Distribution Privacy Under Function Recoverability

Ajaykrishnan Nageswaran and Prakash Narayan

Abstract—A user generates \( n \) independent and identically distributed data random variables with a probability mass function that must be guarded from a querier. The querier must recover, with a prescribed accuracy, a given function of the data from each of \( n \) independent and identically distributed user-devised query responses. The user chooses the data pmf and the random query responses to maximize distribution privacy as gauged by the divergence between the pmf and the querier’s best estimate of it based on the \( n \) query responses. A general lower bound is provided for distribution privacy; and, for the case of binary-valued functions, upper and lower bounds that converge to said bound as \( n \) grows. Explicit strategies for the user and querier are identified.

Index Terms—Distribution privacy, divergence, query response, binary pmf, binary query response, smooth estimator

I. INTRODUCTION

A legitimate user generates data represented by independent and identically distributed (i.i.d.) finite-valued random variables (rvs). The user selects the probability mass function (pmf) of the data and seeks to guard it from a querier. The querier wishes to compute a given function of the data from user-provided i.i.d. query responses that are suitably randomized versions of the data. The user devises the query responses so as to allow the querier to recover the function value from every query response with a prescribed accuracy, while maximizing privacy of the data pmf. Distribution privacy is assessed by the (Kullback-Leibler) divergence between the data pmf and the querier’s best estimate of it.

In our formulation, the user selects the data pmf \( P_X \) and produces i.i.d. query responses according to a stochastic matrix \( W \) such that the querier can recover the function value with probability at least \( \rho \), \( 0 \leq \rho \leq 1 \), from each query response. The querier chooses an estimator \( F_n \) for the pmf \( P_X \) based on the query responses. In our new notion of distribution \( \rho \)-privacy for \( n \) query responses, the divergence between \( P_X \) and the querier’s estimate of it is maximized and minimized respectively with respect to \( (W, P_X) \) and \( F_n \). The order of optimization allows \( F_n \) to depend on \( W \) and \( P_X \) on \( F_n \). Our contributions are as follows. We first provide an asymptotic (in \( n \)) lower bound for distribution \( \rho \)-privacy. Considering the specific case of binary-valued functions, we provide upper (converse) and lower (achievability) bounds for every \( n \). These bounds are shown to be asymptotically tight, converging to said asymptotic lower bound. The achievability proof entails specific strategies for the user and the querier.

An extensive body of work exists on distribution estimation in the context of data privacy (cf. e.g., [7], [8], [4], [9], [1] and references therein). Two lines of work are pertinent. In a series [6], [10], [15], [14], samples of user data are generated according to a probability distribution from a given family of distributions. A randomized version of each of the samples is made available to a querier, with the randomization mechanism being differentially private of a given privacy level. The querier then forms an estimate of the user’s distribution based on the differentially private query responses. Considering the minmax of the expected \( f_2 \)-distance between the user’s distribution and the querier’s estimate (maximum and minimum, respectively, over possible user distributions and estimators), its minimum is examined, over all the differentially private randomization mechanisms of the given level. In another line of work [5], [12], [2], [3], [13], sans privacy considerations but relevant to ours, data samples are generated according to a distribution from a given set. Viewed through our lens the objective can be interpreted as the user selecting a distribution that resists estimation by the best estimator under a divergence cost. Accordingly, the maximum and minimum, respectively, over user distributions and estimators of the expected divergence between user distribution and estimate, is investigated. Also, see [11] for a similar minmax study under other loss measures.

II. PRELIMINARIES

A user generates data represented by i.i.d. rvs \( X_1, \ldots, X_n, n \geq 1 \), with \( X_1 \) taking values in a finite set \( \mathcal{X} \) of cardinality \( |\mathcal{X}| = r \geq 2 \), and with pmf \( P_X \). Consider a given mapping \( f : \mathcal{X} \rightarrow \mathcal{Z} = \{0, 1, \ldots, k-1\}, 2 \leq k \leq r \). For realizations \( X_1 = x_1, \ldots, X_n = x_n \), a querier – who does not know \( x_1, \ldots, x_n \) or \( P_X \) – wishes to compute \( f(x_1), \ldots, f(x_n) \) from \( \mathcal{Z} \)-valued rvs \( Z_1, \ldots, Z_n \), termed query responses (QRs), that are provided by the user. Each QR \( Z_t, t = 1, \ldots, n \), must satisfy the following recoverability condition.

