idea of their proof is to characterize a query by an undirected graph where each vertex corresponds to an output of the query, and an edge is drawn between two vertices if the addition/deletion of a tuple to/from a database can result in such a change in the outputs. Brenner et al. proved that if there is a cycle in the privacy constraint graph, then no universally utility maximizing mechanism exists. However, for count-range queries there is no cycle on the privacy constraint graph, hence Brenner's result cannot be used to prove our result.

3.4 An Approximate Mechanism

Given that there is no optimal mechanism, we turn to consider approximate mechanisms. First, we formulate the notion of *β-approximate universally utility maximizing*, which measures the approximation ratio in terms of the weighted error.

DEFINITION 7. *(β-approximate universally utility maximizing): A differentially private mechanism X is* β-approximate universally utility maximizing *if and only if for any consumer, there exists a differentially private mechanism that is derivable from X whose weighted error for that consumer is at most β times of the minimal weighted error of that consumer.*

We will prove that the range-restricted geometric mechanism is 2-approximate universally utility maximizing for count-range queries.

THEOREM 4. *The range-restricted geometric mechanism* (6) *is 2-approximate universally utility maximizing for count-range queries.*

We consider the range-restricted geometric mechanism as an approximation is because of the following observation: if there were no privacy concern, then the identity matrix I would be a trivial universally utility maximizing mechanism for count-range queries. An identity matrix I means that given a count i, the mechanism always outputs i. In other words, the output probability distribution is 1 at i and 0 everywhere. However, by the requirement of differential privacy, that probability distribution needs to be "flattenned" such that the probability mass of outputting i is assigned to other outputs. Intuitively, after that reassignment, given an output i, the most likely output should still be i, and the probability of outputting j decreases with the increasing in $|j-i|$. The range-restricted geometric mechanism exactly reflects that intuition.

4. OPTIMAL DIFF. PRIVATE MECHANISMS FOR THRESHOLD QUERIES

In this section, we consider threshold queries, a special case of count-range queries which test whether or not the number of rows in a database satisfying a predicate is less/greater than a threshold. More precisely, a threshold query can be characterized by either $\langle p, 0, \theta\rangle$ or $\langle p, \theta, +\infty\rangle$. We first revisit the problem of designing an optimal mechanism for a single consumer, now for the special case of threshold queries. It turns out that a simpler mechanism is possible for threshold queries than for count-range queries, and this simpler mechanism will be useful in our search for an optimal mechanism for multiple consumers for threshold queries. We show that, unlike the case for count-range queries, in the case when multiple consumers ask threshold queries with the same predicate (with possibly different thresholds), there exists a mechanism that simultaneously maximizes every consumer's utility while guaranteeing differential privacy.

4.1 An Optimal Diff. Private Mechanism

As was the case for count-range queries, a straightforward way to find an optimal legal function for a consumer asking a threshold query is to treat each $\phi(i)$, $0 \le i \le n$, as a variable, and to solve the linear programming problem that minimizes her weighted error subject to the requirements of a legal function. This amounts to solving an optimization problem of $n+1$ variables. However, again, we will prove that for the design of an optimal legal function, it suffices to solve an optimization problem with a single variable. First, we prove a theorem about the existence of an optimal legal function of a particular form.

THEOREM 5. *There exists an optimal legal function ϕ^* for a threshold query $\langle p, \theta, +\infty\rangle$ that satisfies the recurrence relation in* (2).

By Theorem 5, when searching for an optimal legal function, it suffices to consider legal functions satisfying (2). As discussed in Section 3, ϕ^* is well-defined if we fix $\phi^*(0) = \beta$. Hence, the weighed error of ϕ can be written as $err(\phi) = err(\beta)$, where $err(\beta)$ is a piecewise linear function in β. To compute the minimum of $err(\beta)$, we can compute the minimum of $err(\beta)$ on each subinterval, which is trivial, and then compare those local minima to get the global minimum. Let that global minimum be $err(\beta^*)$. Then, an optimal legal function ϕ^* is well-defined where $\phi^*(0) = \beta^*$ and ϕ^* satisfies (2).

We can also prove the existence of a particular form of optimal legal functions for a threshold query $\langle p, 0, \theta\rangle$, which is symmetric to Theorem 5.

THEOREM 6. *There exists an optimal legal function ϕ^* for the query $\langle p, 0, \theta\rangle$ that satisfies the recurrence relation in* (3).

4.2 Multiple Consumers

Next, we consider the problem of serving multiple consumers asking the same threshold query. We want to know if there exists a universally utility maximizing mechanism for threshold queries. Surprisingly, unlike the case for count-range queries, we can prove that the range-restricted geometric mechanism is a such mechanism. This is shown in Theorem 7.

THEOREM 7. *The range-restricted geometric mechanism* (6) *is a universally utility maximizing differentially private mechanism for threshold queries.*

Proof Sketch: We can characterize a range-restricted geometric mechanism by a symmetric matrix M of size $(n+1)\times(n+1)$ whose element $m_{i,j} = \Pr[Z(i) = j]$.

$$M = \frac{\alpha-1}{\alpha+1}\begin{pmatrix} \frac{\alpha}{\alpha-1}\cdot 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n} \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-1} & 1 & \alpha^{-1} & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n+1} \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-2} & \alpha^{-1} & 1 & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-n} & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & \frac{\alpha}{\alpha-1}\cdot 1 \end{pmatrix}$$

We can characterize a consumer's optimal differentially private mechanism for threshold queries $\langle p, \theta, +\infty\rangle$ by a vector $\mathbf{z} = (z_0, \ldots, z_n)^t$ satisfying Theorem 5. We can show that M is invertible. Let $\mathbf{t} = M^{-1}\circ\mathbf{z} = (t_0, \ldots, t_n)^t$. Then it suffices to prove that $\mathbf{t}$ is a transformation satisfying Definition 4. Let M_i be the matrix obtained from M by replacing the i^{th} column of M by $\mathbf{z}$. By Cramer's rule, $t_i = \det(M_i)/\det(M)$.

By Theorem 5, for all i, $0 \le i < n$, $z_{i+1} = \min\{\alpha z_i, 1 - (1-z_i)/\alpha\}$. We will prove that for all j, $0 \le j \le n$, $0 \le \det(M_j)/\det(M) \le 1$. Therefore, $\mathbf{t} = (t_0, t_1, \ldots, t_n)^t$ is a transformation. We can prove the same results for threshold queries $\langle p, 0, \theta\rangle$ in a similar way, and we omit the details here. □

The universally utility maximizing differentially private mechanism was first studied for count queries in [9, 10], where only "oblivious" mechanisms were considered. A mechanism is *oblivious* if it sets up an identical distribution over outputs for every pair of databases that has the same unperturbed query result. Naturally, an implementation of an oblivious mechanism only needs to have access to the true query result — the input — and can be oblivious to the database itself. The range-restricted geometric mechanism only depends on the result of a count query instead of the database itself, and thus, it is an oblivious mechanism.

In contrast to previous work, the differentially private mechanisms we are considering in this paper are non-oblivious mechanisms because the true query result of a threshold query is either *yes* or *no*, whereas the mechanisms we have proposed rely on the count of a threshold query rather than just *yes* or *no*. Of course, there are also oblivious mechanisms for threshold queries. We can use a function Φ to characterize the oblivious mechanisms for threshold queries where β_1 (β_2) is the probability of outputting *yes* when the correct answer is *no* (*yes*).

$$\Phi(\mu) = \begin{cases} \beta_1 & \text{if } 0 \leq \mu < \theta \\ \beta_2 & \text{if } \theta \leq \mu \leq n \end{cases}$$

When $0 \leq \beta_2/\alpha \leq \beta_1 \leq \alpha\beta_2 \leq 1$ and $(1-\beta_2)/\alpha \leq (1-\beta_1) \leq \alpha(1-\beta_2)$, it is easy to verify that Φ is a legal function. However, we can show that any legal function Φ is not an optimal legal function unless $\beta_1 = \beta_2 = 1$ or $\beta_1 = \beta_2 = 0$: we construct a function ϕ satisfying (2), and $\phi(\theta) = \beta_2$. It is not difficult to see that ϕ is less likely to commit both types of errors for a threshold query unless $\beta_1 = \beta_2 = 1$ or $\beta_1 = \beta_2 = 0$. Thus, an oblivious differentially private mechanism for threshold queries is not optimal in a general sense.

Following Theorem 7, the database utilizes the range-restricted geometric mechanism to perturb the count of a threshold query only once, and stores that noisy count. For each consumer asking the same threshold query, the database randomly transforms the stored noisy count to *yes* or *no* using the transformation which maximizes that consumer's utility. For consumers asking threshold queries with the same predicate but different thresholds, the database still only needs to perturb the count once since the counts for those queries are the same. Note that Theorem 5 is independent of the threshold θ, and thus, for each consumer, there is an optimal legal function satisfying (2). By Theorem 7, there is a transformation for that consumer such that the induced differentially private mechanism of the range-restricted geometric mechanism and that transformation guarantees optimal utility for that consumer. Therefore, the range-restricted geometric mechanism also simultaneously guarantees optimal utility for all consumers asking threshold queries with the same predicate but different thresholds.

COROLLARY 3. *For consumers asking threshold queries with the same predicate but different thresholds, there is a transformation for each consumer such that the induced differentially private mechanism of the range-restricted geometric mechanism and that transformation guarantees optimal utility for that consumer.*

The range-restricted geometric mechanism also simultaneously maximizes utility for different privacy levels. We refer interested readers to [10] for a complete and precise description of that property.

5. RELATED WORK

The notion of differential privacy was proposed by Dwork et al. in [5]. The same authors also proposed the addition of Laplacian noise to guarantee differential privacy [7] for count queries. McSherry et al. proposed a universal differentially private mechanism for general queries in [15]; see [6] for a recent survey of privacy.

Dinur and Nissim [4] are pioneers in establishing the upper bounds on the number of queries that can be answered with reasonable accuracy. Count queries [4, 8], and more general queries [16, 7, 2] have been studied from that perspective. Recently, Hardt and Talwar [11] gave tight upper and lower bounds on the amount of noise needed to ensure differential privacy for a given number of linear queries. Hay et al. and Li et al. [12, 14] both proposed exploiting consistency constraints to increase accuracy when answering multiple queries.

Ghosh et al. [9] were the first to formally define a universally utility maximizing differentially private mechanism that simultaneously maximizes every consumer's utility for count queries. Their results indicate that the range-restricted geometric mechanism is a universally utility maximizing differentially private mechanism for a single count query such that every consumer can combine her own information and utility function in a way that maximizes her utility, and that transformation is effectively enough to result in an optimal mechanism. Gupte et al. proved a similar result in [10] for a different utility model. Our work extends that idea to threshold queries. Brenner [3], shows that the universally utility maximizing mechanism only exists for a limited class of queries, and gives a criterion that partially characterizes when they do not exist. In our work we give an example of a class of queries (count-range queries) for which no universally utility maximizing mechanism exists that is not covered by Brenner's criterion.

6. CONCLUSION

In this paper, we propose an optimal differentially private mechanism for count-range queries. However, when considering serving multiple consumers, in contrary to previous positive results for count queries, we prove that for count-range queries there is no differentially private utility maximizing mechanism that guarantees optimal utility for every consumer. Despite this negative result, we prove that the range-restricted geometric mechanism is a 2-approximate universally utility maximizing for count-range queries. Furthermore, we show that for threshold queries (a natural restriction on count-range queries), a universally utility maximizing differentially private mechanism that simultaneously maximizes every information consumer's utility does exist.

The optimal mechanisms for both threshold queries and count-range queries we have proposed are non-oblivious, in that they take a count as the input instead of *yes* or *no*. It would be interesting to investigate non-oblivious optimal differentially private mechanisms for other classes of queries. An application of our results to differentially private frequent itemset mining is also an interesting direction for future research, as determining whether an itemset is frequent is akin to answering a threshold query.

7. REFERENCES

[1] http://pages.cs.wisc.edu/~zeng/icdt_submission.pdf.
[2] A. Blum, K. Ligett, and A. Roth. A learning theory approach to non-interactive database privacy. In

Proceedings of the 40th annual ACM symposium on Theory of computing, STOC '08.

[3] H. Brenner and K. Nissim. Impossibility of differentially private universally optimal mechanisms. *Foundations of Computer Science, Annual IEEE Symposium on*, 2010.

[4] I. Dinur and K. Nissim. Revealing information while preserving privacy. In *In PODS*, 2003.

[5] C. Dwork. Differential privacy. In *in ICALP*, pages 1–12. Springer, 2006.

[6] C. Dwork. Differential privacy: a survey of results. In *Proceedings of the 5th international conference on Theory and applications of models of computation*, TAMC'08, 2008.

[7] C. Dwork, F. Mcsherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, 2006.

[8] C. Dwork and K. Nissim. Privacy-preserving datamining on vertically partitioned databases. In *In CRYPTO*, 2004.

[9] A. Ghosh, T. Roughgarden, and M. Sundararajan. Universally utility-maximizing privacy mechanisms. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, 2009.

