The Dirichlet Mechanism for Differential Privacy on the Unit Simplex

Parham Gohari, Bo Wu, Matthew Hale, Ufuk Topcu

***Abstract*— As members of a network share more information with each other and network providers, sensitive data leakage raises privacy concerns. To address this need for a class of problems, we introduce a novel mechanism that privatizes vectors belonging to the unit simplex. Such vectors can be seen in many applications, such as privatizing a decision-making policy in a Markov decision process. We use differential privacy as the underlying mathematical framework for these developments. The introduced mechanism is a probabilistic mapping that maps a vector within the unit simplex to the same domain according to a Dirichlet distribution. We find the mechanism well-suited for inputs within the unit simplex because it always returns a privatized output that is also in the unit simplex. Therefore, no further projection back onto the unit simplex is required. We verify the privacy guarantees of the mechanism for two cases, namely, identity queries and average queries. In the former case, we derive expressions for the differential privacy level of privatizing a single vector within the unit simplex. In the latter case, we study the mechanism for privatizing the average of a collection of vectors, each of which is in the unit simplex. We establish a trade-off between the strength of privacy and the variance of the mechanism output, and we introduce a parameter to balance the trade-off between them. Numerical results illustrate these developments.**

I. Introduction

In many decision-making problems, a policy-maker forms a control policy based on data collected from the individuals in a network. The gathered data often contains sensitive information, which raises privacy concerns [1]. In some applications, privatizing sensitive data has been achieved by adding carefully calibrated noise to sensitive data and functions thereof [2], [3], [4]. These noise-additive approaches are well-suited to some classes of numerical data, though sensitive data may take a form ill-suited to them. For example, developments in [5] explored symbolic control systems in which additive noise cannot be meaningfully implemented.

In this work, we privatize data inputs that belong to the unit simplex, *i.e.*, the set of vectors with non-negative entries that sum to one. Such vectors are seen in many decision-making problems. For example, in Markov decision processes (MDPs), the goal is to find a total-reward-maximizing policy [6], [7]. In certain cases, it is shown that the optimal policy is a randomized function that maps from the MDP's states to a probability distribution on the set of actions available at that state, see, *e.g.*, [8], [9], [10]. Finite action sets give rise to discrete, finitely supported probability distributions, which can be formalized as vectors with non-negative entries summing to one. Policies of this kind arise in applications such as autonomous driving [11] and the smart power grid [12], and revealing them can therefore reveal individuals' behaviors. Thus, there is a need to privatize such policies, and this use represents one application of privatizing sensitive data in the unit simplex. Existing noise-additive approaches will not, in general, produce a privatized vector in the unit simplex, and we therefore propose a new approach to privacy for this context.

In this paper, we use differential privacy as the underlying mathematical framework for privacy. Differential privacy, first introduced in [13], is designed to protect the exact values of sensitive pieces of data, while preserving their usefulness in aggregate statistical analyses. Two desirable properties of differential privacy are (i) that it is immune to post-processing [14], in the sense that arbitrary post-hoc transformations of privatized data do not weaken its privacy guarantees, and (ii) that it is robust to side information, in that gaining additional information about data-producing entities does not weaken its privacy guarantees by much [15]. As a result, differential privacy has been frequently used as the mathematical formulation of privacy in both computer science and, more recently, in control theory [16], [17], [18].

As the main contribution of this paper, we introduce a mechanism that privatizes a vector within the unit simplex. A mechanism is a probabilistic mapping from some pre-defined domain to a pre-defined range, and a mechanism is used to privatize sensitive data. This paper develops a novel mechanism using the Dirichlet distribution, and we therefore call it the Dirichlet mechanism. The Dirichlet distribution is a multivariate distribution supported on the unit simplex, which makes it a natural choice for this setting because its outputs are always elements of the unit simplex.

In our developments, we use probabilistic differential privacy, which is known to imply that the conventional form of differential privacy also holds [19]. Then, we show that the Dirichlet mechanism satisfies probabilistic differential privacy for identity queries. By an identity query, we mean privatizing a single vector within the unit simplex. In the course of proving these privacy guarantees, based on the assumptions we provide, we prove the log-concavity of the cumulative distribution function of a Dirichlet distribution. The proof that we present may be of independent interest in ongoing research on convexity analysis of special functions such as [20]. In this vein, we prove a generalization of Theorem 6 of [21] which has been used in later works for stochastic programming [22].

Parham Gohari is with the Department of Electrical and Computer Engineering, University of Texas at Austin, Austin, TX. Bo Wu and Ufuk Topcu are with the Department of Aerospace Engineering and Engineering Mechanics, and the Oden Institute for Computational Engineering and Sciences, University of Texas at Austin, Austin, TX. email: {pgohari, bwu3, utopcu}@utexas.edu. Matthew Hale is with the Department of Mechanical and Aerospace Engineering at the University of Florida, Gainesville, FL. email: matthewhale@ufl.edu

Beyond identity queries, we further show that the Dirichlet mechanism is differentially private for average queries, in which we privatize the average of a collection of vectors, each within the unit simplex. We derive analytic expressions for privacy levels of the averaging case, and show that the Dirichlet mechanism provides privacy protections whose strength increases with the number of vectors being averaged.

Following the convention in the differential privacy literature, we also analyze the accuracy of the output of the mechanism [14], [23]. In particular, we evaluate the accuracy of the Dirichlet mechanism in terms of the expected value and the variance of its outputs. Similar to additive noise methods, the Dirichlet mechanism output has the same expected value as its input, which implies that its privatized outputs obey a distribution centered on the underlying sensitive data. We show that there exists a trade-off between the privacy and the variance of the output of the mechanism. The derived expression for the output variance shows how to tune the worst-case variance by scaling the input by a parameter that we introduce in the mechanism definition.

We emphasize that additive noise privacy mechanisms are ill-suited to privacy on the unit simplex because they add noise of infinite support. As a result, such mechanisms will output a vector that does not belong to the unit simplex; attempting to normalize the noise would result in its distribution not being one known to provide differential privacy. It is for these reasons that we develop the Dirichlet mechanism. Although its form appears quite different from existing mechanisms, they are related through membership in a broad class of probability distributions. In particular, the Laplacian, Gaussian, and exponential mechanisms all use distributions belonging to a parameterized family of exponential distributions. The outputs of the Dirichlet distribution are equivalent to a normalized vector of i.i.d. exponential random variables, which means their distribution also belongs to the exponential family. This connection reveals why we should expect the Dirichlet mechanism to be well-suited to differential privacy, and the developments of this paper formalize and confirm this intuition.

We also point out here that the exponential mechanism is another widely used differentilly private mechanism which can be used for sensitive data ill-suited to additive approaches [14]. However, the exponential mechanism can be computationally demanding to implement for privacy applications with many possible outputs. The output space here is the unit simplex, which contains uncountably many elements. The resulting complexity of such an implementation therefore makes it infeasible [24], especially in large dimensions, and we avoid it here.

An extended version of this paper which includes the proofs to the technical lemmas used in this paper can be found at [25].