Definition 1. Given \( 0 \leq \rho \leq 1 \), a QR \( Z_t \) is \( \rho \)-recoverable (\( \rho \)-QR) if

\[
P(Z_t = f(x)|X_t = x) \geq \rho, \ x \in \mathcal{X}.
\]

Condition (1) can be written equivalently in terms of a stochastic matrix \( W : \mathcal{X} \rightarrow \mathcal{Z} \) with the requirement

\[
W(f(x)|x) \geq \rho, \ x \in \mathcal{X}
\]

which too will be termed a \( \rho \)-QR. Note that \( \rho \)-recoverability in (1), (2) does not depend on \( P_X \).
The $\rho$-QRs $Z_1, \ldots, Z_n$ are assumed to satisfy
\[ P(Z^n = z^n|X^n = x^n) = P(Z_1 = z_1, \ldots, Z_n = z_n|X_1 = x_1, \ldots, X_n = x_n) \]
\[ = \prod_{t=1}^n P(Z_t = z_t|X_t = x_t) \]
\[ = \prod_{t=1}^n W(z_t|x_t), \quad x^n \in X^n, z^n \in Z^n. \]

The user chooses the pmf $P_X$ and the $\rho$-QRs $Z_1, \ldots, Z_n$ or equivalently $W$. The querier observes $Z_1, \ldots, Z_n$ and seeks to estimate $P_X$ by means of an estimator $\hat{P}_n : Z^n \rightarrow \Delta_r$ with $\Delta_r$ being the $(r-1)$-dimensional simplex associated with $X$.

Our measure of discrepancy between the pmf $P_X$ and the querier’s estimate $\hat{P}_n$ is
\[ \pi_n(\rho, W, \hat{P}_n, P_X) \triangleq \mathbb{E} \left[ D \left( P_X || \hat{P}_n (Z^n) \right) \right] \] (3)
where the expectation is with respect to the pmf $P_X W$ and $\hat{P}_n$, respectively, to maximize and minimize $\pi_n(\rho, W, \hat{P}_n, P_X)$. Our notion of distribution privacy assumes conservatively that the querier is cognizant of the user’s choice of the randomized privacy mechanism $W$ which depends on $0 \leq \rho \leq 1$.

**Definition 2.** For $0 \leq \rho \leq 1$, distribution $\rho$-privacy is
\[ \pi_n(\rho) \triangleq \sup_{W: W(f(x)|z) \geq \rho} \inf_{\hat{P}_n: \Delta_r \rightarrow P_X} \sup_{P_X \in \Delta_r} \pi_n(\rho, W, \hat{P}_n, P_X), \quad n \geq 1 \] (4)
where $W$ is as in (2) and $\pi_n(\rho, W, \hat{P}_n, P_X)$ is given by (3).

**Remarks:**
(i) The order of maximization and minimization in (4) accommodates the dependence of $\hat{P}_n$ on $W$ in providing a conservative measure of distribution privacy. On the other hand, privacy, if gauged by inf sup sup in (4), would be larger, in general, but would not allow the querier to be aware of the privacy mechanism $W$.
(ii) We note that $\pi_n(\rho)$ in (4), if defined instead in terms of sup sup inf, would equal zero. Also, reversing the roles of $P_X W$ and $\hat{P}_n$ in $D(\cdot||\cdot)$ in (3) leads to $\pi_n(\rho) = \infty$.
(iii) Clearly, it suffices to restrict the querier’s estimators $\hat{P}_n$ in (4) to those that satisfy $\hat{P}_n(z^n) > 0$, $z^n \in Z^n$, $x \in X$; else $\pi_n(\rho) = \infty$.