[10] M. Gupte and M. Sundararajan. Universally optimal privacy mechanisms for minimax agents. In *Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems of data*, PODS '10, 2010.

[11] M. Hardt and K. Talwar. On the geometry of differential privacy. In *Proceedings of the 42nd ACM symposium on Theory of computing*, 2010.

[12] M. Hay, V. Rastogi, G. Miklau, and D. Suciu. Boosting the accuracy of differentially-private queries through consistency. In *VLDB*, 2010.

[13] D. Kifer and B.-R. Lin. Towards an axiomatization of statistical privacy and utility. In *Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, PODS '10, 2010.

[14] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor. Optimizing histogram queries under differential privacy. In *PODS*, 2010.

[15] F. McSherry and K. Talwar. Mechanism design via differential privacy. In *FOCS '07: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, 2007.

[16] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, 2007.

APPENDIX

A. LEGAL FUNCTIONS

In section 2, we assume a differentially private mechanism for range/threshold queries is count-oriented. However, that assumption excludes some differentially private mechanisms for threshold queries, which depends on the database itself and not merely the count. To characterize such a mechanism, let X be a differentially private mechanism for threshold queries where x_τ is the probability of X to output *yes* when the underlying database is τ. An obvious way to proceed with this definition is to assume that a consumer's error penalty function ω and prior distribution ρ also depend on databases. For ease of exposition, we only consider the case for threshold queries $\langle p, \theta, +\infty \rangle$ as the other two cases can be proved analogously.

More precisely, let S_i be the set of database instances with count i for the threshold query, and the weighted error of X is:

$$\sum_{i=0}^{\theta-1} \sum_{\tau \in S_i} \omega(\tau)\rho(\tau)x_\tau + \sum_{j=\theta}^{n} \sum_{\tau \in S_j} \omega(\tau)\rho(\tau)(1 - x_\tau). \tag{7}$$

There are two reasons that we do not employ the utility model shown in (7): first, given the large number of possible database instances, it is very hard for a consumer to model either a prior knowledge or error penalty function over the database instances. Second, there is no utility maximizing differentially private mechanism for threshold queries with that utility model. This is shown in Theorem 8.

THEOREM 8. *If a consumer's prior distribution or error penalty function depends on the database instance itself, and not merely the count result of the threshold query, then there is no utility maximizing differential private mechanism for threshold queries.*

PROOF. We set the domain $D = \{0, 1\}$, and $n = 2$. The possible database instances are $(0, 0), (1, 0), (1, 1), (0, 1)$, each with two rows. Consider a threshold query with the threshold $\theta = 1$ and the following predicate on a row: it is the first row and that row is $1 \in D$. Thus the correct answer to the threshold query is *no* for the first and the last database instances and *yes* for the other two. We shall represent the optimal differentially private mechanism for that query by a vector $\mathbf{z} = (z_{(0,0)}, z_{(1,0)}, z_{(1,1)}, z_{(0,1)})^t$, which are the probabilities of returning *yes* in each case. By the proof of Lemma 11 in Appendix E, there is a consumer whose unique optimal mechanism is: $\mathbf{z_1} = (1/(\alpha+1), \alpha/(\alpha+1), \alpha/(\alpha+1), 1/(\alpha+1))^t$. By the proof of Lemma 12, there is also another consumer whose unique optimal mechanism is $\mathbf{z_2} = (1/(\alpha(\alpha+1)), 1/(\alpha+1), \alpha/(\alpha+1), 1/(\alpha+1))^t$. By Theorem 3, no differentially private mechanism can simultaneously maximize both consumers' utilities. $\square$

Therefore, our utility model shall still assume that both a consumer's error penalty function and prior distribution only depend on the count of a threshold query, rather than a richer expression over databases. Then we can define $\rho(i) = \sum_{\tau \in S_i} \rho(\tau) = |S_i|\rho(\tau)$ where for any $\tau \in S_i$, $\rho(\tau)$ is the consumer's a priori probability that τ has count i, and $\omega(i) = \omega(\tau)$ which is the error penalty for any $\tau \in S_i$. Thus, the weighted error of the mechanism X is:

$$\sum_{i=0}^{\theta-1} \frac{\rho(i)\omega(i)}{|S_i|} \sum_{\tau \in S_i} x_\tau + \sum_{j=\theta}^{n} \frac{\rho(j)\omega(j)}{|S_j|} \sum_{\tau \in S_j} (1 - x_\tau). \tag{8}$$

Then, we will prove that in this case, without loss of generality we may focus on count-oriented differentially private mechanisms. This is shown in Theorem 9.

THEOREM 9. *There exists a legal function ϕ whose weighted error is the same as X in (8) for the same consumer.*

PROOF. We construct a function ϕ as follows: for any integer μ, $0 \le \mu \le n$,

$$\phi(\mu) = \frac{\sum_{\tau \in S_\mu} x_\tau}{|S_\mu|}$$

where S_i is the set of database instances whose counts for a threshold query are i.

We claim that ϕ is a legal function. It is obvious that for all $0 \le \mu \le n, 0 \le \phi(\mu) \le 1$. Thus, it suffices to prove that the requirement of differential privacy is satisfied. We start by proving that for all $0 \le i < n$, $\phi(i+1)/\alpha \le \phi(i) \le \alpha\phi(i+1)$.

We construct a bipartite graph (V, W, E) between neighboring databases as follows: let $V = S_i, W = S_{i+1}$ and E denote all pairs (τ_1, τ_2) of neighboring databases where $\tau_1 \in V$ and $\tau_2 \in W$. The neighbors in W of a database $\tau_1 \in V$ are the databases that can be obtained by changing the value of a row that does not satisfy the given predicate in the threshold query to the one that does. Therefore, (V, W, E) is a bipartite graph, which is left-regular with degree $a = (n-i)t$ where t is the number of elements of D that satisfy the predicate of the given threshold query. Similarly, (V, W, E) is right-regular with degree $b = (i+1)(|D| - t)$. By the requirement of differential privacy, x_{τ_1} lies between αx_{τ_2} and x_{τ_2}/α for each pair of neighboring databases τ_1 and τ_2. Summing over all such pairs yields:

$$a \sum_{\tau_1 \in V} x_{\tau_1} = \sum_{(\tau_1,\tau_2)\in E} x_{\tau_1} \leq \sum_{(\tau_1,\tau_2)\in E} \alpha x_{\tau_2} = b\alpha \sum_{\tau_2 \in W} x_{\tau_2}$$

and dividing through by $|E| = a|V| = b|W|$ gives

$$\frac{\sum_{\tau_1 \in V} x_{\tau_1}}{|V|} \leq \alpha \frac{\sum_{\tau_2 \in W} x_{\tau_2}}{|W|}.$$

Thus, $\phi(i) \leq \alpha\phi(i+1)$. Similarly, we can prove $\phi(i) \geq \phi(i+1)/\alpha$, and for all $0 \leq i < n$, $(1-\phi(i+1))/\alpha \leq 1-\phi(i) \leq \alpha(1-\phi(i+1))$. Therefore, ϕ is a legal function.

Equation (8) becomes

$$\sum_{i=0}^{i=\theta-1} \rho(i)\omega(i)\phi(i) + \sum_{j=\theta}^{j=n} \rho(j)\omega(j)(1-\phi(j)).$$

The theorem follows. $\square$

Hence, our assumption that a differentially private mechanism for threshold queries is count-oriented is necessary and without loss of generality for the design of an optimal mechanism for threshold queries. Similarly, We can also prove the same statement for count-range queries.

B. CHARACTERIZING OPTIMAL LEGAL FUNCTIONS FOR THRESHOLD QUERIES

B.1 Monotonicity

We start by proving that there is an optimal legal function for threshold queries that is monotonically non-decreasing in the count.

THEOREM 10. *For any error penalty function ω and any prior distribution ρ, there is an optimal legal function such that for any integer $0 \leq \mu_1 < \mu_2 \leq n$,*

$$\phi^*(\mu_1) \leq \phi^*(\mu_2).$$

PROOF. Assume that there exists an optimal legal function ϕ that is not monotonically non-decreasing in the count μ. Let μ^* be the smallest integer such that $\phi(\mu^*-1) > \phi(\mu^*)$. Therefore, $\phi(\mu^*-2) \leq \phi(\mu^*-1)$ if $\mu^* \geq 2$. We consider two cases:

1. $\mu^* \leq \theta$. We construct another function ϕ' as follows:

$$\phi'(\mu) = \begin{cases} \phi(\mu^*) & \text{if } \mu = \mu^*-1 \\ \phi(\mu) & \text{otherwise.} \end{cases}$$

   First, we prove that the function ϕ' is a legal function.

   (a) $\mu^* = 1$, it is trivial to show that ϕ' is a legal function.

   (b) $\mu^* > 1$. It suffices to prove that the requirement of differential privacy is satisfied when $\mu = \mu^*-2$ and $\mu = \mu^*-1$. At $\mu = \mu^*-1$ this is trivial, as $\phi'(\mu^*-1) = \phi'(\mu^*)$.

$$\begin{aligned} \phi'(\mu^*-2) = \phi(\mu^*-2) &\leq \phi(\mu^*-1) \leq \alpha\phi(\mu^*) = \alpha\phi'(\mu^*-1) \\ \phi'(\mu^*-2) = \phi(\mu^*-2) &\geq \frac{1}{\alpha}\phi(\mu^*-1) > \frac{1}{\alpha}\phi(\mu^*) = \frac{1}{\alpha}\phi'(\mu^*-1) \\ 1-\phi'(\mu^*-2) = 1-\phi(\mu^*-2) &\leq \alpha(1-\phi(\mu^*-1)) < \alpha(1-\phi(\mu^*)) = \alpha(1-\phi'(\mu^*-1)) \\ 1-\phi'(\mu^*-2) = 1-\phi(\mu^*-2) &\geq 1-\phi(\mu^*-1) \geq \frac{1}{\alpha}(1-\phi(\mu^*)) = \frac{1}{\alpha}(1-\phi'(\mu^*-1)) \end{aligned}$$

   Since the range of ϕ' is clearly within $[0, 1]$, ϕ' is a legal function.

For both cases, $err(\phi') \leq err(\phi)$, since the difference is exactly $\rho(\mu^*-1)\omega(\mu^*-1)(\phi(\mu^*)-\phi(\mu^*-1))$.

2. $\mu^* > \theta$. Let μ' be the largest integer ($\theta < \mu' \leq n$) such that $\phi(\mu'-1) > \phi(\mu')$. We construct another function ϕ' as follows:

$$\phi'(\mu) = \begin{cases} \phi(\mu'-1) & \text{if } \mu = \mu' \\ \phi(\mu) & \text{otherwise.} \end{cases}$$

By symmetry, similar to the proof of case 1, ϕ' is also a legal function, and $err(\phi') \leq err(\phi)$.

ϕ' has more monotonic steps than ϕ for $0 \leq \mu \leq n$. If ϕ' is not monotonically non-decreasing, we can repeat the argument and construct a function ϕ'' from ϕ', and by the proof above, $err(\phi'') \leq err(\phi')$. Repeat this until we obtain a monotonically non-decreasing function ϕ^*, and $err(\phi^*) \leq err(\phi)$. Therefore, ϕ^* is also an optimal legal function. $\square$

B.2 Consumer Dependent Optimality

Ideally, we may wish to find a legal function that maximizes the utility for every consumer. More formally, we can define a partial order $\preceq$ on the set of legal functions Ω.

DEFINITION 8. *(Partial order $\preceq$ on Ω): Given two legal functions $\phi_1, \phi_2 \in \Omega$, we define: $\phi_1 \preceq \phi_2$, if and only if for any integer μ, if $0 \leq \mu < \theta$, $F^+_{\phi_1}(\mu) \leq F^+_{\phi_2}(\mu)$ and if $\theta \leq \mu \leq n$, $F^-_{\phi_1}(\mu) \leq F^-_{\phi_2}(\mu)$*

It is clear that Ω is a partially ordered set by $\preceq$. Unfortunately, there is no *least* element in Ω, which would be a universally optimal legal function.

THEOREM 11. *There is no least element in Ω under $\preceq$.*

PROOF. We prove Theorem 11 by contradiction. Assume that ϕ^* is the least element in Ω. Therefore, $\forall \phi \in \Omega$, $\phi^* \preceq \phi$. Because ϕ^* is the least element, clearly ϕ^* is not identically zero, since, for example the zero function $\not\preceq$ the constant function $\phi'(\mu) = \frac{1}{2}$.

By the requirement of differential privacy, for any integer j, $0 \leq j \leq n$, $\phi^*(j) > 0$. We construct a constant function ϕ': $\phi'(\mu) = \phi^*(0)/2$. It is easy to verify that ϕ' is also a legal function, and $F^+_{\phi'}(0) < F^+_{\phi^*}(0)$ if $\theta > 0$, a contradiction. $\square$

B.3 Characterizing Optimal Legal Functions

Let Ω_σ be the subset of monotonically non-decreasing functions in Ω such that, $\phi(\theta) = \sigma$ ($0 \leq \sigma \leq 1$). Then, we prove that the following function ϕ_σ is a least element in Ω_σ: for any integer μ, $0 \leq \mu < n$,

$$\phi_\sigma(\mu+1) = \min\{\alpha\phi_\sigma(\mu), \frac{\alpha - 1 + \phi_\sigma(\mu)}{\alpha}\} \quad (9)$$

and $\phi_\sigma(\theta) = \sigma$.