II. Preliminaries

A. Notation

In this section we establish notation used throughout the paper. We represent the real numbers by $\mathbb{R}$ and the positive reals by $\mathbb{R}_+$. For a positive integer n, let $[n] := \{1, \dots, n\}$. We denote the unit simplex in $\mathbb{R}^n$ by Δ_n where

$$\Delta_n := \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{n} x_i = 1, x_i \geq 0 \text{ for all } i \in [n] \right\}.$$

We use Δ_n° to represent the interior of Δ_n. Letting $W \subseteq [n-1]$ and $\eta, \bar{\eta} \in (0,1)$, we then define the set

$$\Delta_n^{(\eta,\bar{\eta})} := \left\{ p \in \Delta_n^\circ \mid \sum_{i \in W} p_i \leq 1 - \bar{\eta}, p_i \geq \eta \text{ for all } i \in W \right\}.$$

Letting p be a vector in $\mathbb{R}^n$, we use the notation $p_{(i,j)}$ to denote the vector $(p_i, p_j)^T \in \mathbb{R}^2$, where $(\cdot)^T$ is the transpose of a vector, and $p_{-(i,j)} \in \mathbb{R}^{n-2}$ to denote the vector p with i^{th} and j^{th} entries removed. $\mathbb{P}[\cdot]$ denotes the probability of an event. For a random variable, $\mathbb{E}[\cdot]$ denotes its expectation and $\text{Var}[\cdot]$ denotes its variance. We use the notation $|\cdot|$ for the cardinality of a finite set. $||\cdot||_1$ denotes the 1-norm of a vector. We also use special functions

$$\Gamma(z) := \int_0^\infty x^{z-1} \exp(-x) dx, \qquad z \in \mathbb{R}_+,$$

$$\text{beta}(a,b) := \int_0^1 t^{a-1}(1-t)^{b-1} dt, \qquad a, b \in \mathbb{R}_+.$$

B. Differential Privacy

Intuitively, differential privacy guarantees that two *nearby* inputs to a privacy mechanism will generate statistically similar outputs. In differential privacy, the notion of "nearby" is formally defined by an adjacency relation, and we define adjacency over the unit simplex as follows.

Definition 1. *For a constant $b \in (0,1]$ and fixed set W, two vectors $p, q \in \Delta_n^{(\eta,\bar{\eta})}$ are said to be b-adjacent if there exist indices $i, j \in W$ such that*

$$p_{-(i,j)} = q_{-(i,j)} \text{ and } ||p - q||_1 \leq b.$$

In words, two vectors are different if they differ in two entries by an amount not more than b. Ordinarily, differential privacy considers sensitive data differing in a single entry, *e.g.*, one entry in a database [14]. However, it is not possible to do so for an element of the unit simplex because changing only a single entry would violate the condition that vectors' entries sum to one. We therefore consider privacy with the above adjacency relation. Privacy itself is defined next.

Definition 2. *(Probabilistic differential privacy; [26]) Let $b \in (0,1]$ and $W \subseteq [n-1]$ be given. Fix a probability space $(\Omega, \mathcal{F}, \mathbb{P})$. A mechanism $\mathcal{M} : \Delta_n^{\eta,\bar{\eta}} \times \Omega \mapsto \Delta_n$ is said to be probabilistically (ϵ, δ)-differentially private if, for all $p \in \Delta_n^{\eta,\bar{\eta}}$, we can partition the output space Δ_n into two disjoint sets Ω_1, Ω_2, such that*

$$\mathbb{P}[\mathcal{M}(p) \in \Omega_2] \leq \delta, \tag{1}$$

and for all $q \in \Delta_n^{\eta,\bar{\eta}}$ b-adjacent to p and for all $x \in \Omega_1$,

$$\log\left(\frac{\mathbb{P}[\mathcal{M}(p) = x]}{\mathbb{P}[\mathcal{M}(q) = x]}\right) \leq \epsilon.$$

Probabilistic differential privacy is known to imply conventional differential privacy [26], and, with a slight abuse of terminology, we refer to Definition 2 simply as "differential privacy" for the remainder of the paper.

C. Dirichlet Mechanism

One contribution of this paper is to present a differentially private mechanism that, without any need of projection, maps elements of Δ_n to Δ_n. In order to do so, we first introduce the Dirichlet mechanism. A Dirichlet mechanism with parameter $k \in \mathbb{R}_+$, denoted by $\mathcal{M}_D^{(k)}$, takes as input a vector $p \in \Delta_n^\circ$ and outputs $x \in \Delta_n$ according to the Dirichlet probability distribution function (PDF) centered on p, *i.e.*,

$$\mathbb{P}[\mathcal{M}_D^{(k)}(p) = x] = \frac{1}{\mathrm{B}(kp)} \prod_{i=1}^{n-1} x_i^{kp_i - 1} \left(1 - \sum_{i=1}^{n-1} x_i\right)^{kp_n - 1},$$

where

$$\mathrm{B}(kp) := \frac{\prod_{i=1}^{n} \Gamma(kp_i)}{\Gamma\left(k \sum_{i=1}^{n} p_i\right)} \tag{2}$$

is the multi-variate beta function.

We later use the parameter k to adjust the trade-off that we establish between the accuracy and the privacy level of the Dirichlet mechanism. Next, we establish the privacy guarantees that the Dirichlet mechanism provides.

III. Dirichlet Mechanism for Differential Privacy of Identity Queries

We begin by analyzing identity queries under the Dirichlet mechanism. Here, a sensitive vector p is directly input to the Dirichlet mechanism to make it approximately indistinguishable from other adjacent sensitive vectors. To show the level of privacy that holds, we first bound δ, then bound ϵ.

A. Computing δ

Fix $W \subseteq [n-1]$. In accordance with Definition 2, we partition the output space of the Dirichlet mechanism into two sets Ω_1, Ω_2 defined by

$$\Omega_1 := \{x \in \Delta_n \mid x_i \geq \gamma \text{ for all } i \in W\} \tag{3}$$

and

$$\Omega_2 := \{x \in \Delta_n \mid x \notin \Omega_1\}, \tag{4}$$

where $\gamma \in (0,1)$ is a parameter that defines these sets.

Our goal is to show that the Dirichlet mechanism output belongs to Ω_1 with high probability. Let p be a vector in $\Delta_n^{(\eta,\bar{\eta})}$. In the next lemma we show how to calculate $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$.

Lemma 1. *Let $W \subseteq [n-1]$ be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$, let $p \in \Delta_n^{(\eta,\bar{\eta})}$ and let*

$$\mathcal{A}_r := \left\{ x \in \mathbb{R}^{r-1} \mid \sum_{i \in [r-1]} x_i \leq 1, x_i \geq \gamma \text{ for all } i \in W \right\},$$

for all $r \geq |W| + 1$. Then, for a Dirichlet mechanism with parameter $k \in \mathbb{R}+$, we have that $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is equal to

$$\frac{\int_{\mathcal{A}_{|W|+1}} \prod_{i \in W} x_i^{kp_i - 1} \left(1 - \sum_{i \in W} x_i\right)^{k(1 - \sum_{i \in W} p_i) - 1} \prod_{i \in W} dx_i}{\mathrm{B}(k\tilde{p}_W)},$$

where $\tilde{p}_W \in \Delta_{|W|+1}$ is equal to p with its entries outside the set W removed, and with an additional entry equal to $1 - \sum_{i \in W} p_i$ appended as its final entry.