For a given $n$-type $Q^{(n)}$ on $Z$, let $T_{Q^{(n)}}$ be the set of all sequences in $Z^n$ of type $Q^{(n)}$. Let $Q^{(n)}$ be the set of all $n$-types on $Z$. A convenient representation $\pi_n(\rho)$ in (4) is provided below and it shows that it is adequate to consider querier estimators $\hat{P}_n : Q^{(n)} \rightarrow \Delta_r$ that are based on the type $Q^{(n)}$ of $i^n$ in $Z^n$, with the former serving as a sufficient statistic for the latter.

**Lemma 1.** For $0 \leq \rho \leq 1$,
\[ \pi_n(\rho) = \sup W \inf P_n \sup \sum_{Q^{(n)} \in \mathcal{T}_{Q^{(n)}}} (P_X W)^n (T_{Q^{(n)}}) D \left( P_X || \hat{P}_n \left( Q^{(n)} \right) \right) \] (5)
with $\hat{P}_n(Q^{(n)})$ representing identical estimates for all $i^n \in T_{Q^{(n)}}$.

**Corollary:** For $Z = \{0, 1\}$,
\[ \pi_n(\rho) = \sup W \inf P_n \sup \sum_{i^n = 0}^n P \left( \text{Bin}(n, (P_X W)(1)) = i \right) D \left( P_X || \hat{P}_n(i) \right) \] with $\hat{P}_n(i)$ representing identical estimates for all $i^n \in \{0, 1\}^n$ with $\sum i_t = i$.

**Proof:** Observe that for fixed $W, \hat{P}_n, P$,
\[ \pi_n(\rho, W, \hat{P}_n, P_X) = \sum_{Q^{(n)} \in \mathcal{T}_{Q^{(n)}} \cap \mathcal{Q}(n)} (P_X W)^n (i^n) D \left( P_X || \hat{P}_n \left( i^n \right) \right). \] (6)
For a fixed $Q^{(n)}$, since $(P_X W)^n(i^n)$ is the same for all $i^n \in \mathcal{T}_{Q^{(n)}}$, if $\hat{P}_n(i^n)$ were to vary across $i^n \in \mathcal{T}_{Q^{(n)}}$, we can pick that $\hat{i}^n$, say, in $\mathcal{T}_{Q^{(n)}}$ for which $D \left( P_X || \hat{P}_n \left( i^n \right) \right)$ is smallest over $\mathcal{T}_{Q^{(n)}}$ and use $\hat{P}_n(\hat{i}^n)$ as the estimate of $P_X$ for all $i^n \in \mathcal{T}_{Q^{(n)}}$, denoting it $\hat{P}_n(Q^{(n)})$; this will only serve to decrease the right-side of (6), bearing in mind the inf with respect to $\hat{P}_n$ in the left-side of (5). Then the right-side of (6) becomes
\[ \sum_{Q^{(n)} \in \mathcal{T}_{Q^{(n)}} \cap \mathcal{Q}(n)} (P_X W)^n (T_{Q^{(n)}}) D \left( P_X || \hat{P}_n \left( Q^{(n)} \right) \right) \]
leading to (5).

The Corollary follows readily.

For $P_X \in \Delta_r$, denote a derived pmf $P_X (f^{-1}) \triangleq (P_X (f^{-1}(0)), P_X (f^{-1}(1)), \ldots, P_X (f^{-1}(k-1)))$.

We close this section with a preliminary characterization of $\pi_n(\rho)$ for low values of $\rho$ and a lower bound for it that does not depend on $\rho$ or $n$.