This first-order linear recurrence can be understood as follows: First note that following either alternatives, the function is monotonically increasing. Now $\alpha\phi_\sigma(\mu) \leq \frac{\alpha-1+\phi_\sigma(\mu)}{\alpha}$ iff $\phi_\sigma(\mu) \leq \frac{1}{\alpha+1}$, in which case $\phi_\sigma(\mu+1) = \alpha\phi_\sigma(\mu) \leq \frac{\alpha}{\alpha+1}$. Conversely, if $\phi_\sigma(\mu+1) \leq \frac{\alpha}{\alpha+1}$, then $\phi_\sigma(\mu) \leq \frac{1}{\alpha+1}$, for otherwise we would have $\phi_\sigma(\mu+1) = \frac{\alpha-1+\phi_\sigma(\mu)}{\alpha} > \frac{\alpha}{\alpha+1}$. So in this case, $\phi_\sigma(\mu+1) = \alpha\phi_\sigma(\mu)$. In other words, the first alternative holds in (9) iff $\phi_\sigma(\mu) \leq \frac{1}{\alpha+1}$, and also iff $\phi_\sigma(\mu+1) \leq \frac{\alpha}{\alpha+1}$. Thus, given $\phi_\sigma(\theta) = \sigma$, (9) defines ϕ_σ uniquely not only forward for $\mu > \theta$, but also backward for $\mu < \theta$. It is also clear from the definition that (9) ensures differential privacy.

We will prove that ϕ_σ is the least element in Ω_σ.

LEMMA 4. *For all $\phi \in \Omega_\sigma$, if there is an integer μ', such that $\phi(\mu') \leq \phi_\sigma(\mu')$, then, for all $\mu \geq \mu'$, $\phi(\mu) \leq \phi_\sigma(\mu)$, and "=" holds only if $\phi(\mu') = \phi_\sigma(\mu')$.*

PROOF. We prove Lemma 4 by induction. The base case $\mu = \mu'$ is given. Assume for $\mu \geq \mu'$, $\phi(\mu) \leq \phi_\sigma(\mu)$ and "=" holds only if $\phi(\mu') = \phi_\sigma(\mu')$. By differential privacy:

$$\phi(\mu+1) \leq \min\{\alpha\phi(\mu), \frac{\alpha - 1 + \phi(\mu)}{\alpha}\}$$

Therefore,

$$\phi(\mu+1) \leq \min\{\alpha\phi(\mu), \frac{\alpha-1+\phi(\mu)}{\alpha}\} \leq \min\{\alpha\phi_\sigma(\mu), \frac{\alpha-1+\phi_\sigma(\mu)}{\alpha}\} = \phi_\sigma(\mu+1)$$

The second "$\leq$" is because of our induction assumption that $\phi(\mu) \leq \phi_\sigma(\mu)$, and "=" holds only if $\phi(\mu') = \phi_\sigma(\mu')$. □

COROLLARY 4. *$\forall \phi \in \Omega_\sigma$, for any integer $\mu, \theta \leq \mu \leq n$, $F^-_{\phi_\sigma}(\mu) \leq F^-_\phi(\mu)$.*

PROOF. Since $\phi(\theta) = \phi_\sigma(\theta) = \sigma$, by Lemma 4, the corollary follows. □

COROLLARY 5. *$\forall \phi \in \Omega_\sigma$, for any integer μ, $0 \leq \mu < \theta$, $F^+_{\phi_\sigma}(\mu) \leq F^+_\phi(\mu)$.*

PROOF. We prove Corollary 5 by contradiction. Assume that there is an integer $i, 0 \leq i < \theta$, such that, $\phi(i) < \phi_\sigma(i)$. By Lemma 4, for all $\mu \geq i$, $\phi(\mu) < \phi_\sigma(\mu)$. Therefore, $\phi(\theta) = \sigma < \phi_\sigma(\theta) = \sigma$, a contradiction. Hence, for all $0 \leq \mu < \theta$, $\phi_\sigma(\mu) \leq \phi(\mu)$. The corollary follows. □

Since ϕ_σ minimizes the probability of both types of errors in Ω_σ, ϕ_σ is the least element in Ω_σ.

THEOREM 12. *ϕ_σ is the least element in Ω_σ*

We can prove Theorem 6 in a similar way.

C. UNIVERSALLY UTILITY MAXIMIZING MECHANISM

The range-restricted geometric mechanism can be represented as a row-stochastic matrix M of size $(n+1) \times (n+1)$ whose element is defined by $m_{i,j} = \Pr[Z(i) = j]$, for $0 \leq i, j \leq n$, where the random variable $Z(i)$ is drawn from the range-restricted geometric mechanism defined in (6).

The matrix M is given in (10). To prove Theorem 7, we first show that M is invertible. Then we show that for every optimal legal function for a threshold query, which is characterized by a vector $\mathbf{z} = (z_0, z_1, \ldots, z_n)^t$ satisfying Theorem 5, if we set $\mathbf{t} = M^{-1} \circ \mathbf{z} = (t_0, \ldots, t_n)^t$, then each $t_i \in [0, 1]$.

LEMMA 5.

$$\det(M) = \frac{(\alpha-1)^{2n-1}}{\alpha^{2n-2}(\alpha+1)} > 0.$$

PROOF. The matrix M is of the form shown in Equation (10).

$$M = \frac{\alpha-1}{\alpha+1} \begin{pmatrix} \frac{\alpha}{\alpha-1}\cdot 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n} \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-1} & 1 & \alpha^{-1} & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n+1} \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-2} & \alpha^{-1} & 1 & \cdots & \frac{\alpha}{\alpha-1}\cdot\alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha}{\alpha-1}\cdot\alpha^{-n} & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & \frac{\alpha}{\alpha-1}\cdot 1 \end{pmatrix} \tag{10}$$

Thus,

$$\det(M) = \left(\frac{\alpha-1}{\alpha+1}\right)^{n+1} \left(\frac{\alpha}{\alpha-1}\right)^2 \det(M') = \frac{\alpha^2(\alpha-1)^{n-1}}{(\alpha+1)^{n+1}} \det(M')$$

where M' is the symmetric matrix shown in (11).

$$M' = \begin{pmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-n} \\ \alpha^{-1} & 1 & \alpha^{-1} & \cdots & \alpha^{-n+1} \\ \alpha^{-2} & \alpha^{-1} & 1 & \vdots & \alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{-n} & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & 1 \end{pmatrix} \tag{11}$$

Let C_i be the i^{th} column in M'. For the column index i from 0 up to $n-1$, do the column transformation for each column: $C_i := C_i - \alpha^{-1}C_{i+1}$.

$$\det(M') = \begin{vmatrix} 1-\alpha^{-2} & \alpha^{-1}-\alpha^{-3} & \alpha^{-2}-\alpha^{-4} & \cdots & \alpha^{-n} \\ 0 & 1-\alpha^{-2} & \alpha^{-1}-\alpha^{-3} & \cdots & \alpha^{-n+1} \\ 0 & 0 & 1-\alpha^{-2} & \cdots & \alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = (1-\alpha^{-2})^n$$

The lemma follows. $\square$

We shall use Cramer's rule to complete the proof of Theorem 7. Given the vector $\mathbf{z}$ satisfying Theorem 5, let M_i be the matrix obtained from M by replacing the i^{th} column of M by $\mathbf{z}$. By Cramer's rule, if $\mathbf{t} = M^{-1} \circ \mathbf{z} = (t_0, t_1, \ldots, t_n)^t$, then $t_i = \det(M_i)/\det(M)$. We will prove that $0 \le t_i \le 1$, for all $0 \le i \le n$.

Lemma 6. *For all* $0 \le i \le n$, $t_i \in [0,1]$.

Proof. Since $\det(M)$ has been computed by Lemma 5, we only need to compute $\det(M_i)$. Let M'_i be the matrix obtained from M' by replacing the i^{th} column of M' by $\mathbf{z}$, and let C^i_j be the j^{th} column in the matrix M'_i. We consider three cases:

1. $i = 0$.

$$\det(M_0) = \left(\frac{\alpha-1}{\alpha+1}\right)^{n-1} \left(\frac{\alpha}{\alpha+1}\right) \det(M'_0)$$

where

$$M'_0 = \begin{pmatrix} z_0 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-n} \\ z_1 & 1 & \alpha^{-1} & \cdots & \alpha^{-n+1} \\ z_2 & \alpha^{-1} & 1 & \cdots & \alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & 1 \end{pmatrix}$$

For $j = n$ down to 2, perform the column transformations: $C^0_j := C^0_j - \alpha^{-1}C^0_{j-1}$, we get:

$$\begin{pmatrix} z_0 & \alpha^{-1} & 0 & \cdots & 0 \\ z_1 & 1 & 0 & \cdots & 0 \\ z_2 & \alpha^{-1} & 1-\alpha^{-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_n & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & 1-\alpha^{-2} \end{pmatrix}$$

Hence

$$\det(M'_0) = (1-\alpha^{-2})^{n-1} \begin{vmatrix} z_0 & \alpha^{-1} \\ z_1 & 1 \end{vmatrix}$$

It follows that

$$\frac{\det(M_0)}{\det(M)} = \frac{\alpha}{\alpha-1} \begin{vmatrix} z_0 & \alpha^{-1} \\ z_1 & 1 \end{vmatrix}$$

We can rewrite the constraint $z_j = \min\{\alpha z_{j-1}, (\alpha - 1 + z_{j-1})/\alpha\}$ as:

$$z_j = \begin{cases} \alpha z_{j-1} & \text{if } z_{j-1} \le 1/(\alpha+1) \\ \frac{\alpha-1+z_{j-1}}{\alpha} & \text{otherwise.} \end{cases}$$

Thus,

$$\begin{vmatrix} z_0 & \alpha^{-1} \\ z_1 & 1 \end{vmatrix} = \begin{cases} 0 & \text{if } z_0 \le 1/(\alpha+1) \\ \frac{(\alpha-1)[(\alpha+1)z_0-1]}{\alpha^2} & \text{otherwise.} \end{cases}$$

Hence,

$$\frac{\det(M_0)}{\det(M)} = \begin{cases} 0 & \text{if } z_0 \le 1/(\alpha+1) \\ \frac{[(\alpha+1)z_0-1]}{\alpha} & \text{otherwise.} \end{cases}$$

When $z_0 > 1/(1+\alpha)$, recall that $z_0 \le 1$ since it is a probability, we have $[(\alpha+1)z_0 - 1]/\alpha \in (0,1]$. Thus, $0 \le \det(M_0)/\det(M) \le 1$.

2. $i = n$.

$$\det(M_n) = \left(\frac{\alpha-1}{\alpha+1}\right)^{n-1} \left(\frac{\alpha}{\alpha+1}\right) \det(M_n')$$

where

$$M_n' = \begin{pmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & z_0 \\ \alpha^{-1} & 1 & \alpha^{-1} & \cdots & z_1 \\ \alpha^{-2} & \alpha^{-1} & 1 & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{-n} & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & z_n \end{pmatrix}$$

For $j = 0$ up to $n-2$, perform the column transformations on the matrix M_n': $C_j^n := C_j^n - \alpha^{-1}C_{j+1}^n$. We get

$$\det(M_n') = (1-\alpha^{-2})^{n-1} \cdot \begin{vmatrix} 1 & z_{n-1} \\ \alpha^{-1} & z_n \end{vmatrix}.$$

Then, the proof is similar to the case when $i = 0$.