Proof. Without loss of generality, take $W = [|W|]$. In order to find $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$, we need to integrate the Dirichlet PDF over the region $\mathcal{A}_n$. Therefore, we need to evaluate the $(n-1)$-fold integral

$$\frac{\int_{\mathcal{A}_n} \prod_{i=1}^{n-1} x_i^{kp_i - 1} \left(1 - \sum_{i=1}^{n-1} x_i\right)^{kp_n - 1} dx_{n-1} \ldots dx_1}{\mathrm{B}(kp)}. \tag{5}$$

Using a method similar to the one adopted in [27], let $y := \sum_{i=1}^{n-2} x_i$. Then we can rewrite (5) as

$$\frac{1}{\mathrm{B}(kp)} \int_{\mathcal{A}_{n-2}} \int_0^{1-y} \prod_{i=1}^{n-1} x_i^{kp_i - 1} (1 - y - x_{n-1})^{kp_n - 1} dx_{n-1} \ldots dx_1. \tag{6}$$

Now let $u := \frac{x_{n-1}}{1-y}$ and take the inner integral with respect to u. Then (6) becomes

$$\frac{1}{\mathrm{B}(kp)} \int_{\mathcal{A}_{n-2}} \prod_{i=1}^{n-2} x_i^{kp_i - 1} (1-y)^{k(p_{n-1}+p_n)-1} \int_0^1 u^{kp_{n-1}-1} (1-u)^{kp_n - 1} du \; dx_{n-2} \ldots dx_1.$$

From the definition of the beta function, we have

$$\int_0^1 u^{kp_{n-1}-1} (1-u)^{kp_n - 1} du = \mathrm{beta}(kp_{n-1}, kp_n).$$

Using the gamma function representation of beta functions, *i.e.*,

$$\mathrm{beta}(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}, \; a, b \in \mathbb{R}_+, \tag{7}$$

and (2), we find that $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is equal to

$$\frac{1}{\mathrm{B}(kp)} \frac{\Gamma(kp_{n-1})\Gamma(kp_n)}{\Gamma(k(p_{n-1}+p_n))} \int_{\mathcal{A}_{n-2}} \prod_{r=1}^{n-2} x_r^{kp_r - 1} \left(1 - \sum_{l=1}^{n-2} x_l\right)^{k(p_{n-1}+p_n)-1} dx_{n-2} \ldots dx_1.$$

Using the same trick, for the next step, let $y := \sum_{l=1}^{n-3} x_l$ and

$u := \frac{x_{n-2}}{1-y}$. Then $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is equal to

$$\frac{1}{\mathrm{B}(kp)} \frac{\Gamma(kp_{n-2})\Gamma(kp_{n-1})\Gamma(kp_n)}{\Gamma(k(p_{n-2}+p_{n-1}+p_n))} \int_{\mathcal{A}_{n-3}} \prod_{r=1}^{n-3} x_r^{kp_r-1} \left(1-\sum_{l=1}^{n-3} x_l\right)^{k(p_{n-2}+p_{n-1}+p_n)-1} dx_{n-3}\dots dx_1.$$

We continue to adopt the same change of variable strategy until we are left with an integral over the region $\mathcal{A}_{|W|+1}$, which concludes the proof. ■

In the previous lemma we showed how to calculate $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$. In particular we showed that instead of an $(n-1)$-fold integral of the Dirichlet PDF, the computations can be reduced to a $|W|$-fold integral. However, the expression still depends on the input vector p, which is undesirable and generally incompatible with differential privacy. The reason is that (ϵ, δ)-differential privacy is a guarantee for all adjacent input data and not for a specific data point. In the next lemma, we show that $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is a log-concave function of p over the region $\Delta_n^{(\eta,\bar{\eta})}$, which we will use to derive a bound for δ that holds for all p of interest.

Lemma 2. *Let W be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$ and let $\mathcal{M}_D^{(k)}$ be the Dirichlet mechanism with parameter k and input p. Then, $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is a log-concave function of p over the domain $\Delta_n^{(\eta,\bar{\eta})}$.*

The proof of this lemma may be found in the extended version at [25]. Revisiting the definition of Ω_1, Ω_2 in (3) and (4), we find that

$$\begin{aligned}\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_2] &= 1 - \mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1] \\ &\leq 1 - \min_p \mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1] = \delta.\end{aligned} \tag{8}$$

From this, we see that bounding δ can be by minimizing $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$, an explicit form of which was given in Lemma 1. Above, we established the log-concavity of the function that we seek to minimize. As a result, instead of minimizing $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ over the entire continuous domain of $\Delta_n^{(\eta,\bar{\eta})}$, we can only consider the extreme points. Note that the set of points within $\Delta_n^{(\eta,\bar{\eta})}$ form a polyhedron with at most $|W|(|W|+1)/2$ vertices. As the minimum of an unsorted list of n entries can be found in linear time, the time complexity of finding $\min \mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is $\mathcal{O}(|W|^2)$. This analytical bound will be further explored through numerical results in Section VI. Next, we develop analogous bounds for ϵ.

B. Computing ϵ

As above, fix $\eta, \bar{\eta} \in (0,1)$, $b \in (0,1]$, and $W \subseteq [n-1]$. Then, for a given $k \in \mathbb{R}_+$, bounding ϵ requires evaluating the term

$$\log\left(\frac{\mathbb{P}[\mathcal{M}_D^{(k)}(p) = x]}{\mathbb{P}[\mathcal{M}_D^{(k)}(q) = x]}\right),$$

where p and q are any b-adjacent vectors in $\Delta_n^{(\eta,\bar{\eta})}$. Let $i, j \in W$ be the indices in which p and q differ. Using the definition of the Dirichlet mechanism, we find

$$\begin{aligned}\log\left(\frac{\mathbb{P}[\mathcal{M}_D^{(k)}(p) = x]}{\mathbb{P}[\mathcal{M}_D^{(k)}(q) = x]}\right) &= \log\left(\frac{\mathrm{B}(kq)\prod_{i=1}^n x_i^{kp_i-1}}{\mathrm{B}(kp)\prod_{i=1}^n x_i^{kq_i-1}}\right) \\ &= \log\left(\frac{\Gamma(kq_i)\Gamma(kq_j)x_i^{kp_i-1}x_j^{kp_j-1}}{\Gamma(kp_i)\Gamma(kp_j)x_i^{kq_i-1}x_j^{kq_j-1}}\right) \\ &= \log\left(\frac{\Gamma(kq_i)\Gamma(kq_j)}{\Gamma(kp_i)\Gamma(kp_j)} x_i^{k(p_i-q_i)} x_j^{k(p_j-q_j)}\right).\end{aligned}$$

Since p and q are b-adjacent, we have that $p_i + p_j = q_i + q_j$. Therefore, we can compute ϵ by evaluating the term

$$\log\left(\frac{\Gamma(kq_i)\Gamma(kq_j)}{\Gamma(kp_i)\Gamma(kp_j)}\left(\frac{x_i}{x_j}\right)^{k(p_i-q_i)}\right). \tag{9}$$

Note that if either x_i or x_j goes to 0, then the term in (9) would be unbounded. Recalling that the indices in which p and q can differ at are restricted to the set W, we find that the values at these indices must be bounded below by η, and therefore the ratios of interest remain bounded as well.

Lemma 4 below will provide an explicit value of ϵ, aided in part by the next lemma.

Lemma 3. *Let W be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$ and let p, q be any b-adjacent vectors in $\Delta_n^{(\eta,\bar{\eta})}$ with their i^{th} and j^{th} entries different. Then, for a constant $k \in \mathbb{R}_+$, we have that*

$$\frac{\mathrm{beta}(kq_i, kq_j)}{\mathrm{beta}(kp_i, kp_j)} \leq \frac{\mathrm{beta}(kq_i, k(1-\bar{\eta}-q_i))}{\mathrm{beta}(kp_i, k(1-\bar{\eta}-p_i))}.$$

The proof of this lemma may be found in the extended version of this paper at [25].

Lemma 4. *Let W be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$ and $\mathcal{M}_D^{(k)}$ be a Dirichlet mechanism with parameter k. Then, for all $x \in \Omega_1$ we have that*

$$\begin{aligned}\log\left(\frac{\mathbb{P}[\mathcal{M}_D^{(k)}(p) = x]}{\mathbb{P}[\mathcal{M}_D^{(k)}(q) = x]}\right) \leq \\ \log\left(\frac{\mathrm{beta}(k\eta, k(1-\bar{\eta}-\eta))}{\mathrm{beta}(k(\eta+\frac{b}{2}), k(1-\bar{\eta}-\eta-\frac{b}{2}))}\right) \\ + \frac{kb}{2}\log\left(\frac{1-(|W|-1))\gamma}{\gamma}\right),\end{aligned}$$

where the parameter $\gamma \in (0,1)$ takes the same value of γ used to compute δ in Section III-A.