**Theorem 2.** For each $n \geq 1$, $\pi_n(\rho)$ is nonincreasing in $0 \leq \rho \leq 1$ with
\[ \pi_n(\rho) \begin{cases} = \log r, & 0 \leq \rho \leq 1/k, \\ \geq \max_{j \in \mathbb{Z}} \log \left| f^{-1}(j) \right|, & 0 \leq \rho \leq 1. \end{cases} \] (7) (8)

**Remark:** For the special case of a binary-valued mapping $f$ (in Section IV below), in the interesting regime $0.5 < \rho \leq 1$, the lower bound in (8) possesses the significance of being the asymptotic limit (in $n$) of $\pi_n(\rho)$. See Theorem 3.
**Proof:** For each \( n \), the monotonicity of \( \pi_n(\rho) \) in \( 0 \leq \rho \leq 1 \) is obvious. To show (7), upon choosing \( \hat{P}_n(i^n)(x) = 1/r, x \in \mathcal{X}, \ i^n \in \mathcal{Z} \), we get

\[
\pi_n(\rho) \leq \sup_{W} \sup_{P_X} \frac{1}{k^n} \sum_{i^n \in \mathcal{Z}^n} D \left( P_X \| \hat{P}_n(i^n) \right) = \log r \inf_{P_X} H(P_X) = \log r.
\]  

(9)

For \( 0 \leq \rho \leq 1/k \), choose \( W(j|x) = 1/k, x \in \mathcal{X}, \ j \in \mathcal{Z} \). Then, for every \( P_X \in \Delta_r \), \( P_XW \) is the uniform pmf on \( \mathcal{Z} \). Hence,

\[
\pi_n(\rho) \geq \inf_{P_X} \sup_{P_X} \frac{1}{k^n} \sum_{i^n \in \mathcal{Z}^n} D \left( P_X \| \hat{P}_n(i^n) \right)
\]

\[
\geq \inf_{P_X} \sup_{P_X} D \left( P_X \| \frac{1}{k^n} \sum_{i^n \in \mathcal{Z}^n} \hat{P}_n(i^n) \right),
\]

by the convexity of \( D(\cdot||\cdot) \)

\[
\geq \inf_{R \in \Delta_r} \sup_{P_X} D \left( P_X \| R \right) = \log r
\]

(10)

and is attained by \( P_X \) being any point mass on \( \mathcal{X} \) and \( R \) the uniform pmf on \( \mathcal{X} \). From (9) and (10), (7) follows.

Turning to (8), we note that

\[
\pi_n(\rho) \geq \pi_n(1), \ 0 \leq \rho \leq 1
\]

and \( \rho = 1 \) means that

\[
W(j|x) = 1 \ (j = f(x)), \ x \in \mathcal{X}, \ j \in \mathcal{Z},
\]

and so \( P_XW = P_X(f^{-1}), \ i.e., (P_XW)(j) = P_X(f^{-1}(j)), \ j \in \mathcal{Z}. \) Since, sup can be expressed as

\[
\sup_{\alpha=(\alpha_0, \alpha_1, ..., \alpha_{k-1})} \sup_{P_X} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

\[
= \inf_{\alpha} \sup_{\alpha \in \Delta_k} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

\[
\geq \sup_{\alpha \in \Delta_k} \inf_{\alpha} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

\[
\geq \sup_{\alpha \in \Delta_k} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

\[
\geq \sup_{\alpha \in \Delta_k} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

Next, for fixed \( \alpha = (\alpha_0, \alpha_1, ..., \alpha_{k-1}) \) and \( R \) in (11), \( D(\cdot||R) \) is maximized by \( P_X \) with probability \( \alpha_j \) on the lowest \( R \)-probability symbol in \( f^{-1}(j), \ j \in \mathcal{Z} \). Accordingly, the pmf \( R \) that maximizes said lowest probabilities (without knowledge of \( P_X \)), and thereby minimizes \( D(\cdot||R) \), assigns “locally uniform” pmfs to \( f^{-1}(j), \ j \in \mathcal{Z} \), i.e.,

\[
R(x) = \frac{\beta_j}{\left| f^{-1}(j) \right|}, \ x \in f^{-1}(j), \ j \in \mathcal{Z}
\]

for some \( \beta = (\beta_0, \beta_1, ..., \beta_{k-1}) \in \Delta_k \). Hence, in (11), for fixed \( \alpha \in \Delta_k \),

\[
\inf_{\alpha \in \Delta_k} \sup_{P_X} \left[ D \left( P_X \| \hat{P}_n(Z^n) \right) \right]
\]

\[
= \inf_{\alpha \in \Delta_k} \sum_{j \in \mathcal{Z}} \alpha_j \log \frac{\alpha_j}{|f^{-1}(j)|}
\]

\[
= \inf_{\beta \in \Delta_k} \sum_{j \in \mathcal{Z}} \alpha_j \log \left| f^{-1}(j) \right| + D(\alpha||\beta)
\]