3. $0 < i < n$.

$$\det(M_i) = \left(\frac{\alpha-1}{\alpha+1}\right)^{n-2} \left(\frac{\alpha}{\alpha+1}\right)^2 \det(M_i')$$

where

$$M_i' = \begin{pmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-i+1} & z_0 & \alpha^{-i-1} & \cdots & \alpha^{-n} \\ \alpha^{-1} & 1 & \alpha^{-1} & \cdots & \alpha^{-i+2} & z_1 & \alpha^{-i} & \cdots & \alpha^{-n+1} \\ \alpha^{-2} & \alpha^{-1} & 1 & \cdots & \alpha^{-i+3} & z_2 & \alpha^{-i+1} & \cdots & \alpha^{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^{-n} & \alpha^{-n+1} & \alpha^{-n+2} & \cdots & \alpha^{-n+i-1} & z_n & \alpha^{-n+i+1} & \cdots & 1 \end{pmatrix}$$

If $i \ge 2$, then for $j = 0$ up to $i-2$, perform the column transformations on the matrix M_i': $C_j^i := C_j^i - \alpha^{-1}C_{j+1}^i$. This will create a square matrix whose upper left $(i-1)\times(i-1)$ block is an upper triangular matrix with diagonals all equal to $1-\alpha^{-2}$, and its lower left $(n-i+2)\times(i-1)$ block is identically zero. Then, if $i \le n-2$, for $j = n$ down to $i+2$, perform the column transformations $C_j^i := C_j^i - \alpha^{-1}C_{j-1}^i$. This will further change the square matrix for columns $i+2$ to n, without changing columns 0 to $i+1$. The lower right $(n-i-1)\times(n-i-1)$ block has become a lower triangular matrix with diagonals all equal to $1-\alpha^{-2}$, and its upper right $(i+2)\times(n-i-1)$ block is identically zero. The columns indexed by $i-1, i, i+1$ are unchanged. From that we get:

$$\begin{pmatrix} 1-\alpha^{-2} & \alpha^{-1}(1-\alpha^{-2}) & \cdots & \alpha^{-i+2}(1-\alpha^{-2}) & \alpha^{-i+1} & z_0 & \alpha^{-i-1} & 0 & \cdots & 0 \\ 0 & 1-\alpha^{-2} & \cdots & \alpha^{-i+3}(1-\alpha^{-2}) & \alpha^{-i+2} & z_1 & \alpha^{-i} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1-\alpha^{-2} & \alpha^{-1} & z_{i-2} & \alpha^{-3} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & z_{i-1} & \alpha^{-2} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha^{-1} & z_i & \alpha^{-1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha^{-2} & z_{i+1} & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha^{-3} & z_{i+2} & \alpha^{-1} & 1-\alpha^{-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \alpha^{-n+i-1} & z_n & \alpha^{-n+i+1} & \alpha^{-n+i+2}(1-\alpha^{-2}) & \cdots & 1-\alpha^{-2} \end{pmatrix}$$

Therefore,

$$\det(M_i') = (1-\alpha^{-2})^{n-2} \begin{vmatrix} 1 & z_{i-1} & \alpha^{-2} \\ \alpha^{-1} & z_i & \alpha^{-1} \\ \alpha^{-2} & z_{i+1} & 1 \end{vmatrix}$$

Now we consider three cases, according to the magnitude of z_i.

(a) If $z_i \le 1/(\alpha+1)$, then $z_i = \alpha z_{i-1} = z_{i+1}/\alpha$. Therefore,

$$\begin{vmatrix} 1 & z_{i-1} & \alpha^{-2} \\ \alpha^{-1} & z_i & \alpha^{-1} \\ \alpha^{-2} & z_{i+1} & 1 \end{vmatrix} = z_{i-1} \begin{vmatrix} 1 & 1 & \alpha^{-2} \\ \alpha^{-1} & \alpha & \alpha^{-1} \\ \alpha^{-2} & \alpha^2 & 1 \end{vmatrix} = 0.$$

Thus,

$$\frac{\det(M_i)}{\det(M)} = 0.$$

(b) If $z_i \ge \alpha/(\alpha+1)$, then it is not difficult to show that $1 - z_i = \alpha(1 - z_{i+1}) = (1 - z_{i-1})/\alpha$. Therefore,

$$\begin{vmatrix} 1 & z_{i-1} & \alpha^{-2} \\ \alpha^{-1} & z_i & \alpha^{-1} \\ \alpha^{-2} & z_{i+1} & 1 \end{vmatrix} = \frac{(\alpha-1)^3(\alpha+1)}{\alpha^4}$$

Then it follows that

$$\frac{\det(M_i)}{\det(M)} = 1.$$

(c) If $1/(\alpha+1) < z_i < \alpha/(\alpha+1)$, then similarly it is easy to show that $z_i = \alpha z_{i-1}$, and $1 - z_i = \alpha(1 - z_{i+1})$. Thus,

$$\begin{vmatrix} 1 & z_{i-1} & \alpha^{-2} \\ \alpha^{-1} & z_i & \alpha^{-1} \\ \alpha^{-2} & z_{i+1} & 1 \end{vmatrix} = \frac{(\alpha-1)^2(\alpha+1)[(\alpha+1)z_i - 1]}{\alpha^4}.$$

Therefore,

$$\frac{\det(M_i)}{\det(M)} = \frac{(\alpha+1)z_i - 1}{\alpha - 1}.$$

Since $1/(\alpha+1) < z_i < \alpha/(\alpha+1)$, $0 < \det(M_i)/\det(M) < 1$.

Therefore, in all cases, $\det(M_i)/\det(M) \in [0, 1]$.

□

We can prove the same result for threshold queries $\langle p, 0, \theta\rangle$ in a similar way, and we omit the details here.

D. CHARACTERIZING OPTIMAL LEGAL FUNCTIONS FOR COUNT RANGE QUERIES

Given an error penalty function ω and a prior distribution ρ, let ϕ^* be an optimal legal function for the count range query $\langle p, \theta_1, \theta_2\rangle$. We start by exploring the property of optimal legal functions for count range queries.

D.1 Monotonicity

Unlike the case for threshold queries, ϕ^* is not monotonic over the whole domain $\{0, \ldots, n\}$.

D.1.1 Monotonic Intervals

When the count μ is less than the small threshold θ_1, ϕ^* is monotonically non-decreasing in μ as shown in Lemma 7.

LEMMA 7. *For any integer μ, $1 \le \mu < \theta_1$, $\phi^*(\mu - 1) \le \phi^*(\mu)$.*

PROOF. The proof is similar to Theorem 10. We omit the details here. □

By symmetry, we can also prove that ϕ^* is monotonically non-increasing in μ when $\theta_2 < \mu \le n$.

LEMMA 8. *For any integer μ, $\theta_2 + 1 < \mu \le n$, $\phi^*(\mu - 1) \ge \phi^*(\mu)$.*

D.1.2 Non-monotonic Intervals

For the domain $\{\theta_1, \dots, \theta_2\}$, we will prove that ϕ^* is first monotonically non-decreasing and then monotonically non-increasing.

LEMMA 9. *There are no three consecutive integers μ_1, μ_2, μ_3, $\theta_1 \leq \mu_1 < \mu_2 < \mu_3 \leq \theta_2$ such that:*

$$\phi^*(\mu_1) > \phi^*(\mu_2) \wedge \phi^*(\mu_2) \leq \phi^*(\mu_3) \tag{12}$$

or

$$\phi^*(\mu_1) \geq \phi^*(\mu_2) \wedge \phi^*(\mu_2) < \phi^*(\mu_3) \tag{13}$$

PROOF. Assume that there is an optimal legal function ϕ and such three consecutive integers exist. We consider two cases:

1. There are three consecutive integers $\mu_1 < \mu_2 < \mu_3$ satisfying (12). We construct a function ϕ' as follows:

$$\phi'(\mu) = \begin{cases} \phi(\mu) & \text{if } \mu \neq \mu_2 \\ \phi(\mu_1) & \text{otherwise.} \end{cases}$$

First, we prove that ϕ' is a legal function. It suffices to prove that the requirement of differential privacy is satisfied when $\mu = \mu_2$ and $\mu = \mu_3$. At $\mu = \mu_1$, this is trivial, as $\phi'(\mu_1) = \phi'(\mu_2)$.

$$\begin{aligned}
\phi'(\mu_2) = \phi(\mu_1) \leq \alpha\phi(\mu_2) \leq \alpha\phi(\mu_3) = \alpha\phi'(\mu_3) \\
\phi'(\mu_2) = \phi(\mu_1) > \phi(\mu_2) \geq \frac{1}{\alpha}\phi(\mu_3) = \frac{1}{\alpha}\phi'(\mu_3) \\
1 - \phi'(\mu_2) = 1 - \phi(\mu_1) < 1 - \phi(\mu_2) \leq \alpha(1 - \phi(\mu_3)) = \alpha(1 - \phi'(\mu_3)) \\
1 - \phi'(\mu_2) = 1 - \phi(\mu_1) \geq \frac{1}{\alpha}(1 - \phi(\mu_2)) \geq \frac{1}{\alpha}(1 - \phi(\mu_3)) = \frac{1}{\alpha}(1 - \phi'(\mu_3))
\end{aligned}$$

Hence, ϕ' satisfies differential privacy when $\mu = \mu_2$ and $\mu = \mu_3$. Since the range of ϕ' is clearly $[0, 1]$, ϕ' is a legal function, and $err(\phi') \leq err(\phi)$ because the difference is exactly $\omega(\mu_2)\rho(\mu_2)(\phi(\mu_2) - \phi(\mu_1))$.

2. There are three consecutive integers $\mu_1 < \mu_2 < \mu_3$ satisfying (13). We construct another function ϕ' as follows:

$$\phi'(\mu) = \begin{cases} \phi(\mu) & \text{if } \mu \neq \mu_2 \\ \phi(\mu_3) & \text{otherwise.} \end{cases}$$

Similarly, we can prove that ϕ' is a legal function, and $err(\phi') \leq err(\phi)$.

Since ϕ' has less number of integers satisfying either (12) or (13) than ϕ, if there are still three consecutive integers satisfying either (12) or (13) in ϕ', we can repeat the argument and construct a function ϕ'' from ϕ', and by the proof above, $err(\phi'') \leq err(\phi')$. Repeat this until we obtain a function ϕ^* such that there are no three consecutive integers satisfying either (12) or (13), and $err(\phi^*) \leq err(\phi)$. Therefore, ϕ^* is also an optimal legal function. $\square$

By Lemma 9, we can prove that the optimal legal functions must be first monotonically non-decreasing and then monotonically non-increasing over the domain $\{\theta_1, \dots, \theta_2\}$ as shown in Corollary 6.

COROLLARY 6. *There is an integer $\gamma, \theta_1 \leq \gamma \leq \theta_2$, such that ϕ^* is monotonically non-decreasing over μ when $\theta_1 \leq \mu \leq \gamma$, and monotonically non-increasing when $\gamma + 1 \leq \mu \leq \theta_2$.*

PROOF. Let $\phi^*(\gamma)$ be the maximum value of ϕ^* over the domain $\{\theta_1, \dots, \theta_2\}$. We start by claiming that ϕ^* is monotonically non-decreasing over $\{\theta_1, \dots, \gamma\}$. We prove that claim by contradiction. Assume that claim is false. Let μ $(\theta_1 + 1 \leq \mu \leq \gamma)$ be the largest integer such that $\phi^*(\mu - 1) > \phi^*(\mu)$. Therefore, $\mu \leq \gamma - 1$ or else $\phi^*(\gamma)$ is not the maximum value. Since $\phi^*(\mu) \leq \phi^*(\mu + 1)$, for three consecutive integers $\mu - 1, \mu, \mu + 1$ $(\mu + 1 \leq \gamma \leq \theta_2$, $\mu - 1 \geq \theta_1)$,

$$\phi^*(\mu - 1) > \phi^*(\mu) \wedge \phi^*(\mu) \leq \phi^*(\mu + 1)$$

which is in contradiction to Lemma 9. Therefore, ϕ^* is monotonically non-decreasing over $\{\theta_1, \dots, \gamma\}$. Similarly, we can prove that ϕ^* is monotonically non-increasing over $\{\gamma + 1, \dots, \theta_2\}$. $\square$

D.2 Optimal Legal Functions for Range Queries

By Lemma 7, Lemma 8 and Corollary 6, we conclude that there is an optimal legal function for count range queries that is first monotonically non-decreasing and then monotonically non-increasing over the domain $\{0, \ldots, n\}$.

THEOREM 13. *There is an integer $\gamma, \theta_1 \leq \gamma \leq \theta_2$, such that ϕ^* is monotonically non-decreasing in μ when $0 \leq \mu \leq \gamma$, and monotonically non-increasing when $\gamma + 1 \leq \mu \leq n$.*

Next, we construct a function ϕ_{δ_1,δ_2} as follows:

$$\phi_{\delta_1,\delta_2}(\mu) = \min\{\psi_1(\mu), \psi_2(\mu)\}$$

where ψ_1 and ψ_2 satisfy (2) and (3), respectively, and $\psi_1(\theta_1) = \delta_1$, $\psi_2(\theta_2) = \delta_2$. Therefore, For any integer μ,

$$\psi_1(\mu) = \min\{\alpha\psi_1(\mu-1), \frac{\alpha - 1 + \psi_1(\mu-1)}{\alpha}\}$$
$$\psi_2(\mu) = \max\{\frac{1}{\alpha}\psi_2(\mu-1), 1 - \alpha + \alpha\psi_2(\mu-1)\}$$

It is easy to see that ϕ_{δ_1,δ_2} is well-defined. First, we prove that ϕ_{δ_1,δ_2} is a legal function.