Proof. Let

$$
\begin{aligned}
v := \quad & \max_{p,q,x} \quad \log\left(\frac{\Gamma(kq_i)\Gamma(kq_j)}{\Gamma(kp_i)\Gamma(kp_j)}\left(\frac{x_i}{x_j}\right)^{k(p_i-q_i)}\right) \\
& \text{subject to} \quad |p_i - q_i| \le \frac{b}{2}, \\
& \qquad\qquad p_i + p_j = q_i + q_j, \\
& \qquad\qquad p_i + p_j \le 1 - \bar{\eta}, \\
& \qquad\qquad p_{(i,j)} \in [\eta, 1 - \bar{\eta} - \eta], \\
& \qquad\qquad q_{(i,j)} \in [\eta, 1 - \bar{\eta} - \eta], \\
& \qquad\qquad x_{(i,j)} \in [\gamma, 1 - (|W| - 1)\gamma],
\end{aligned} \tag{10}
$$

and let $\mathcal{C}$ denote the set of feasible points of the optimization problem in (10); we note that the first constraint enforces adjacency, while the others encode $p, q \in \Delta_n^{(\eta,\bar{\eta})}$ and $x \in \Omega_1$.

By sub-additivity of the maximum, we have

$$
\begin{aligned}
v \le \max_{p,q,x\in\mathcal{C}} \log\left(\frac{\Gamma(kq_i)\Gamma(kq_j)}{\Gamma(kp_i)\Gamma(kp_j)}\right) + \\
\max_{p,q,x\in\mathcal{C}} \log\left(\frac{x_i}{x_j}\right)^{k(p_i-q_i)}.
\end{aligned} \tag{11}
$$

Now, with

$$
v_1 := \max_{p,q,x\in\mathcal{C}} \log\left(\frac{x_i}{x_j}\right)^{k(p_i-q_i)},
$$

we find

$$
\begin{aligned}
v_1 &\le \max_{p,q,x\in\mathcal{C}} |k(p_i - q_i)| \left|\log\left(\frac{x_i}{x_j}\right)\right| \\
&= \frac{kb}{2}\log\left(\frac{1 - (|W| - 1)\gamma}{\gamma}\right).
\end{aligned}
$$

Next, let $c := p_i + p_j = q_i + q_j$ and substitute q_j, p_j with $c - q_i$ and $c - p_i$ respectively. Let

$$
\begin{aligned}
v_2 := \quad & \max_{p_i,q_i,c} \quad \log\left(\frac{\Gamma(kq_i)\Gamma(k(c - q_i))}{\Gamma(kp_i)\Gamma(k(c - p_i))}\right) \\
& \text{subject to} \quad |p_i - q_i| \le \frac{b}{2}, \\
& \qquad\qquad c \in [2\eta, 1 - \bar{\eta}], \\
& \qquad\qquad p_i \in [\eta, 1 - \bar{\eta} - \eta], \\
& \qquad\qquad q_i \in [\eta, 1 - \bar{\eta} - \eta],
\end{aligned}
$$

where the constraints again encode adjacency of p and q and their containment in $\Delta_n^{(\eta,\bar{\eta})}$.

Then, from Lemma 3 and Equation (7), we have that

$$
\begin{aligned}
v_2 \le \quad & \max_{p_i,q_i,c} \quad \log\left(\frac{\text{beta}(kq_i, k(1 - \bar{\eta} - q_i))}{\text{beta}(kp_i, k(1 - \bar{\eta} - p_i))}\right) \\
& \text{subject to} \quad |p_i - q_i| \le \frac{b}{2}, \\
& \qquad\qquad p_i \in [\eta, 1 - \bar{\eta} - \eta], \\
& \qquad\qquad q_i \in [\eta, 1 - \bar{\eta} - \eta].
\end{aligned} \tag{12}
$$

Evaluating the gradient of the objective function in the optimization problem in (12), it can be shown that the Karush-Kuhn-Tucker (KKT) conditions of optimality are not satisfied in the interior of the set of feasible points except for points that lie on the line $p_i = q_i$. However, since the KKT conditions are only sufficient conditions (see chapter 11 of [28]), satisfying them does not imply optimality which is indeed the case here.

Evaluating points on the boundary of the feasible region shows that KKT conditions are also not satisfied, thus, the only points remaining are (p_i, q_i)'s in the set

$$
\begin{aligned}
\left\{\left(\eta + \frac{b}{2}, \eta\right), \left(1 - \bar{\eta} - \eta - \frac{b}{2}, 1 - \bar{\eta} - \eta\right),\right. \\
\left.\left(\eta, \eta + \frac{b}{2}\right), \left(1 - \bar{\eta} - \eta, 1 - \bar{\eta} - \eta - \frac{b}{2}\right)\right\}.
\end{aligned} \tag{13}
$$

Note that since $\text{beta}(a, b) = \text{beta}(b, a)$, the points in the first row give equal positive objectives and the points in the second row have equal negative objectives. Hence, we can choose the first point in Equation (13) to find

$$
v_2 = \log\left(\frac{\text{beta}(k\eta, k(1 - \bar{\eta} - \eta))}{\text{beta}(k(\eta + \frac{b}{2}), k(1 - \bar{\eta} - \eta - \frac{b}{2}))}\right). \tag{14}
$$

Substituting v_1 and v_2 in (11) concludes the proof. ∎

We now state the main theorem of this section, which formally establishes the (ϵ, δ)-differential privacy of the Dirichlet mechanism for identity queries.

Theorem 1. *Fix $\eta, \bar{\eta} \in (0, 1)$ and $b \in (0, 1]$, and consider b-adjacent vectors $p, q \in \Delta_n^{(\eta,\bar{\eta})}$. Let $W \subseteq [n - 1]$ be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$. Then the Dirichlet mechanism with parameter $k \in \mathbb{R}_+$ is (ϵ, δ)-differentially private, where*

$$
\begin{aligned}
\epsilon = \log\left(\frac{\text{beta}(k\eta, k(1 - \bar{\eta} - \eta))}{\text{beta}(k(\eta + \frac{b}{2}), k(1 - \bar{\eta} - \eta - \frac{b}{2}))}\right) + \\
\frac{kb}{2}\log\left(\frac{1 - (|W| - 1)\gamma}{\gamma}\right),
\end{aligned}
$$

and

$$
\delta = 1 - \min_p \mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1].
$$

Proof. The expression for ϵ results immediately from Lemma 4 and the expression for δ is a direct result of (8). ∎

The expression given for ϵ in Theorem 1 contains a ratio of beta functions. In the following lemma we present upper and lower bounds for beta functions in terms of simpler functions to provide a simplified upper bound for ϵ.

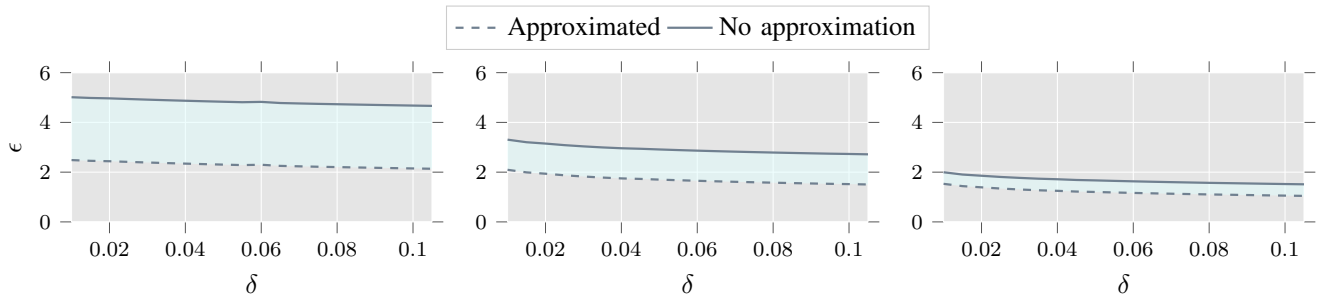
Lemma 5. *Let $a, b > 1$. Then*

$$
\exp(2 - a - b) \le \text{beta}(a, b) \le \frac{a + b - 1}{(2a - 1)(2b - 1)}. \tag{15}
$$

Proof: See [25]. ∎

Lemma 5 offers a straightforward simplification of Theorem 1, though due to space restrictions we evaluate its accuracy numerically.