(12)

and is attained by \( \beta = \alpha \). Finally, by (11), (12),

\[
\pi_n(\rho) = \sup_{\alpha \in \Delta_k} \sum_{j \in \mathcal{Z}} \alpha_j \log \left| f^{-1}(j) \right| = \max_{j \in \mathcal{Z}} \log \left| f^{-1}(j) \right|
\]

III. Main Result

Hereafter, we restrict ourselves to the case \( f : \mathcal{X} \to \mathcal{Z} = \{0, 1\} \). Recalling the Corollary to Lemma 1, among the querier’s estimators \( \hat{P}_n : \{0, 1, ..., n\} \to \Delta_r, n \geq 1 \), pertinent to our converse and achievability proofs for \( \pi_n(\rho) \), respectively, will be classes of “locally uniform estimators” and “smooth estimators.” Furthermore, from the user’s standpoint “binary pmfs \( P_X^b \)” and “binary \( \rho \)-QRs \( W^b \)” are pertinent in the converse proof.

**Definition 3.** (i) For \( n \geq 1 \) and \( \beta^{(n)} = (\beta_0, \beta_1, ..., \beta_n) \), \( 0 \leq \beta_i \leq 1, \ 0 \leq i \leq n \), a locally uniform estimator \( \hat{P}_n \) : \( \{0, 1, ..., n\} \to \Delta_r \) is defined by

\[
\hat{P}_n^{\beta^{(n)}(i)}(x) = \begin{cases} \frac{x}{f^{-1}(1)} & x \in f^{-1}(1) \\ \frac{x}{f^{-1}(0)} & x \in f^{-1}(0) \end{cases}
\]

(ii) A smooth estimator \( \hat{P}_n : \{0, 1, ..., n\} \to \Delta_r, n \geq 1 \), is such that for some \( \gamma_n \) and \( \tilde{\gamma}_n = \gamma_n \), with \( \gamma_n = 0 \), \( \lim_n \tilde{\gamma}_n = 0, \) \( \lim_n \gamma_n = 0 \), \( \lim_n \gamma_n = 0 \) it holds that whenever \( i \neq i' \) with \( |i - i'| \leq \gamma_n \), \( \var|\hat{P}_n(i), \hat{P}_n(i')| \leq \tilde{\gamma}_n \) where \( \var|\cdot, \cdot| \) denotes variational distance, and \( \hat{P}_n(i)(x) \geq c\gamma_n, \ x \in \mathcal{X}, \ 0 \leq i \leq n, \ c > 0. \) Denote the class of all such estimators by \( \mathcal{S}_n, n \geq 1 \).

Remarks: A smooth estimator has the feature that neighboring QRs lead to proximate pmf estimates by the querier. Its second feature is motivated by Remark (iii) following Definition 2.

**Definition 4.** (i) A binary pmf \( P_X^b \) on \( \mathcal{X} \) is defined by

\[
P_X^b(x) = \begin{cases} \alpha, & for some x \in f^{-1}(1) \\ 1 - \alpha, & for some x \in f^{-1}(0) \end{cases}
\]

for some \( 0 \leq \alpha \leq 1 \).

(ii) A binary \( \rho \)-QR \( W^b : \mathcal{X} \to \{0, 1\} \) is of the form

\[
W^b(x) = \begin{cases} (\rho_1, 1 - \rho_1), & x \in f^{-1}(1) \\ (1 - \rho_0, \rho_0), & x \in f^{-1}(0) \end{cases}
\]

for some \( \rho_0, \rho_1 \) with \( \rho \leq \rho_0, \rho_1 \leq 1 \).