LEMMA 10. *$\forall \delta_1, \delta_2 \in [0, 1]$, ϕ_{δ_1,δ_2} is a legal function.*

PROOF. We consider two cases:

1. $\delta_1 = 0, 1$ or $\delta_2 = 0, 1$. Without loss of generality, let $\delta_1 = 0$ (1). Therefore, $\phi_{\delta_1,\delta_2}(\mu) = 0(\psi_2(\mu))$. For both cases, it is trivial to show that ϕ_{δ_1,δ_2} is a legal function.
2. $\delta_1, \delta_2 \in (0, 1)$. It is not difficult to show that for any integer μ, $0 < \psi_1(\mu), \psi_2(\mu) < 1$,and ψ_1 is strictly monotonically increasing in μ while ψ_2 is strictly monotonically decreasing in μ. Hence, there exists an integer γ such that $\psi_1(\gamma) \leq \psi_2(\gamma)$ and $\psi_1(\gamma+1) \geq \psi_2(\gamma+1)$. We consider two cases:
   (a) $\gamma \leq 0$ or $\gamma \geq n$. Then for all $0 \leq \mu \leq n$, $\phi_{\delta_1,\delta_2}(\mu) = \psi_2(\mu)$ or $\phi_{\delta_1,\delta_2}(\mu) = \psi_1(\mu)$. For both cases, it is trivial to show that ϕ_{δ_1,δ_2} is a legal function.
   (b) $0 < \gamma < n$. Hence,

$$\phi_{\delta_1,\delta_2}(\mu) = \begin{cases} \psi_1(\mu) & \text{if } 0 \leq \mu \leq \gamma \\ \psi_2(\mu) & \text{if } \gamma < \mu \leq n \end{cases}$$

   Therefore, it suffices to prove the privacy requirement is satisfied when $\mu = \gamma$ and $\mu = \gamma + 1$. Because

$$\frac{\phi_{\delta_1,\delta_2}(\gamma)}{\phi_{\delta_1,\delta_2}(\gamma+1)} = \frac{\psi_1(\gamma)}{\psi_2(\gamma+1)} \leq \frac{\psi_2(\gamma)}{\psi_2(\gamma+1)} \leq \alpha$$

$$\frac{\phi_{\delta_1,\delta_2}(\gamma)}{\phi_{\delta_1,\delta_2}(\gamma+1)} = \frac{\psi_1(\gamma)}{\psi_2(\gamma+1)} \geq \frac{\psi_1(\gamma)}{\psi_1(\gamma+1)} \geq \frac{1}{\alpha}$$

$$\frac{1-\phi_{\delta_1,\delta_2}(\gamma)}{1-\phi_{\delta_1,\delta_2}(\gamma+1)} = \frac{1-\psi_1(\gamma)}{1-\psi_2(\gamma+1)} \leq \frac{1-\psi_1(\gamma)}{1-\psi_1(\gamma+1)} \leq \alpha$$

$$\frac{1-\phi_{\delta_1,\delta_2}(\gamma)}{1-\phi_{\delta_1,\delta_2}(\gamma+1)} = \frac{1-\psi_1(\gamma)}{1-\psi_2(\gamma+1)} \geq \frac{1-\psi_2(\gamma)}{1-\psi_2(\gamma+1)} \geq \frac{1}{\alpha}$$

   Note that all denominators are guaranteed to be greater than 0. Thus, the privacy requirement is satisfied when $\mu = \gamma$ and $\mu = \gamma + 1$.

Therefore, ϕ_{δ_1,δ_2} satisfies differential privacy. Since the range of ϕ_{δ_1,δ_2} is clearly $[0, 1]$, ϕ_{δ_1,δ_2} is a legal function. □

We will prove that for any legal function ϕ, by carefully calibrating δ_1 and δ_2, there is a function ϕ_{δ_1,δ_2} that is less likely to commit both types of errors than ϕ.

THEOREM 14. *For any legal function ϕ, $\exists \delta_1, \delta_2 \in [0,1]$, such that ϕ_{δ_1,δ_2} is no more likely to commit both types of errors than ϕ.*

PROOF. For the design of an optimal legal function, without loss of generality, we shall assume that ϕ satisfies Theorem 13. Therefore, there is an integer $\gamma, \theta_1 \leq \gamma \leq \theta_2$ such that ϕ is monotonically non-decreasing over $\{0, \ldots, \gamma\}$, and monotonically non-increasing over $\{\gamma, \ldots, n\}$. Set $\delta_1 = \phi(\theta_1)$, $\delta_2 = \phi(\theta_2)$.

$$\phi_{\delta_1,\delta_2}(\mu) = \begin{cases} \psi_1(\mu) & \text{if } 0 \leq \mu \leq \gamma' \\ \psi_2(\mu) & \text{if } \gamma' + 1 \leq \mu \leq n \end{cases}$$

where γ' is the integer satisfying:

$$\psi_1(\gamma') \leq \psi_2(\gamma'),\ \psi_1(\gamma' + 1) \geq \psi_2(\gamma' + 1)$$

We claim that $\theta_1 \leq \gamma' \leq \theta_2$. We prove that claim by contradiction. Assume that $\gamma' > \theta_2$. Therefore, $\phi(\theta_2) = \psi_2(\theta_2) > \psi_1(\theta_2)$. However, since $\phi(\theta_1) = \psi_1(\theta_1)$, by Lemma 4, for any integer μ, $\mu \geq \theta_1$, $\phi(\mu) \leq \psi_1(\mu)$. Hence, $\phi(\theta_2) \leq \psi_1(\theta_2)$, a contradiction. Therefore, $\gamma' \leq \theta_2$. Similarly, we can prove that $\gamma' \geq \theta_1$, and then our claim follows.

First, we prove ϕ_{δ_1,δ_2} is no more likely to commit a false positive error than ϕ. For any integer μ,

1. $0 \leq \mu < \theta_1$, because $\psi_1(\theta_1) = \phi(\theta_1)$, by Corollary 5, $\phi_{\delta_1,\delta_2}(\mu) = \psi_1(\mu) \leq \phi(\mu)$.
2. $\theta_2 < \mu \leq n$. The proof is similar to that when $0 \leq \mu < \theta_1$.

Next, we will prove that ϕ_{δ_1,δ_2} is no more likely to commit a false negative error than ϕ. We consider two cases:

1. $\gamma' \leq \gamma$. For any integer μ, we consider three cases:
   (a) $\theta_1 \leq \mu \leq \gamma'$. Because $\phi_{\delta_1,\delta_2}(\mu) = \psi_1(\mu)$, it suffices to prove $\psi_1(\mu) \geq \phi(\mu)$. Since $\psi_1(\theta_1) = \phi(\theta_1)$, by Lemma 4, $\psi_1(\mu) \geq \phi(\mu)$.
   (b) $\gamma \leq \mu \leq \theta_2$. The proof is similar to the case where $\theta_1 \leq \mu \leq \gamma'$.
   (c) $\gamma' < \mu < \gamma$. Since $\phi_{\delta_1,\delta_2}(\mu) = \psi_2(\mu)$ and ψ_2 is monotonically non-increasing, $\phi_{\delta_1,\delta_2}(\mu) = \psi_2(\mu) \geq \psi_2(\gamma)$. Because ϕ is monotonically non-decreasing when $0 \leq \mu \leq \gamma$, $\phi(\mu) \leq \phi(\gamma)$. Therefore, $\phi_{\delta_1,\delta_2}(\mu) \geq \psi_2(\gamma) \geq \phi(\gamma) \geq \phi(\mu)$.
2. $\gamma' > \gamma$. The proof is similar to that when $\gamma' \leq \gamma$. We omit the details here.

The theorem follows. □

E. THE MECHANISM $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$

Consider a special case where the size of the database $n = 3$, and two thresholds $\theta_1 = 1$, $\theta_2 = 2$. Therefore, we can represent the optimal mechanism for a count range query by a consumer as a vector $(z_0, z_1, z_2, z_3)^t$ where z_i $(0 \leq i \leq 3)$ is the probability of outputting *yes* when the count is i.

LEMMA 11. *There exists an information consumer, whose only optimal differentially private mechanism is:*

$$\hat{\mathbf{x}} = (\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{\alpha}{\alpha+1}, \frac{1}{\alpha+1})^t$$

PROOF. Suppose a consumer has a uniform error penalty function and a uniform prior distribution. Then minimizing her weighted error can be written as the following optimization problem:

$$\min_{z_i \in [0,1], 0 \leq i \leq 3} \{z_0 + (1 - z_1) + (1 - z_2) + z_3\}$$

subject to the privacy constraints: for any integer $i, 0 \leq i \leq 2$, $1/\alpha \leq z_i/z_{i+1} \leq \alpha$, $1/\alpha \leq (1 - z_i)/(1 - z_{i+1}) \leq \alpha$. By symmetry, it suffices to just consider the following optimization problem:

$$\min_{z_0, z_1 \in [0,1]} \{z_0 + (1 - z_1)\}$$

subject to the privacy constraints. Let z_0^* and z_1^* be the solution that minimizes $z_0 + (1 - z_1)$. We claim that $z_0^* \leq z_1^*$. Or else, let $z_0' = z_1' = z_1^*$, and

$$z_0' + (1 - z_1') = z_1^* + (1 - z_1^*) < z_0^* + (1 - z_1^*)$$

which is in contradiction to our assumption that z_0^* and z_1^* minimizes $z_0 + (1 - z_1)$. Hence, we can rewrite the privacy constraint as: $z_1 \leq \min(\alpha z_0, 1 - (1 - z_0)/\alpha)$. We consider two cases:

1. $z_0 \leq 1/(\alpha + 1)$,

$$\begin{aligned} z_0 + 1 - z_1 &\geq z_0 + 1 - \min(\alpha z_0, 1 - \frac{1 - z_0}{\alpha}) \\ &= z_0 + 1 - \alpha z_0 \\ &\geq \frac{1}{\alpha + 1} + 1 - \frac{\alpha}{\alpha + 1} \\ &= \frac{2}{\alpha + 2} \end{aligned}$$

   and when $z_0 = 1/(\alpha + 1)$ and $z_1 = \alpha/(\alpha + 1)$, $z_0 + 1 - z_1 = 2/(\alpha + 2)$.

2. $z_0 > 1/(\alpha + 1)$,

$$\begin{aligned} z_0 + 1 - z_1 &\geq z_0 + 1 - \min(\alpha z_0, 1 - \frac{1 - z_0}{\alpha}) \\ &= z_0 + \frac{1 - z_0}{\alpha} \\ &> \frac{1}{\alpha + 1} + \frac{1 - \frac{1}{\alpha+1}}{\alpha} \\ &= \frac{2}{\alpha + 2} \end{aligned}$$

Hence, $z_0^* = 1/(\alpha + 1)$ and $z_1^* = \alpha/(\alpha + 1)$. By symmetry, $z_2^* = \alpha/(\alpha + 1)$, $z_3^* = 1/(\alpha + 1)$. Therefore, $\hat{\mathbf{x}}$ is the only optimal differentially private mechanism for that consumer. □

LEMMA 12. *There exists an information consumer whose only optimal differentially private mechanism is:*

$$\hat{\mathbf{y}} = (\frac{1}{(\alpha + 1)\alpha}, \frac{1}{\alpha + 1}, \frac{\alpha}{\alpha + 1}, \frac{1}{\alpha + 1})^t$$

PROOF. Suppose a consumer has a uniform error penalty function and a prior distribution of the following form $(\alpha^2/(\alpha + 1)^2, 1/(\alpha + 1)^2, \alpha/(\alpha + 1)^2, \alpha/(\alpha + 1)^2)^t$. Then minimizing her weighted error can be written as the following optimization problem:

$$\min_{z_i \in [0,1], 0 \leq i \leq 3} \{\alpha z_0 + \frac{1}{\alpha}(1 - z_1) + (1 - z_2) + z_3\}$$

subject to the privacy constraints: for any integer i, $0 \leq i \leq 2$, $1/\alpha \leq z_i/z_{i+1} \leq \alpha$, $1/\alpha \leq (1 - z_i)/(1 - z_{i+1}) \leq \alpha$.

Let z_i^* $(0 \leq i \leq 3)$ be the solution that minimizes her weighted error. Similar to the proof in Lemma 11, we can prove that $z_0^* \leq z_1^*$ and $z_2^* \geq z_3^*$. Hence, we can rewrite the privacy constraints as: $z_0 \geq \max\{z_1/\alpha, \alpha z_1 + 1 - \alpha\}$, and $z_3 \geq \max\{z_2/\alpha, \alpha z_2 + 1 - \alpha\}$. We consider two cases:

1. $z_1 < z_2$.
   (a) $z_2 \leq \alpha/(\alpha + 1)$. Therefore,

$$\begin{aligned} \alpha z_0 + \frac{1}{\alpha}(1 - z_1) + (1 - z_2) + z_3 &\geq \alpha \max\{\frac{z_1}{\alpha}, \alpha z_1 + 1 - \alpha\} + \frac{1}{\alpha}(1 - z_1) + (1 - z_2) + \max\{\frac{z_2}{\alpha}, \alpha z_2 + 1 - \alpha\} \\ &= z_1 + \frac{1}{\alpha}(1 - z_1) + (1 - z_2) + \frac{z_2}{\alpha} \\ &= 1 + \frac{1}{\alpha} + (1 - \frac{1}{\alpha})(z_1 - z_2) \\ &\geq 1 + \frac{1}{\alpha} + (1 - \frac{1}{\alpha})(\frac{z_2}{\alpha} - z_2) \\ &\geq 1 + \frac{1}{\alpha} - (1 - \frac{1}{\alpha})^2 \frac{\alpha}{\alpha + 1} \\ &= \frac{4}{\alpha + 1} \end{aligned}$$

   and when $z_0 = 1/(\alpha(\alpha + 1))$, $z_1 = z_3 = 1/(\alpha + 1)$ and $z_2 = \alpha/(\alpha + 1)$, the weighted error is $4/(\alpha + 1)$.