Remark. Note that if a mechanism is ϵ_1-differentially private, it is also ϵ_2-differentially private for all $\epsilon_2 \ge \epsilon_1$. Therefore, if the upper bound for ϵ after simplification of beta functions



a: $\eta = 0.15$, $\bar{\eta} = 0.15$, $k = 6.7$ b: $\eta = 0.20$, $\bar{\eta} = 0.20$, $k = 5.1$ c: $\eta = 0.25$, $\bar{\eta} = 0.25$, $k = 4.1$

Fig. 1: An example where $|W| = 3$ to compare the approximated and original values of ϵ. At each level of δ, first γ is optimized according to the optimization problem in (16), then the optimal γ is substituted in the expressions for the original and approximated values.

is still within the acceptable range, *e.g.,* $\delta \leq 0.05$ and $\epsilon \leq 5$ [29], [30], [31], then using the approximate value of ϵ does not substantially harm interpretation of the Dirichlet mechanism's protections. In Figure 1, for three instances of $(\eta, \bar{\eta}, k)$ and $b = 0.1$, we show how the approximation captures the behavior of ϵ. All three cases show that the approximation causes an offset to the exact value of ϵ, and the level of offset decreases with the value of the original ϵ.

Next, we point out that the parameter γ, which is used in the definition of Ω_2, is not a parameter of the mechanism, in the sense that changing γ does not change the mechanism itself. Instead, γ balances the trade-off between privacy level and the probability of failing to guarantee that privacy level, *i.e.,* changing γ can decrease ϵ in exchange for increasing δ and vice versa.

In some cases, we are given the highest probability of privacy failure, δ, that is acceptable, and one must maximize the level of privacy subject to that upper bound. Let $\hat{\delta}$ denote maximum admissible value of δ. Then we are interested in minimizing ϵ while obeying $\delta \leq \hat{\delta}$. Using Theorem 1 to substitute ϵ, let V be the set of vertices of $\Delta_n^{(\eta,\bar{\eta})}$. Then we must solve

$$\begin{aligned} &\min_{\gamma} \quad \gamma \\ &\text{subject to} \quad \mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1] \geq 1 - \hat{\delta} \text{ for all } p \in V. \end{aligned} \tag{16}$$

Note that the constraint set of the optimization problem (16) form a convex set as the function $\mathbb{P}[\mathcal{M}_D^{(k)}(p) \in \Omega_1]$ is a strictly decreasing function of γ. Therefore, ϵ can be optimized for a given $\hat{\delta}$ using off-the-shelf convex optimization tool-boxes, and this will be done below in Section VI. Next, we apply the Dirichlet mechanism to average queries.

IV. Dirichlet Mechanism for Differential Privacy of Average Queries

In this section we consider a collection of N vectors indexed over $i \in [N]$, with the i^{th} denoted $p^i \in \Delta_n^\circ$. The goal is to compute the average of the collection $\{p^i\}_{i\in[N]}$ while providing differential privacy. We first re-define the adjacency relationship for the average query setting.

Definition 3. *Fix a scalar $b \in (0, 1]$. Two collections $\{p^i\}_{i\in[N]}$ and $\{q^i\}_{i\in[N]}$ are adjacent if there is some j such that*

1) *$p^i = q^i$ for all $j \neq i$,*
2) *there exist m and l such that $p^j_{-(m,l)} = q^j_{-(m,l)}$ and $||p^j_{(m,l)} - q^j_{-(m,l)}|| \leq b$.*

As mentioned earlier, the query we now consider is the average. Set $\mathcal{P} = \{p^i\}_{i\in[N]}$ and $\mathcal{Q} = \{q^i\}_{i\in[N]}$. Mathematically we write

$$\mathcal{A}(\mathcal{P}) := \frac{1}{N}\sum_{i=1}^{N} p^i, \tag{17}$$

with $\mathcal{A}(\mathcal{Q})$ defined analogously. The next theorem formalizes the privacy protections of the Dirichlet mechanism when applied to such averages.

Theorem 2. *Fix $\eta, \bar{\eta} \in (0, 1)$ and $b \in (0, 1]$. Let $W \subseteq [n-1]$ be a given set of indices which is used to construct $\Delta_n^{(\eta,\bar{\eta})}$, let $\mathcal{P} = \{p^i\}_{i\in[N]}$ be a collection of N-vectors within $\Delta_n^{(\eta,\bar{\eta})}$, let $\mathcal{A}(\mathcal{P})$ be the average of the collection, and let $\mathcal{Q} = \{q^i\}_{i\in[N]}$ be adjacent to $\mathcal{P}$. Then the Dirichlet mechanism with parameter $k \in \mathbb{R}_+$ and input $\mathcal{A}(\mathcal{P})$ is (ϵ, δ)-differentially private, where*

$$\epsilon = \log\left(\frac{\text{beta}(k\eta, k(1-\bar{\eta}-\eta))}{\text{beta}(k(\eta+\frac{b}{2n}), k(1-\bar{\eta}-\eta-\frac{b}{2n}))}\right) + \frac{kb}{2n}\log\left(\frac{1-(|W|-1)\gamma}{\gamma}\right), \tag{18}$$

and

$$\delta = 1 - \min_{\mathcal{A}(\mathcal{P})} \mathbb{P}[\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{P})) \in \Omega_1]. \tag{19}$$

Proof. For all $i \in [n]$, let $A(p_i) := \mathcal{A}(\mathcal{P})_i$ and $x \in \Omega_1$. Then, we are interested in the quantity

$$\frac{\mathbb{P}[\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{P})) = x]}{\mathbb{P}[\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{Q})) = x]} = \frac{\text{B}(k\mathcal{A}(\mathcal{Q}))\prod_{i=1}^{n} x_i^{kA(p_i)-1}}{\text{B}(k\mathcal{A}(\mathcal{P}))\prod_{i=1}^{n} x_i^{kA(q_i)-1}}. \tag{20}$$

Based on the definition of the adjacency relationship for average queries in Definition 3, $A(p)$ and $A(q)$ will differ only in their m^{th} and l^{th} entries. Taking the logarithm from both sides of (20) and using the same approach for the identity queries we have that

$$\log\left(\frac{\mathbb{P}[\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{P}))=x]}{\mathbb{P}[\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{Q}))=x]}\right)\leq \max_{\mathcal{A}(\mathcal{P}),\mathcal{A}(\mathcal{Q})}\log\left(\frac{\mathrm{B}(k\mathcal{A}(\mathcal{Q}))}{\mathrm{B}(k\mathcal{A}(\mathcal{P}))}\right)+ \max_{\mathcal{A}(\mathcal{P}),\mathcal{A}(\mathcal{Q})}\log\left(\frac{1-(|W|-1)\gamma}{\gamma}\right)^{k|A(p_m)-A(q_m)|}. \tag{21}$$

Because $\mathcal{P}$ and $\mathcal{Q}$ are b-adjacent, and each entry of $\mathcal{A}(\cdot)$ represents the average of the vectors, we have that

$$|A(p_m)-A(q_m)|\leq\frac{b}{2n}. \tag{22}$$

Combining (21), (22) and Lemma 4 completes the proof for the value of ϵ. For δ, same approach for calculating δ in identity queries applies to average queries. ■

Remark. As seen in (18), the level of privacy increases with the number of vectors present in the collection. In particular, $\epsilon\to 0$ as $n\to\infty$. This is consistent with the intuition that it would be harder to track each individual of a population when their data is mixed together in an act of averaging.