Our main result is
Theorem 3. For every $n \geq 1$, 

(i) $\pi_n(\rho) = \log r$ for $0 \leq \rho \leq 0.5$;

(ii) $\pi_n(\rho) \leq \max_{j \in \{0, 1\}} \log |f^{-1}(j)| + \Gamma_n(\rho)$, $0.5 < \rho \leq 1$, where

$$
\Gamma_n(\rho) \triangleq \sup_{\rho \leq \rho_0, \rho_1 \leq 1} \sup_{1 - \rho_0 \leq \alpha \leq \rho_1} E \left[ D \left( \operatorname{Ber} \left( \frac{\alpha - (1 - \rho_0)}{\rho_0 + \rho_1 - 1} \right) \bigg| \operatorname{Ber} \left( \sum_{i=1}^{n} z_i \right) \right) \right]
$$

with $\beta_i$, $0 \leq i \leq n$ given by

$$
\beta_i = \begin{cases} 
\frac{\lfloor n(1-\rho_0) \rfloor + 1}{n+1}, & \frac{i}{n} < 1 - \rho_0 \\
\frac{\lfloor n(1-\rho_1) \rfloor + 1}{n+1}, & 1 - \rho_0 \leq \frac{i}{n} \leq \rho_1 \\
\frac{\lfloor n(1-\rho_0) \rfloor + 1}{n+1}, & \frac{i}{n} > \rho_1.
\end{cases}
$$

(iii) for the class of smooth estimators

$$
\pi_n(\rho) = \sup_{W} \inf_{P_{\rho} \in S_{\rho}} \sup_{P_X} \pi_n \left( \rho, W, \hat{P}_{n}, P_X \right)
\geq \left( \max_{j \in \{0, 1\}} \log |f^{-1}(j)| + \Lambda_n(\rho) - \frac{\hat{\gamma}_n}{\sqrt{\log n}} \right) \left( 1 - \frac{2}{n} \right),
$$

where

$$
\Lambda_n(\rho) \triangleq \begin{cases} 
\log \left( 1 + \frac{|f^{-1}(0)|}{|f^{-1}(1)|} \frac{1}{(2\rho - 1) \epsilon} \left( \rho - \frac{|n\rho|}{n} \right) \right), & \rho \leq \frac{|n\rho|}{n} \\
\log \left( 1 + \frac{|f^{-1}(1)|}{|f^{-1}(0)|} \frac{1}{(2\rho - 1) \epsilon} \left( \frac{|n(1-\rho)|}{n} - (1 - \rho) \right) \right), & |f^{-1}(1)| > |f^{-1}(0)|
\end{cases},
$$

with equality iff $P$ is a two-point mass with

$$
P(x') = P(A) \text{ for some } x' \in A, \\
P(x''') = P(A^c) \text{ for some } x'' \in A^c.
$$

Proof: The proof is a straightforward exercise.

First we show that when the querier uses a locally uniform estimator, the user’s choice can be limited to binary pmfs and binary $\rho$-QRs without loss of distribution privacy.

Lemma 5. For every $n \geq 1$ and $\beta^{(n)}$,

$$
\sup_{W} \inf_{P_{\beta^{(n)}}} \sup_{P_X} \pi_n \left( \rho, W, \hat{P}_{n}^{\beta^{(n)}}, P_X \right) = \sup_{W} \inf_{P_{\beta^{(n)}}} \sup_{P_X} \pi_n \left( \rho, W^{b}, \hat{P}_{n}^{\beta^{(n)}}, P_X^{b} \right).
$$

Idea of proof: Since the suprema in the right-side of (14) are over restricted sets, it suffices to show that (14) holds with “$\leq$.” Specifically, we show that for every $P_X$ and $W$, there exist $P_X^{b}$ and $W^{b}$ such that

$$
\pi_n \left( \rho, W, \hat{P}_{n}^{\beta^{(n)}}, P_X \right) \leq \pi_n \left( \rho, W^{b}, \hat{P}_{n}^{\beta^{(n)}}, P_X^{b} \right).
$$