(b) $z_2 > \alpha/(\alpha+1)$. Because $(1-z_1)/(1-z_2) \le \alpha$, $z_1 \ge 1-\alpha+\alpha z_2$. Hence,

$$\begin{aligned}
\alpha z_0 + \frac{1}{\alpha}(1-z_1) + (1-z_2) + z_3 &\ge \alpha \max\{\frac{z_1}{\alpha}, \alpha z_1 + 1 - \alpha\} + \frac{1}{\alpha}(1-z_1) + (1-z_2) + \max\{\frac{z_2}{\alpha}, \alpha z_2 + 1 - \alpha\} \\
&\ge z_1 + \frac{1}{\alpha}(1-z_1) + (1-z_2) + \alpha z_2 + 1 - \alpha \\
&= 2 - \alpha + \frac{1}{\alpha} + (1-\frac{1}{\alpha})z_1 + (\alpha-1)z_2 \\
&\ge 2 - \alpha + \frac{1}{\alpha} + (1-\frac{1}{\alpha})(1-\alpha(1-z_2)) + (\alpha-1)z_2 \\
&> 2 - \alpha + \frac{1}{\alpha} + (1-\frac{1}{\alpha})(1-\alpha(1-\frac{\alpha}{\alpha+1}) + (\alpha-1)\frac{\alpha}{\alpha+1} \\
&= \frac{4}{\alpha+1}
\end{aligned}$$

2. $z_1 > z_2$.

$$\begin{aligned}
\alpha z_0 + \frac{1}{\alpha}(1-z_1) + (1-z_2) + z_3 &\ge \alpha \max\{\frac{z_1}{\alpha}, \alpha z_1 + 1 - \alpha\} + \frac{1}{\alpha}(1-z_1) + (1-z_2) + \max\{\frac{z_2}{\alpha}, \alpha z_2 + 1 - \alpha\} \\
&\ge z_1 + \frac{1}{\alpha}(1-z_1) + 1 - z_2 + \frac{z_2}{\alpha} \\
&= 1 + \frac{1}{\alpha} + (1-\frac{1}{\alpha})(z_1 - z_2) \\
&\ge 1 + \frac{1}{\alpha} \\
&> \frac{4}{\alpha+1}
\end{aligned}$$

Hence, $z_0^* = 1/(\alpha(\alpha+1))$, $z_1^* = 1/(\alpha+1)$, $z_2^* = \alpha/(\alpha+1)$, $z_3^* = 1/(\alpha+1)$, and thus, $\hat{\mathbf{y}}$ is the only optimal differentially private mechanism for that consumer. □

We will prove that $\hat{\mathbf{x}}$ can not be derived by the range-restricted geometric mechanism. In particular, the range-restricted geometric mechanism when $n = 3$ is of the following form:

$$M = \frac{\alpha-1}{\alpha+1}\begin{pmatrix} \frac{\alpha}{\alpha-1} & \alpha^{-1} & \alpha^{-2} & \frac{\alpha}{\alpha-1}\alpha^{-3} \\ \frac{\alpha}{\alpha-1}\alpha^{-1} & 1 & \alpha^{-1} & \frac{\alpha}{\alpha-1}\alpha^{-2} \\ \frac{\alpha}{\alpha-1}\alpha^{-2} & \alpha^{-1} & 1 & \frac{\alpha}{\alpha-1}\alpha^{-1} \\ \frac{\alpha}{\alpha-1}\alpha^{-3} & \alpha^{-2} & \alpha^{-1} & \frac{\alpha}{\alpha-1} \end{pmatrix}$$

THEOREM 15. *$\hat{\mathbf{x}}$ can not be derived by M.*

PROOF. Let $\mathbf{t} = (t_0, t_1, t_2, t_3)^t = M^{-1} \circ \hat{\mathbf{x}}$, and M_2 be the matrix obtained by replacing M's 2^{nd} column with $\hat{\mathbf{x}}$. By Cramer's rule, $t_2 = \det(M_2)/\det(M)$. By the proof of Lemma 6,

$$\begin{aligned}
\det(M_2) &= \frac{\alpha-1}{\alpha+1}(\frac{\alpha}{\alpha+1})^2 \begin{vmatrix} 1 & \alpha^{-1} & \frac{1}{\alpha+1} & \alpha^{-3} \\ \alpha^{-1} & 1 & \frac{\alpha}{\alpha+1} & \alpha^{-2} \\ \alpha^{-2} & \alpha^{-1} & \frac{\alpha}{\alpha+1} & \alpha^{-1} \\ \alpha^{-3} & \alpha^{-2} & \frac{1}{\alpha+1} & 1 \end{vmatrix} \\
&= \frac{\alpha-1}{\alpha+1}(\frac{\alpha}{\alpha+1})^2 \frac{(\alpha-1)^2}{\alpha^2}(1-\alpha^{-2})
\end{aligned}$$

By Lemma 5, it follows that:

$$\frac{\det(M_2)}{\det(M)} = \frac{\alpha^2}{\alpha^2-1} > 1$$

Thus, t is not a transformation. Therefore, $\hat{\mathbf{x}}$ can not be derived from the range-restricted geometric mechanism. □

For the general case where the size of the database is n, and two thresholds are θ_1 and θ_2, we can characterize a consumer's optimal mechanism by a vector of $n+1$ elements $(z_0, \ldots, z_n)^t$ where z_i is the probability of outputting *yes* when the count is i.

If $\theta_1 + \theta_2$ is odd, let $k = (\theta_1 + \theta_2 - 1)/2$. Or else, let $k = (\theta_1 + \theta_2)/2$.

LEMMA 13. *There exists an information consumer whose only optimal differentially private mechanism is:*

$$\mathbf{x} = (x_0, \ldots, x_n)^t$$

where for all i, $0 \le i \le k$, $x_i = 1/(\alpha^{k-1-i}(\alpha+1))$, and for all $j, k+1 \le j \le n$, $x_j = 1/(\alpha^{j-k-2}(\alpha+1))$.

PROOF. Suppose an information consumer has a uniform error penalty function, and a prior distribution ρ of the following form: $\rho(0)/\rho(k) = \alpha^{k-1}$, $\rho(k) = \rho(k+1)$, $\rho(n)/\rho(k+1) = \alpha^{n-k-2}$, and 0 otherwise. Because $\theta_1 \le k < k+1 \le \theta_2$, minimizing the weighted error for that consumer can be expressed as the following optimization problem:

$$\min_{z_0, z_k, z_{k+1}, z_n \in [0,1]} \{\alpha^{k-1} z_0 + 1 - z_k + 1 - z_{k+1} + \alpha^{n-k-2} z_n\}$$

subject to the privacy constraints: for any integer $i, 0 \le i < n$,

$$\frac{1}{\alpha} \le \frac{z_i}{z_{i+1}} \le \alpha,\ \frac{1}{\alpha} \le \frac{1 - z_i}{1 - z_{i+1}} \le \alpha \tag{14}$$

We start by solving the following optimization problem:

$$\min_{z_0, z_k \in [0,1]} \{\alpha^{k-1} z_0 + 1 - z_k\}$$

subject to the privacy constraints in (14). By Lemma 11,

$$\alpha^{k-1} z_0 + 1 - z_k \ge z_{k-1} + 1 - z_k \ge \frac{2}{\alpha+1}$$

and both "=" hold if and only if $z_0 = 1/(\alpha^{k-1}(\alpha+1))$ and $z_k = \alpha/(\alpha+1)$. Similarly, we can prove that

$$1 - z_{k+1} + \alpha^{n-k-2} z_n \ge \frac{2}{\alpha+1}$$

and "=" holds if and only if $z_{k+1} = \alpha/(\alpha+1)$ and $z_n = 1/(\alpha^{n-k-2}(\alpha+1))$. Hence, to minimize the weighted error, $x_0 = 1/(\alpha^{k-1}(\alpha+1))$, $x_k = x_{k+1} = \alpha/(\alpha+1)$, and $x_n = 1/(\alpha^{n-k-2}(\alpha+1))$.

Next, we claim that for all i, $0 \le i \le k$, $x_i = 1/(\alpha^{k-1-i}(\alpha+1))$. Or else, there is an integer $i^*, 0 \le i^* \le k$ such that:

1. $x_{i^*} < 1/(\alpha^{k-1-i^*}(\alpha+1))$. Hence,

   $$\frac{\alpha}{\alpha+1} = x_k \le \alpha^{k-i^*} x_{i^*} < \frac{\alpha}{\alpha+1}$$

   a contradiction.
2. $x_{i^*} > 1/(\alpha^{k-1-i^*}(\alpha+1))$. Hence,

   $$\frac{1}{\alpha^{k-1}(\alpha+1)} = x_0 \ge \alpha^{-i^*} x_{i^*} > \frac{1}{\alpha^{k-1}(\alpha+1)}$$

   a contradiction

We have thus obtained a contradiction for both cases. The lemma follows. □

LEMMA 14. *There exists an information consumer whose only optimal differentially private mechanism is:*

$$\mathbf{y} = (y_0, \ldots, y_n)^t$$

where for all i, $0 \le i \le k$, $y_i = 1/(\alpha^{k-i}(\alpha+1))$, and for all $j, k+1 \le j \le n$, $y_j = 1/(\alpha^{j-k-2}(\alpha+1))$.

PROOF. Suppose an information consumer has a uniform error penalty function, and a prior distribution ρ of the following form: $\rho(0)/\rho(k) = \alpha^{k+1}$, $\alpha\rho(k) = \rho(k+1)$, $\rho(n)/\rho(k+1) = \alpha^{n-k-2}$, and 0 otherwise. Because $\theta_1 \leq k < k+1 \leq \theta_2$, minimizing the weighted error for that consumer can be expressed as the following optimization problem:

$$\min_{z_0, z_k, z_{k+1}, z_n \in [0,1]} \{\alpha^k z_0 + \frac{1}{\alpha}(1 - z_k) + (1 - z_{k+1}) + \alpha^{n-k-2} z_n\}$$

subject to the privacy constraints in (14). By the proof of Lemma 12,

$$\begin{aligned} \alpha^k z_0 + \frac{1}{\alpha}(1 - z_k) + (1 - z_{k+1}) + \alpha^{n-k-2} z_n &\geq \alpha z_{k-1} + \frac{1}{\alpha}(1 - z_k) + (1 - z_{k+1}) + z_{k+2} \\ &= \frac{4}{\alpha + 1} \end{aligned}$$

and both "=" hold if and only if $z_0 = 1/(\alpha^k(\alpha+1))$, $z_k = 1/(\alpha+1)$, $z_{k+1} = \alpha/(\alpha+1)$ and $z_n = 1/(\alpha^{n-k-2}(\alpha+1))$. Similar to the proof in Lemma 13, in order to minimize the weighted error of that consumer, for all i, $0 \leq i \leq k$, $y_i = 1/(\alpha^{k-i}(\alpha + 1))$, and for all $j, k + 1 \leq j \leq n$, $y_j = 1/(\alpha^{j-k-2}(\alpha + 1))$. $\square$

F. AN APPROXIMATE UUM MECHANISM FOR RANGE QUERIES

Given a count range query $\langle p, \theta_1, \theta_2\rangle$, we can characterize an optimal mechanism by a consumer for that query by a vector $\mathbf{z} = (z_0, \dots, z_n)^t$ satisfying Theorem 1. Let $\mathbf{t} = (t_0, \dots, t_n)^t = M^{-1}\mathbf{z}$ where M is the matrix in (10) defined by the range-restricted geometric mechanism (6). We construct a vector $\mathbf{t}' = (t'_0, \dots, t'_n)^t$ as follows: for all $0 \leq i \leq n$

$$t'_i = \begin{cases} t_i & \text{if } 0 \leq t_i \leq 1 \\ 1 & \text{otherwise.} \end{cases}$$

We will show later that in fact for all i, $t_i \geq 0$, and so $t_i \geq t'_i$.

Let $\mathbf{z}' = (z'_0, \dots, z'_n)^t = M \circ \mathbf{t}'$. We shall prove that the weighted error incured by the differentially private mechanism $\mathbf{z}'$ for that consumer is at most twice that by the optimal mechanism $\mathbf{z}$.