V. Accuracy Analysis

We briefly analyze the accuracy of the Dirichlet mechanism by two metrics. First, in terms of the expected location of the mechanism output on the unit simplex and second in terms of the variance of the output vector.

Proposition 1. *Let $x\in\Delta_n$ be the output of a Dirichlet mechanism with input $p\in\Delta_n^\circ$ and parameter $k\in\mathbb{R}_+$. Then we have that $\mathbb{E}[x_i]=p_i$ and*

$$\mathrm{Var}[x_i]=\frac{p_i(1-p_i)}{k+1}. \tag{23}$$

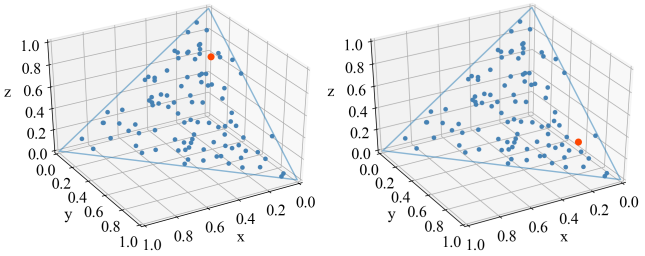
Proof. See [25]. ■

Remark. As seen in (23) the variance of the output depends on the input data p_i. However, we can find the worst-case variance by maximizing the expression for the variance which occurs at $p_i=0.5$. Hence, we have that

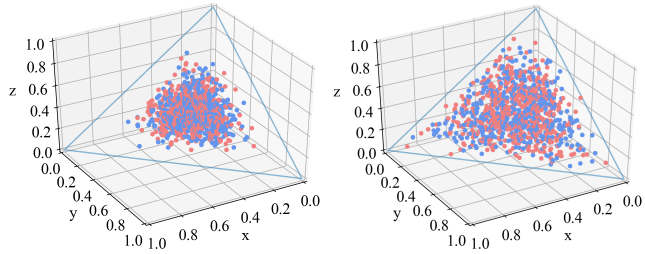
$$Var[x_i]\leq\frac{1}{4(k+1)}. \tag{24}$$

VI. Simulation Results

In this section, we simulate the output of the Dirichlet mechanism for an average query. As an example of average queries, suppose we ask a number of experts for their opinion on the probability of certain events happening, thus, a vector in the unit simplex. In order to make a decision based on all opinions, we need to integrate the opinions into one [32]. One possible way of integrating the opinions is to take the average of the opinions. Privatizing the average of the experts' opinion while keeping their individual forecasts private is an example of average queries.



(a) Visualization of two 1-adjacent vector collections $\mathcal{P}$ and $\mathcal{Q}$. The left figure depicts $\mathcal{P}$ and the right figure corresponds to $\mathcal{Q}$. The data points with orange markers correspond to the vectors in which $\mathcal{P}$ and $\mathcal{Q}$ differ.



(b) The output of the Dirichlet mechanism when the input is $\mathcal{P}$ vs. $\mathcal{Q}$. The left plot shows the case where $k=24$ and the right plot corresponds to $k=10$. Each red data point corresponds to an independent run of $\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{P}))$ and the blue data points correspond to $\mathcal{M}_D^{(k)}(\mathcal{A}(\mathcal{Q}))$.

Fig. 2: An average query on a collection of 100 vectors within Δ_3.

In Figure 2, we show an example of privatizing the average of 100 experts' opinions. In this example we have a collection of opinions $\mathcal{P}$, and we want to compare the output of the Dirichlet mechanism with the output of the mechanism when fed with a collection $\mathcal{Q}$ that is 1-adjacent to $\mathcal{P}$.

We chose $k=24$ to keep the variance of the output below 0.01 according to (24). We have fixed W to be the set $\{1,2\}$, $\eta=0.05$ and $\bar{\eta}=0.05$. Using Theorem 2, for $\hat{\delta}=0.05$, we find that the mechanism is $(1.18,0.05)$-differentially private. Table I shows the empirical accuracy analysis of mechanism. In Figure 2, we can observe that, given the location of the mechanism output, it is not possible to determine with high probability whether the input is $\mathcal{P}$ or $\mathcal{Q}$. Table I, shows that we were able to achieve the desired variance.

In order to illustrate the effect of changing k in the mechanism accuracy, Figure 2b compares the output of the mechanism when $k=24$ and $k=10$. As seen in the figure, the output when $k=10$ is less concentrated around the average. It can also be seen that the probability that the output belongs to Ω_2 is higher when $k=10$, which is consistent with the expressions derived in the theorems.

Statistics	Values
$\mathcal{A}(\mathcal{P})$	$(0.314923, 0.315923, 0.320923)$
$\mathcal{A}(\mathcal{Q})$	$(0.314923, 0.320923, 0.315923)$
$\hat{\mathcal{M}}_D(\mathcal{A}(\mathcal{P}))$	$(0.327731, 0.336119, 0.336149)$
$\hat{\mathcal{M}}_D(\mathcal{A}(\mathcal{Q}))$	$(0.326620, 0.338976, 0.334402)$
$\hat{Var}[\mathcal{M}_D(\mathcal{A}(\mathcal{P}))]$	$(0.00934632, 0.00983122, 0.0102117)$
$\hat{Var}[\mathcal{M}_D(\mathcal{A}(\mathcal{Q}))]$	$(0.00922426, 0.0100889, 0.0100757)$

TABLE I: Comparing the average of the output of the mechanism with input collections $\mathcal{P}$ and $\mathcal{Q}$, alongside with their empirical variances. The values correspond to $k = 24$.

VII. Conclusion

In this work we introduced a mechanism used for privatizing data inputs that belong to the unit simplex. We used the Dirichlet distribution to probabilistically map a vector within the unit simplex to itself. We proved that the Dirichlet mechanism is differentially private with high probability in both identity and average queries. Our simulation results validated that the privacy bounds and the accuracy of the mechanism are within ranges typically considered in the differential privacy literature.

As an extension to this work, we are interested in applying the Dirichlet mechanism to privatizing a policy in a Markov decision process. In particular, we are interested in showing how accurate the Dirichlet mechanism is in terms of the total-accumulated rewards.

References

[1] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[2] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, March 2017.

[3] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 395–408, March 2018.

[4] M. Hale, A. Jones, and K. Leahy, "Privacy in feedback: The differentially private lqg," in *2018 Annual American Control Conference (ACC)*, June 2018, pp. 3386–3391.

[5] A. Jones, K. Leahy, and M. Hale, "Towards differential privacy for symbolic systems," in *2019 American Control Conference (ACC)*, July 2019, pp. 372–377.

[6] M. L. Puterman, *Markov Decision Processes.: Discrete Stochastic Dynamic Programming*. John Wiley & Sons, 2014.

[7] R. S. Sutton, A. G. Barto *et al.*, *Introduction to reinforcement learning*. MIT press Cambridge, 1998, vol. 2, no. 4, ch. 3.

[8] Y. Savas, M. Ornik, M. Cubuktepe, M. O. Karabag, and U. Topcu, "Entropy maximization for markov decision processes under temporal logic constraints," *IEEE Transactions on Automatic Control*, 2019.

[9] B. Wu, M. Cubuktepe, and U. Topcu, "Switched linear systems meet markov decision processes: Stability guaranteed policy synthesis," in *2019 IEEE 58th Annual Conference on Decision and Control (CDC)*. IEEE, 2019, to appear, preprint arXiv:1904.11456.