Turning to Theorem 3 (ii), note by (4) that upon restricting the querier’s choice to locally uniform estimators and using Lemma 5

$$
\pi_n(\rho) \leq \sup_{W} \inf_{P_{\rho} \in S_{\rho}} \sup_{P_X} \pi_n \left( \rho, W^{b}, \hat{P}_{n}^{\beta^{(n)}}, P_X^{b} \right).
$$

For fixed $W^{b}$, $\hat{P}_{n}^{\beta^{(n)}}$ and $P_X^{b}$

$$
\alpha = (P_X^{b} W^{b}) (1) = P_X^{b} (f^{-1}(1)) \rho_1 + P_X^{b} (f^{-1}(0)) \times (1 - \rho_0) = P_X^{b} (f^{-1}(1)) \rho_0 + P_X^{b} (f^{-1}(0)) + (1 - \rho_0)
$$

for some $\rho \leq \rho_0, \rho_1 \leq 1$. Observe by (16) that $1 - \rho_0 \leq \alpha \leq \rho_1$. Then,

$$
\pi_n \left( \rho, W^{b}, \hat{P}_{n}^{\beta^{(n)}}, P_X^{b} \right) = \sum_{i=0}^{n} P(Bin(n, \alpha) = i) D \left( P_X^{b} \bigg| \hat{P}_{n}^{\beta^{(n)}} (i) \right) + P_X^{b} (f^{-1}(1)) \log |f^{-1}(1)| + P_X^{b} (f^{-1}(0)) \log |f^{-1}(0)|
$$

by Lemma 4. Next, note from (16) that

$$
P_X^{b} (f^{-1}(1)) = \frac{(P_X^{b} W^{b}) (1) - (1 - \rho_0)}{\rho_1 - (1 - \rho_0)}
$$

893
Then from (17) and (18),
\[
\pi_n(\rho, W^b, \tilde{P}_n^{\beta(n)}, P_X) \leq \max_{j \in \{0,1\}} \log |f^{-1}(j)| + \sum_{i=0}^{n} P(\text{Bin}(n, \alpha) = i) \times D\left(\text{Ber}\left(\frac{\alpha - (1 - \rho_0)}{\rho_0 + \rho_1 - 1}\right) \left|\text{Ber}(\beta_i)\right.\right).
\] (19)

Hence, in (15) upon using (17)-(19),
\[
\pi_n(\rho) \leq \max_{j \in \{0,1\}} \log |f^{-1}(j)| + \sup_{\rho \leq \rho_0, \rho_1 \leq 1} \inf_{1 - \rho_0 \leq \alpha \leq \rho_1} \sum_{i=0}^{n} P(\text{Bin}(n, \alpha) = i) \times D\left(\text{Ber}\left(\frac{\alpha - (1 - \rho_0)}{\rho_0 + \rho_1 - 1}\right) \left|\text{Ber}(\beta_i)\right.\right).
\] (20)

The right-side of (20) is bounded above further by choosing
\[
\beta_i = \begin{cases} \frac{\lfloor (n(1 - \rho_0) + 1)(1 - \rho_0) \rfloor}{\rho_0 + \rho_1 - 1}, & \frac{1}{n} < 1 - \rho_0 \\ \frac{1}{n} - \frac{1}{\rho_0 + \rho_1 - 1}, & 1 - \rho_0 \leq \frac{1}{n} \leq \rho_1 \\ \frac{\lfloor (n(1 - \rho_0) + 1)(1 - \rho_0) \rfloor}{\rho_0 + \rho_1 - 1}, & \frac{1}{n} > \rho_1. \end{cases}
\] (21)