THEOREM 4. *The range-restricted geometric mechanism* (6) *is* 2*-approximate universally utility maximizing for count range queries.*

PROOF. Given a count range query $\langle p, \theta_1, \theta_2\rangle$, let the optimal mechanism for a consumer be $\mathbf{z} = (z_0, \dots, z_n)^t$ satisfying Theorem 1. We shall assume that $\theta_1 > 0$ and $\theta_2 < n$, or else, it is not difficult to see that when $\theta_2 = n$, $\mathbf{z}$ satisfies (2) and when $\theta_1 = 0$, $\mathbf{z}$ satisfies (3). By Theorem 7 and Theorem 6, the range-restricted geometric mechanism can derive $\mathbf{z}$ for both cases. Let $\mathbf{t} = (t_0, \dots, t_n)^t = M^{-1} \circ \mathbf{z}$ where M is the range-restricted geometric mechanism. By Theorem 1,

$$z_i = \begin{cases} \psi_1(i) & \text{if } 0 \leq i \leq \gamma \\ \psi_2(i) & \text{otherwise.} \end{cases}$$

where γ is an integer between θ_1 and θ_2. By Theorem 7, for all i, $i \leq \gamma - 1$ or $i \geq \gamma + 2$, $0 \leq t_i \leq 1$. Therefore, only t_γ and $t_{\gamma+1}$ could be greater than 1 or less than 0 (we will prove that $t_\gamma, t_{\gamma+1} \geq 0$). We construct a transformation $\mathbf{t}' = (t'_0, \dots, t'_n)^t$ as follows:

$$t'_i = \begin{cases} t_i & \text{if } 0 \leq t_i \leq 1 \\ 1 & \text{otherwise.} \end{cases}$$

Let $\mathbf{z}' = (z'_0, \dots, z'_n)^t = M \circ \mathbf{t}'$. We shall prove that the weighted error incurred by the differentially private mechanism $\mathbf{z}'$ for that consumer is at most twice that by the optimal mechanism $\mathbf{z}$. We start by proving that for $i = \gamma, \gamma+1$, $(1-z'_i)/(1-z_i) \leq 2$. With the knowledge that $t_\gamma, t_{\gamma+1} \geq 0$, we have $\delta_1 = t_\gamma - t'_\gamma$ and $\delta_2 = t_{\gamma+1} - t'_{\gamma+1}$. In particular, $\delta_1, \delta_2 \geq 0$, and

$$\begin{aligned} \frac{1 - z'_\gamma}{1 - z_\gamma} &= 1 + (\frac{\alpha - 1}{\alpha + 1})\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1 - z_\gamma} \\ \frac{1 - z'_{\gamma+1}}{1 - z_{\gamma+1}} &= 1 + (\frac{\alpha - 1}{\alpha + 1})\frac{\frac{1}{\alpha}\delta_1 + \delta_2}{1 - z_{\gamma+1}} \end{aligned}$$

It suffices to prove

$$\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1 - z_\gamma} \leq \frac{\alpha + 1}{\alpha - 1}, \quad \text{and} \quad \frac{\frac{1}{\alpha}\delta_1 + \delta_2}{1 - z_{\gamma+1}} \leq \frac{\alpha + 1}{\alpha - 1}$$

Let M_j be the matrix obtained by replacing the j^{th} column of M with $\mathbf{z}$. There are two cases:

1. $1 \leq \gamma < n-1$, by the proof of Theorem 7 in Appendix C,

$$t_\gamma = \frac{\det(M_\gamma)}{\det(M)} = \frac{\alpha^4}{(\alpha-1)^3(\alpha+1)} \begin{vmatrix} 1 & z_{\gamma-1} & \alpha^{-2} \\ \alpha^{-1} & z_\gamma & \alpha^{-1} \\ \alpha^{-2} & z_{\gamma+1} & 1 \end{vmatrix}$$

$$t_{\gamma+1} = \frac{\det(M_{\gamma+1})}{\det(M)} = \frac{\alpha^4}{(\alpha-1)^3(\alpha+1)} \begin{vmatrix} 1 & z_\gamma & \alpha^{-2} \\ \alpha^{-1} & z_{\gamma+1} & \alpha^{-1} \\ \alpha^{-2} & z_{\gamma+2} & 1 \end{vmatrix}$$

By differential privacy, $z_{\gamma+1}/\alpha \leq z_\gamma \leq \alpha z_{\gamma+1}$, $(1-z_{\gamma+1})/\alpha \leq 1-z_\gamma \leq \alpha(1-z_{\gamma+1})$. We consider four cases according to the magnitude of z_γ and $z_{\gamma+1}$:

(a) $z_\gamma, z_{\gamma+1} \leq \alpha/(\alpha+1)$. Thus, $z_{\gamma-1} = z_\gamma/\alpha$, $z_{\gamma+2} = z_{\gamma+1}/\alpha$. Therefore,

$$t_\gamma = \frac{\alpha(\alpha z_\gamma - z_{\gamma+1})}{(\alpha-1)^2}$$
$$t_{\gamma+1} = \frac{\alpha(\alpha z_{\gamma+1} - z_\gamma)}{(\alpha-1)^2}$$

In this case, clearly $t_\gamma, t_{\gamma+1} \geq 0$ by differential privacy. If $t_\gamma \leq 1$, then $\delta_1 = 0$. If $t_\gamma > 1$, then

$$\begin{aligned} \delta_1 &= t_\gamma - t'_\gamma \\ &= \frac{\alpha(\alpha z_\gamma - z_{\gamma+1})}{(\alpha-1)^2} - 1 \\ &\leq \frac{(\alpha^2-1)z_\gamma}{(\alpha-1)^2} - 1 \\ &\leq \frac{1}{\alpha-1} \end{aligned}$$

where we uses the differential privacy condition $z_\gamma \leq \alpha z_{\gamma+1}$, and the condition in this case $z_\gamma \leq \alpha/(\alpha+1)$. Hence $\delta_1 \leq 1/(\alpha-1)$. Similarly, $\delta_2 \leq 1/(\alpha-1)$. Hence, when $t_\gamma \leq 1, t_{\gamma+1} > 1$ or $t_\gamma > 1, t_{\gamma+1} \leq 1$, one of δ_1, δ_2 is zero, and $\delta_1 + \delta_2/\alpha \leq 1/(\alpha-1)$ in all cases.
When $t_\gamma, t_{\gamma+1} > 1$, writing $\delta_1 = t_\gamma - 1$ and $\delta_2 = t_{\gamma+1} - 1$, we have

$$\begin{aligned} \delta_1 + \frac{1}{\alpha}\delta_2 &= \frac{\alpha+1}{\alpha-1} z_\gamma - 1 - \frac{1}{\alpha} \\ &\leq (\frac{\alpha+1}{\alpha-1})(\frac{\alpha}{\alpha+1}) - 1 - \frac{1}{\alpha} \\ &= \frac{1}{\alpha(\alpha-1)} \end{aligned}$$

It follows that:

$$\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1 - z_\gamma} \leq \frac{\frac{1}{\alpha-1}}{1 - \frac{\alpha}{\alpha+1}} = \frac{\alpha+1}{\alpha-1}$$

Similarly, $(\delta_1/\alpha + \delta_2)/(1 - z_{\gamma+1}) \leq (\alpha+1)/(\alpha-1)$.

(b) $\alpha/(\alpha+1) < z_\gamma, z_{\gamma+1} \leq 1$. It is not difficult to show that $z_{\gamma-1} = \alpha z_\gamma + 1 - \alpha$, $z_{\gamma+2} = \alpha z_{\gamma+1} + 1 - \alpha$. Hence,

$$t_\gamma = \frac{z_\gamma - \alpha z_{\gamma+1} + \alpha^2 - \alpha}{(\alpha-1)^2}$$
$$t_{\gamma+1} = \frac{z_{\gamma+1} - \alpha z_\gamma + \alpha^2 - \alpha}{(\alpha-1)^2}$$

By differential privacy, $z_{\gamma+1} \leq 1 - (1 - z_\gamma)/\alpha$,

$$\begin{aligned} t_\gamma &= \frac{z_\gamma - \alpha z_{\gamma+1} + \alpha^2 - \alpha}{(\alpha-1)^2} \\ &\geq \frac{z_\gamma - \alpha(1 - (1-z_\gamma)/\alpha) + \alpha^2 - \alpha}{(\alpha-1)^2} \\ &= 1 \end{aligned} \tag{15}$$

Similarly, $t_{\gamma+1} \geq 1$. Therefore,

$$\begin{aligned}
\delta_1 + \frac{1}{\alpha}\delta_2 &= t_\gamma + \frac{1}{\alpha}t_{\gamma+1} - 1 - \frac{1}{\alpha} \\
&= (\frac{\alpha+1}{\alpha-1})\frac{1-z_{\gamma+1}}{\alpha} \\
&\leq (\frac{\alpha+1}{\alpha-1})(1-z_\gamma)
\end{aligned}$$

It follows that:

$$\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1-z_\gamma} \leq \frac{\alpha+1}{\alpha-1}$$

Similarly, $(\delta_1/\alpha + \delta_2)/(1 - z_{\gamma+1}) \leq (\alpha+1)/(\alpha-1)$.

(c) $z_\gamma \leq \alpha/(\alpha+1)$, $z_{\gamma+1} > \alpha/(\alpha+1)$. It is not difficult to show that $z_{\gamma-1} = z_\gamma/\alpha$, $z_{\gamma+2} = \alpha z_{\gamma+1} - \alpha + 1$, $z_\gamma > 1/(\alpha+1)$, $z_{\gamma+1} \leq 1 - 1/(\alpha(\alpha+1))$. Thus,

$$\begin{aligned}
t_\gamma &= \frac{\alpha(\alpha z_\gamma - z_{\gamma+1})}{(\alpha-1)^2} \\
t_{\gamma+1} &= \frac{z_{\gamma+1} - \alpha z_\gamma + \alpha^2 - \alpha}{(\alpha-1)^2}
\end{aligned}$$

By the proof in (15), $t_{\gamma+1} \geq 1$. By differential privacy, $t_\gamma \geq 0$. Also by differential privacy, $z_\gamma \geq \alpha z_{\gamma+1} - \alpha + 1$, and thus,

$$\begin{aligned}
\delta_2 &= t_{\gamma+1} - 1 \\
&= \frac{z_{\gamma+1} - \alpha z_\gamma + \alpha^2 - \alpha}{(\alpha-1)^2} - 1 \\
&\leq \frac{z_{\gamma+1} - \alpha(\alpha z_{\gamma+1} - \alpha + 1) + \alpha^2 - \alpha}{(\alpha-1)^2} - 1 \\
&= \frac{\alpha+1}{\alpha-1}(1 - z_{\gamma+1})
\end{aligned}$$

Hence, if $t_\gamma \leq 1$, then $\delta_1 = 0$,

$$\begin{aligned}
\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1-z_\gamma} &\leq \frac{\alpha+1}{\alpha(\alpha-1)}\frac{1-z_{\gamma+1}}{1-z_\gamma} \\
&\leq \frac{\alpha+1}{\alpha(\alpha-1)}\alpha \\
&= \frac{\alpha+1}{\alpha-1}
\end{aligned}$$

$$\frac{\frac{1}{\alpha}\delta_1 + \delta_2}{1-z_{\gamma+1}} \leq (\frac{\alpha+1}{\alpha-1})\frac{1-z_{\gamma+1}}{1-z_{\gamma+1}} = \frac{\alpha+1}{\alpha-1}$$

If $t_\gamma > 1$, we substitute $\delta_1 = t_\gamma - 1$ and $\delta_2 = t_{\gamma+1} - 1$ and simplify

$$\begin{aligned}
\delta_1 + \frac{1}{\alpha}\delta_2 &= \frac{(\alpha+1)(z_\gamma - \frac{z_{\gamma+1}}{\alpha}) + 1}{\alpha-1} - \frac{\alpha+1}{\alpha} \\
&\leq \frac{\frac{(\alpha-1)(\alpha+1)}{\alpha}z_\gamma + 1}{\alpha-1} - \frac{\alpha+1}{\alpha} \\
&\leq \frac{1}{\alpha(\alpha-1)}
\end{aligned}$$

where the first inequality uses $z_{\gamma+1} \geq z_\gamma$, and the second inequality uses $z_\gamma \leq \alpha/(\alpha+1)$. The next equality is a simple substitution:

$$\frac{\delta_1}{\alpha} + \delta_2 = \frac{1}{\alpha}t_\gamma + t_{\gamma+1} - \frac{\alpha+1}{\alpha} = \frac{1}{\alpha(\alpha-1)}$$

It follows that:

$$\frac{\delta_1 + \frac{\delta_2}{\alpha}}{1-z_\gamma} \leq \frac{\frac{1}{\alpha(\alpha-1)}}{1-\frac{\alpha}{\alpha+1}} \leq \frac{\alpha+1}{\alpha(\alpha-1)} < \frac{\alpha+1}{\alpha-1}$$

$$\frac{\frac{\delta_1}{\alpha} + \delta_2}{1-z_{\gamma+1}} \leq \frac{\frac{1}{\alpha(\alpha-1)}}{1-(1-\frac{1}{\alpha(\alpha+1)})} = \frac{\alpha+1}{\alpha-1}$$

(d) $z_\gamma > \alpha/(\alpha+1)$, $z_{\gamma+1} \le \alpha/(\alpha+1)$. The proof is similar to that of case 1c.