[10] K. Chatterjee, R. Majumdar, and T. A. Henzinger, "Markov decision processes with multiple objectives," in *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, 2006, pp. 325–336.

[11] S. Brechtel, T. Gindele, and R. Dillmann, "Probabilistic mdp-behavior planning for cars," in *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, Oct 2011, pp. 1537–1542.

[12] S. Misra, A. Mondal, S. Banik, M. Khatua, S. Bera, and M. S. Obaidat, "Residential energy management in smart grid: A markov decision process-based approach," in *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of things and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 1152–1157.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of cryptography conference*. Springer, 2006, pp. 265–284.

[14] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[15] S. P. Kasiviswanathan and A. Smith, "On the'semantics' of differential privacy: A bayesian formulation," *Journal of Privacy and Confidentiality*, vol. 6, no. 1, 2014.

[16] K. Nissim and A. Wood, "Is privacy privacy?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2128, p. 20170358, 2018.

[17] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *2016 IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 4252–4272.

[18] S. Han and G. J. Pappas, "Privacy in control and dynamical systems," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 309–332, 2018.

[19] M. Gotz, A. Machanavajjhala, G. Wang, X. Xiao, and J. Gehrke, "Publishing search logs—a comparative study of privacy guarantees," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 3, pp. 520–532, 2011.

[20] D. B. Karp, "Normalized incomplete beta function: log-concavity in parameters and other properties," *Journal of Mathematical Sciences*, vol. 217, no. 1, pp. 91–107, 2016.

[21] A. Prékopa, "On logarithmic concave measures and functions," *Acta Scientiarum Mathematicarum*, vol. 34, pp. 335–343, 1973.

[22] A. Prékopa, "Logarithmic concave measures with application to stochastic programming," *Acta Scientiarum Mathematicarum*, vol. 32, pp. 301–316, 1971.

[23] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, Oct 2007, pp. 94–103.

[24] S. Vadhan, "The complexity of differential privacy," in *Tutorials on the Foundations of Cryptography*. Springer, 2017, pp. 347–450.

[25] P. Gohari, B. Wu, M. Hale, and U. Topcu, "The dirichlet mechanism for differential privacy on the unit simplex," extended version. [Online]. Available: https://users.oden.utexas.edu/~bwu/ACC2020_With_Proofs.pdf

[26] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*. IEEE Computer Society, 2008, pp. 277–286.

[27] J. Rao and M. Sobel, "Incomplete dirichlet integrals with applications to ordered uniform spacings," *Journal of Multivariate Analysis*, vol. 10, no. 4, pp. 603–610, 1980.

[28] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[29] F. McSherry and R. Mahajan, "Differentially-private network trace analysis," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 123–134, 2011.

[30] L. Bonomi, L. Xiong, R. Chen, and B. Fung, "Privacy preserving record linkage via grams projections," *arXiv preprint arXiv:1208.2773*, 2012.

[31] J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, B. C. Pierce, and A. Roth, "Differential privacy: An economic method for choosing epsilon," in *2014 IEEE 27th Computer Security Foundations Symposium*. IEEE, 2014, pp. 398–410.

[32] R. T. Clemen and R. L. Winkler, "Combining probability distributions from experts in risk analysis," *Risk analysis*, vol. 19, no. 2, pp. 187–203, 1999.

[33] S. Kotz, N. Balakrishnan, and N. L. Johnson, *Continuous multivariate distributions, Volume 1: Models and applications*. John Wiley & Sons, 2004, vol. 1.

APPENDIX

We first state a theorem from [21] which we later use to prove Lemma 2.

Theorem 3. *Let $f_1, \dots, f_k$ be non-negative and Borel measurable functions defined on $\mathbb{R}^n$ and let*

$$r(t) = \sup_{\lambda_1 x_1 + \dots + \lambda_k = t} f_1(x_1) \dots f_k(x_k), \quad t \in \mathbb{R}^n,$$

where $\lambda_1, \dots, \lambda_k$ are positive constants satisfying the equality $\lambda_1 + \dots + \lambda_k = 1$. Then, the function $r(t)$ also Borel measurable and we have the following inequality

$$\int_{\mathbb{R}^n} r(t)dt \geq \left(\int_{\mathbb{R}^n} f_1^{\frac{1}{\lambda_1}} dt \right)^{\lambda_1} \dots \left(\int_{\mathbb{R}^n} f_k^{\frac{1}{\lambda_k}} dt \right)^{\lambda_k}.$$

A. Proof of Lemma 2

We first review the definition of log-concave functions. A function $g : \mathbb{R}^n \mapsto \mathbb{R}$ is said to be log-concave if for all $x_1, x_2 \in \mathbb{R}^n$ and $\theta \in [0,1]$, we have that

$$g(\theta x_1 + (1-\theta)x_2) \geq (g(x_1))^{\theta} (g(x_2))^{1-\theta}.$$

The above condition is equivalent to

$$g(t) \geq \sup_{\theta u + (1-\theta)v = t} g(u)^{\theta} g(v)^{1-\theta}.$$

Note that function g is log-concave if and only if $\log g$ is concave. Next, for $x \in \mathbb{R}^{|W|}$ and $p \in \Delta_{|W|}^{(\eta,\bar{\eta})}$ let $f : \mathbb{R}^{|W|} \times \Delta_{|W|}^{(\eta,\bar{\eta})} \mapsto [0,1]$ be

$$f(x,p) = \frac{\prod_{i \in W} x_i^{kp_i - 1} \left(1 - \sum_{i \in W} x_i\right)^{k(1 - \sum_{i \in W} p_i) - 1}}{B(kp_W)}.$$

For a fixed $p \in \Delta_{|W|}^{\eta,\bar{\eta}}$, let

$$f_1(x) := f(x,p).$$

Function $f_1(x)$ is the Dirichlet probability distribution function with parameter $\alpha \in \mathbb{R}^W$ where $\alpha := kp_W$. Since $p \in \Delta_{|W|}^{\eta,\bar{\eta}}$, we have that $\alpha_i \geq 1$, for all $i \in [|W|]$. Therefore f_1 is a log-concave function [22]. Therefore,

$$f(t_x, p) \geq \sup_{\alpha u_x + (1-\alpha)v_x = t_x} f(u_x,p)^{\alpha} f(v_x,p)^{1-\alpha}, \quad (25)$$

for all $p \in \Delta_{|W|}^{(\eta,\bar{\eta})}$, $t_x, u_x, v_x \in \mathbb{R}^{|W|}$ and $\alpha \in [0,1]$. Similarly, for a fixed $x \in \mathbb{R}^{|W|}$, let

$$f_2(p) := f(x,p).$$

Evaluating the Hessian of $\log f_2(p)$, let

$$\bar{\psi} := \psi^{(0)} \left(k \left(1 - \sum_{i \in [|W|]} x_i \right) \right),$$

where $\psi^{(0)}$ is the digamma function. Then,

$$-\frac{\left(\nabla^2 \log f_2(p)\right)_{i,j}}{k^2} = \begin{cases} \psi^{(0)}(kp_i) + \bar{\psi} & i = j \\ \bar{\psi} & i \neq j \end{cases},$$

The digamma function is strictly increasing on interval $(0, +\infty)$. Therefore, the Hessian matrix is a sum of two negative semi definite matrices and as a result, negative semi definite itself. The aforementioned argument results in log-concavity of $f_2(p)$. Therefore,

$$f(x,t_p) \geq \sup_{\beta u_p + (1-\beta)v_p = t_p} f(x,u_p)^{\beta} f(x,v_p)^{1-\beta}, \quad (26)$$

for all $x \in \mathbb{R}^{|W|}$, $t_p, u_p, v_p \in \Delta_{|W|}^{(\eta,\bar{\eta})}$ and $\beta \in [0,1]$. Let $\lambda \in [0,1]$, choose $\tilde{u_x}, \tilde{v_x}, \tilde{u_p}, \tilde{v_p}$ such that

$$\lambda \tilde{u_x} + (1-\lambda)\tilde{v_x} = t_x,$$
$$\lambda \tilde{u_p} + (1-\lambda)\tilde{v_p} = p.$$