2. $\gamma = n-1$. Then

$$t_{n-1} = \frac{\det(M_\gamma)}{\det(M)} = \frac{\alpha^4}{(\alpha-1)^3(\alpha+1)} \begin{vmatrix} 1 & z_{n-2} & \alpha^{-2} \\ \alpha^{-1} & z_{n-1} & \alpha^{-1} \\ \alpha^{-2} & z_n & 1 \end{vmatrix}$$
$$t_n = \frac{\det(M_n)}{\det(M)} = \frac{\alpha}{\alpha-1} \begin{vmatrix} 1 & z_{n-1} \\ \alpha^{-1} & z_n \end{vmatrix}$$

We consider two cases:

(a) $z_{n-1} \le \alpha/(\alpha+1)$. It is not difficult to show that $z_{n-2} = z_n = z_{n-1}/\alpha$. Therefore, $t_n = 0$, $t_{n-1} = \frac{\alpha+1}{\alpha-1} z_{n-1}$. Thus,

$$t_{n-1} = \frac{\alpha+1}{\alpha-1} z_{n-1} \le \frac{\alpha}{\alpha-1}$$

where we uses the condition $z_{n-1} \le \alpha/(\alpha+1)$. Hence,

$$\frac{\delta_1 + \delta_2/\alpha}{1 - z_{n-1}} \le \frac{\frac{\alpha}{\alpha-1} - 1}{1 - \frac{\alpha}{\alpha+1}} = \frac{\alpha+1}{\alpha-1}$$
$$\frac{\delta_1/\alpha + \delta_2}{1 - z_n} \le \frac{\frac{1}{\alpha-1} - \frac{1}{\alpha}}{1 - \frac{1}{\alpha+1}} < \frac{\alpha+1}{\alpha-1}$$

where the first one uses $z_{n-1} \le \alpha/(\alpha+1)$, and the second one uses $z_n = z_{n-1}/\alpha \le 1/(\alpha+1)$.

(b) $\alpha/(\alpha+1) < z_{n-1} \le 1$. It is not difficult to show that $z_{n-2} = z_n = 1 + \alpha z_{n-1} - \alpha$. Hence, $t_n = (\alpha+1)z_{n-1} - \alpha \in [0,1]$, and

$$t_{n-1} = \frac{2\alpha - (\alpha+1)z_{n-1}}{\alpha - 1}$$

Thus, $\delta_2 = 0$. By the proof in (15), $t_{n-1} \ge 1$. We substitute t_{n-1} into $\delta_1 = t_{n-1} - 1$ and simplify

$$\delta_1 = t_{n-1} - 1 = (\frac{\alpha+1}{\alpha-1})(1 - z_{n-1})$$

Hence,

$$\frac{\delta_1 + \delta_2/\alpha}{1 - z_{n-1}} = (\frac{\alpha+1}{\alpha-1}) \frac{1 - z_{n-1}}{1 - z_{n-1}} = \frac{\alpha+1}{\alpha-1}$$
$$\frac{\delta_1/\alpha + \delta_2}{1 - z_n} = \frac{\delta_1/\alpha}{\alpha(1 - z_{n-1})} = \frac{\alpha+1}{\alpha^2(\alpha-1)} < \frac{\alpha+1}{\alpha-1}$$

We have noted that for all cases, $t_\gamma, t_{\gamma+1} \ge 0$, and thus, $\delta_1, \delta_2 \ge 0$. Therefore, for all i, $0 \le i \le \gamma$,

$$\begin{aligned}
\frac{1 - z_i'}{1 - z_i} &= 1 + \frac{z_i - z_i'}{1 - z_i} \\
&= 1 + (\frac{\alpha-1}{\alpha+1})(\frac{\alpha^{i-\gamma}\delta_1 + \alpha^{i-\gamma-1}\delta_2}{1 - z_i}) \\
&\le 1 + (\frac{\alpha+1}{\alpha-1})(\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1 - z_i}) \\
&\le 1 + (\frac{\alpha+1}{\alpha-1})(\frac{\delta_1 + \frac{1}{\alpha}\delta_2}{1 - z_\gamma}) \\
&= \frac{1 - z_\gamma'}{1 - z_\gamma} \\
&\le 2
\end{aligned}$$

Similarly, for all $\gamma + 1 \le j \le n$,

$$\frac{1 - z_j'}{1 - z_j} \le \frac{1 - z_{\gamma+1}'}{1 - z_{\gamma+1}} \le 2$$

On the other hand, since $\delta_1, \delta_2 \ge 0$, $t_\gamma' \le t_\gamma$ and $t_{\gamma+1}' \le t_{\gamma+1}$. It follows that for all $0 \le i \le n$, $z_i' \le z_i$, as all entries of M are positive. Therefore, for all $0 \le i \le n$,

$$\frac{1 - z_i'}{1 - z_i} \le 2, \quad \text{and} \quad \frac{z_i'}{z_i} \le 1 < 2$$

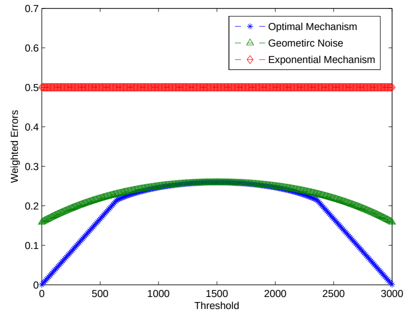

Figure 4: Uniform error penalty function and prior distribution

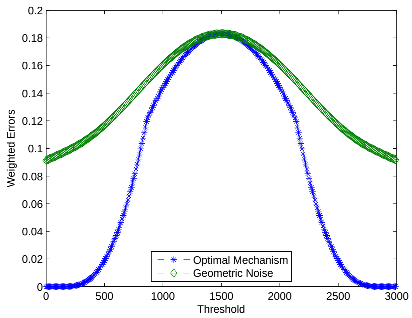

Figure 5: Non-uniform error penalty function and uniform prior distribution

Hence, the probabilities of the mechanism $\mathbf{z}'$ to commit both types of errors are at most twice that of the optimal mechanism $\mathbf{z}$, and thus, the range-restricted geometric mechanism is 2-approximate universally utility maximizing for count range queries. $\square$

G. COMPARISONS OF THE OPTIMAL MECHANISM AND GEOMETRIC NOISE

In this section, we explore the improvement of our optimal mechanism over the baseline solution using geometric noise described earlier. In the rest of this section we will refer that baseline solution as the *geometric noise*. We set the privacy parameter $\alpha = exp(0.001)$, the number of rows in a database $n = 3000$. We vary both a consumer's error penalty function and prior distribution to compare the improvement of our optimal mechanism over geometric noise. In each comparison, we fix a consumer's error penalty function and prior distribution, and vary the threshold to compare the weighted error incurred by the optimal mechanism and the geometric noise.

G.1 Uniform Error Penalty Function and Uniform Prior Distribution

In addition to our optimal mechanism and geometric noise, another alternative to guarantee differential privacy for threshold queries is to use the exponential mechanism proposed in [15]. That is, for each pair of count μ and the output r (0 or 1), we assign a score $\kappa(\mu, r)$, and the probability of outputting r when the count is μ is in proportion to $\alpha^{\kappa(\mu,r)}$. In our context, the score is specified by a combination of error penalty function and prior distribution:

$$\kappa(\mu, 1) = \begin{cases} \rho(\mu)\omega(\mu) & \text{if } \mu < \theta \\ 1 - \rho(\mu)\omega(\mu) & \text{otherwise} \end{cases}$$

and $\kappa(\mu, 0) = 1 - \kappa(\mu, 1)$. Recall that θ is the threshold. As proved in [15], the exponential mechanism is $\alpha^{2\Delta\kappa}$-differentially private where $\Delta\kappa = \max_{i=1}^{n-1}\{|\kappa(i, 1) - \kappa(i + 1, 1)|, |\kappa(i, 0) - \kappa(i + 1, 0|\}$.

Figure 4 shows the comparisons between the three mechanisms when the error penalty function and prior distribution are both uniform. We observe that the optimal differentially private mechanism outperforms both geometric noise and the exponential mechanism. Furthermore, we find that the exponential mechanism has the lowest utility. The reason why the utility is a constant for the exponential mechanism is because both the prior distribution and error weight functions are uniform, and thus, for each count, the probability to commit an error is the same. This confirms that the exponential mechanism is not an optimal mechanism for threshold queries. Therefore, in the following we will only compare the geometric mechanism and our optimal mechanism.

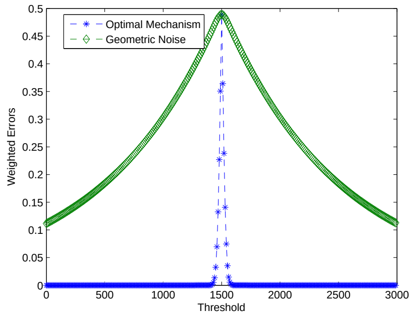

Figure 6: Uniform error penalty function and non-uniform prior distribution $\sim N(1500, 750)$

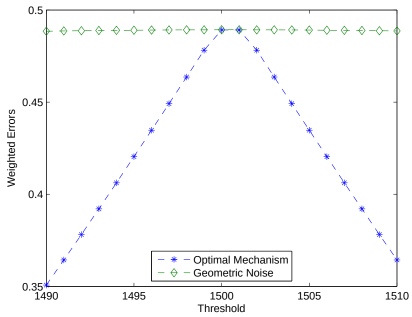

Figure 7: Peaks of uniform error penalty function and non-uniform prior distribution $\sim N(1500, 750)$

G.2 Non-uniform Error Penalty Function and Uniform Prior Distribution

As described in Section 2, the main motivation for our introduction of consumer specific error penalty functions is to provide the flexibility to measure the perceived errors for different consumers. Therefore, instead of using the uniform error penalty function, we use the following:

$$\omega(\mu) \sim exp(-\frac{10000}{|\mu - \theta|})$$

The intuition of ω is that the number of rows needed to change a "true" result of a threshold query to "false" is $|\mu - \theta|$, and when the count μ is close to θ, that number is small. Thus, the error in that sense does not severely impact utility. On the other hand, if the count μ differs from θ a lot, then the number of rows required to change the "true" result is large, and thus, the error is far from being correct in that sense, which incurs huge utility loss. Figure 5 shows the weighted errors by the optimal mechanism and the geometric noise. We can see that the improvements made by our optimal mechanism over the geometric noise are larger than that when both error penalty function and prior distribution are uniform.

G.3 Uniform Error Penalty Function and Non-uniform Prior Distribution

A non-uniform prior distribution might stem from a consumer's prior knowledge or prior interaction with the underlying database. Suppose a consumer has the following prior distribution:

$$\rho \sim N(1500, 750)$$

We present that result in Figure 6. We can see that our optimal mechanism is significantly better than the geometric noise. We also present a detailed result for the case that the threshold is between $[1490, 1510]$ in Figure 7. We can see that our optimal mechanism is still significantly better than the geometric noise. The reason why the peaks converge is that the optimal mechanism for the threshold 1500 is exactly the geometric noise in this case. An explanation for this is that the prior distribution is symmetric at 1500, and the error penalty function is uniform, thus, the combination of that prior distribution and error penalty function is still symmetric at 1500. Therefore, the optimal legal function should also be symmetric to minimize the weighted error, which is exactly the geometric noise. Next, we change the variance of that normal distribution. We set the prior distribution to be:

$$\rho \sim N(1500, 10000)$$

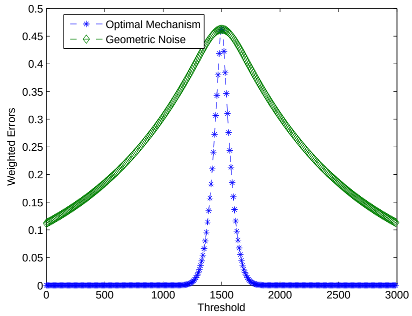

Figure 8: Uniform error penalty function and prior distribution $\sim N(1500, 10000)$

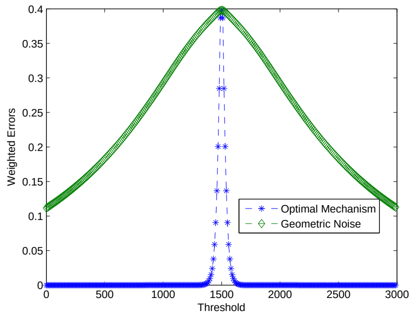

Figure 9: Non-uniform error penalty function and prior distribution

which is flatter than $N(1500, 750)$. Figure 8 shows that result, and we still see substantial improvement of our optimal mechanism over the geometric noise.

G.4 Non-uniform Error Penalty function and Non-uniform Prior Distribution

We set the error penalty function and prior distribution to be:

$$\begin{aligned} \omega(i) &\sim exp(-\frac{10000}{|i-\theta|}) \\ \rho &\sim N(1500, 10000) \end{aligned} \tag{16}$$

Figure 9 shows the result, and we can see that our optimal mechanism also substantially improves the geometric noise in significantly reducing the weighted error.