Assigning u_x to x in (26), we find

$$\begin{aligned} f(u_x,p) &\geq \sup_{\beta u_p + (1-\beta)v_p = p} f(u_x,u_p)^{\beta} f(u_x,v_p)^{1-\beta} \\ &\geq f(u_x,\tilde{u_p})^{\lambda} f(u_x,\tilde{v_p})^{1-\lambda}. \end{aligned} \quad (27)$$

Similarly, we can write

$$\begin{aligned} f(v_x,p) &\geq \sup_{\beta u_p + (1-\beta)v_p = p} f(v_x,u_p)^{\beta} f(v_x,v_p)^{1-\beta} \\ &\geq f(v_x,\tilde{u_p})^{\lambda} f(v_x,\tilde{v_p})^{1-\lambda}. \end{aligned} \quad (28)$$

Revisiting (25), using (27) and (28), we can write

$$\begin{aligned} f(t_x,p) &\geq \sup_{\alpha u_x + (1-\alpha)v_x = t_x} f(u_x,p)^{\alpha} f(v_x,p)^{1-\alpha} \\ &\geq \sup_{\lambda \tilde{u_x} + (1-\lambda)\tilde{v_x} = t_x} f(u_x,p)^{\lambda} f(v_x,p)^{1-\lambda} \quad (29) \\ &\geq \sup_{\lambda \tilde{u_x} + (1-\lambda)\tilde{v_x} = t_x} f(u_x,\tilde{u_p})^{\lambda^2} f(u_x,\tilde{v_p})^{\lambda(1-\lambda)} \\ &\quad f(v_x,\tilde{u_p})^{(1-\lambda)\lambda} f(v_x,\tilde{v_p})^{(1-\lambda)^2}. \end{aligned}$$

The second line in (29) is true since we have fixed α and the set of points satisfying the constraints is a subset of one where we are free to adjust α. Note that

$$\begin{aligned} &\lambda \tilde{u_x} + (1-\lambda)\tilde{v_x} = \\ &\quad \lambda^2 \tilde{u_x} + \lambda(1-\lambda)\tilde{u_x} + \lambda(1-\lambda)\tilde{v_x} + (1-\lambda)^2 \tilde{v_x}. \end{aligned}$$

Since $\lambda^2 + \lambda(1-\lambda) + \lambda(1-\lambda) + (1-\lambda)^2 = 1$, Theorem 3 applies. Therefore, we can write

$$\begin{aligned} &\int_{\mathcal{A}} f(t_x,p)dt_x \geq \\ &\quad \left(\int_{\mathcal{A}} f(u_x,\tilde{u_p})du_x \right)^{\lambda^2} \left(\int_{\mathcal{A}} f(u_x,\tilde{v_p})du_x \right)^{\lambda(1-\lambda)} \\ &\quad \left(\int_{\mathcal{A}} f(v_x,\tilde{u_p})dv_x \right)^{(1-\lambda)\lambda} \left(\int_{\mathcal{A}} f(v_x,\tilde{v_p})dv_x \right)^{(1-\lambda)^2}. \end{aligned}$$

By renaming the variables t_x, u_x and v_x to x inside the integrals and merging the similar terms into one, we find

$$\begin{aligned} &\int_{\mathcal{A}} f(x,p)dx \geq \\ &\quad \left(\int_{\mathcal{A}} f(x,\tilde{u_p})dx \right)^{\lambda} \left(\int_{\mathcal{A}} f(x,\tilde{v_p})dx \right)^{(1-\lambda)}, \end{aligned}$$

where $\lambda \tilde{u_p} + (1-\lambda)\tilde{v_p} = p$. Therefore, $\int_{\mathcal{A}} f(x,p)dx$ is log-concave which concludes the promised results. ■

B. Proof of Lemma 3

Let

$$\begin{aligned} c &:= p_i + p_j \\ &= q_i + q_j. \end{aligned}$$

Then using (7), we have that

$$\begin{aligned} \frac{\text{beta}(kp_i, kp_j)}{\text{beta}(kq_i, kq_j)} &= \frac{\Gamma(kq_i)\Gamma(k(c-q_i))}{\Gamma(kp_i)\Gamma(k(c-p_i))} \\ &= \frac{\Gamma(kq_j)\Gamma(k(c-q_j))}{\Gamma(kp_j)\Gamma(k(c-p_j))}. \end{aligned} \tag{30}$$

Using the definition of digamma function, we have

$$\frac{\partial}{\partial x}\left[\frac{\Gamma(x-a)}{\Gamma(x-b)}\right] = \frac{\Gamma(x-a)[\psi^{(0)}(x-a) - \psi^{(0)}(x-b)]}{\Gamma(x-b)}. \tag{31}$$

As the digamma function is strictly increasing on interval $(0, +\infty)$, the derivative in (31) is positive if and only if $x - b < x - a$, which is true if and only if $a < b$. Returning to (30), we will construct an upper bound using the first identity if $q_i < p_i$ and we will construct an upper bound using the second identity if $q_j < p_j$. For correctness, suppose $q_i < p_i$. Then

$$\begin{aligned} \frac{\text{beta}(kp_i, kp_j)}{\text{beta}(kq_i, kq_j)} &= \frac{\Gamma(kq_i)\Gamma(k(c-q_i))}{\Gamma(kp_i)\Gamma(k(c-p_i))} \\ &\leq \frac{\text{beta}(kq_i, k(1-\bar{\eta}-q_j))}{\text{beta}(kp_i, k(1-\bar{\eta}-p_i))}. \end{aligned}$$

The other case will work identically. ■

C. Proof of Lemma 5

From Jensen's inequality we have that

$$\phi\left(\int_a^b f\ dx\right) \leq \int_a^b \phi(f)\ dx,$$

where f is integrable over the domain of interest and ϕ is a convex function. Since the exponential function is convex, we have that

$$\begin{aligned} \text{beta}(a,b) &= \int_0^1 \exp\left(\log\left(x^{a-1}(1-x)^{b-1}\right)\right)dx \\ &\geq \exp\left(\int_0^1 \log\left(x^{a-1}(1-x)^{b-1}\right)dx\right). \end{aligned}$$

Evaluating the integral, we find

$$\exp\left(\int_0^1 \log\left(x^{a-1}(1-x)^{b-1}\right)dx\right) =$$
$$\int_0^1 (a-1)\log(x) + (b-1)\log(1-x)dx = 2 - (a+b).$$

Then

$$\text{beta}(a,b) \geq \exp(2-(a+b)).$$

The upper bound follows from the identity that

$$2\alpha\beta \leq \alpha^2 + \beta^2, \text{ for all } \alpha, \beta \in \mathbb{R}.$$

Substituting α, β with x^{a-1} and y^{b-1} in the integral representation of the beta function results in the introduced upper bound. ■

D. Proof of Proposition 1

Let $\bar{p} = \sum_{r=1}^{n} kp_r$. Using equation (49.9) in [33] we can write

$$\mathbb{E}[x_i] = \frac{kp_i}{\bar{p}} = p_i,$$

and

$$\text{Var}[x_i] = \frac{kp_i(\bar{p} - kp_i)}{\bar{p}^2(\bar{p}+1)}.$$

Since input p belongs to the unit simplex, we have that $\bar{p} = k$. Substituting $\bar{p}$ with k concludes the promised results. ■