This choice is motivated upon the querier using the first terms in the numerator of \(\beta_i\) above as appropriate estimates of \(\alpha = (P_X W^b)(1)\). Combining (20) and (21), we obtain
\[
\pi_n(\rho) \leq \max_{j \in \{0,1\}} \log |f^{-1}(j)| + \Gamma_n(\rho),
\]
where
\[
\Gamma_n(\rho) \triangleq \sup_{\rho \leq \rho_0, \rho_1 \leq 1} \sup_{1 - \rho_0 \leq \alpha \leq \rho_1} \mathbb{E}
\left[ D\left(\text{Ber}\left(\frac{\alpha - (1 - \rho_0)}{\rho_0 + \rho_1 - 1}\right) \left|\text{Ber}(\beta_n \sum_{i=1}^{n} Z_i)\right.\right) \right]
\]
for \(\beta_n \sum_{i=1}^{n} Z_i\) in (21), noting that \(\sum_{i=1}^{n} Z_i \sim \text{Bin}(n, \alpha)\). A last step entails showing that \(\lim_{n} \Gamma_n(\rho) = 0\) for \(\rho > 0.5\).

\[\]

**III-B. Proof of Theorem 3 (iii)**

The following technical lemma, whose straightforward proof is omitted, is relevant.

**Lemma 6.** Consider pmfs \(P, Q, Q_o\) on \(X\) such that \(\text{support}(P) \subseteq \text{support}(Q) \subseteq \text{support}(Q_o)\). Then
\[
D(P \parallel Q) \geq D(P \parallel Q_o) - \frac{\text{var}(Q_o)}{Q_o^{\min}}
\]
where \(Q_o^{\min}\) is the smallest nonzero value of \(Q_o\).

The user selects \(P_X\) and \(\rho\)-QR \(W^b: X \to \{0,1\}\) defined by \(W^b_{\rho}(j|x) = \rho, \ x \in f^{-1}(j), \ j \in \{0,1\}\). Correspondingly, for the querier’s choice of any smooth estimator \(\tilde{P}_n \in S_n\), by the Corollary to Lemma 1,
\[
\pi_n(\rho, W^b, \tilde{P}_n, P_X) = \sum_{i=0}^{n} P(\text{Bin}(n, \alpha) = i) \times D\left(P_X \parallel \tilde{P}_n(i)\right)
\]
with \(\alpha = (P_X W^b)(1)\) and
\[
(P_X W^b)(1) = \sum_{x \in f^{-1}(0)} P_X(x)(1 - \rho) + \sum_{x \in f^{-1}(1)} P_X(x)\rho = P_X(f^{-1}(0))(1 - \rho) + P_X(f^{-1}(1))\rho,
\]
where \(1 - \rho \leq \alpha \leq \rho\). Then,
\[
\pi_n(\rho) \geq \sup_{\tilde{P}_n \in S_n} \inf_{1 - \rho_0 \leq \alpha \leq \rho_1} \sum_{i=0}^{n} P(\text{Bin}(n, \alpha) = i) \times D\left(P_X \parallel \tilde{P}_n(i)\right)
\]
\[
\geq \sup_{\tilde{P}_n \in S_n} \inf_{1 - \rho_0 \leq \alpha \leq \rho_1} \sum_{i=0}^{n} P(\text{Bin}(n, \alpha) = i) \times D\left(P_X \parallel \tilde{P}_n(i)\right)
\]
where \(\gamma_n, n \geq 1,\) is chosen to satisfy
\[
\lim_{n} \gamma_n = 0, \ \lim n\gamma_n^2 = \infty.
\]
Since \(\tilde{P}_n\) is a smooth estimator (cf. Definition 3 (ii)), \(|i/n - \alpha| \leq \gamma_n\) implies \(\text{var}(\tilde{P}_n(i), \tilde{P}_n(\lfloor n\alpha \rfloor)) \leq \gamma_n\) where \(\gamma_n(\gamma_n) \to 0\) as \(\gamma_n \to 0\). Accordingly, by Lemma 6,
\[
D\left(P_X \parallel \tilde{P}_n(i)\right) \geq D\left(P_X \parallel \tilde{P}_n(\lfloor n\alpha \rfloor)\right) - \frac{\gamma_n}{n\gamma_n^2}
\]
\[
\geq D\left(P_X \parallel \tilde{P}_n(\lfloor n\alpha \rfloor)\right) - \frac{\gamma_n}{c_n^2\gamma_n}
\]
Also, by Hoeffding’s inequality, for every \(n\),
\[
P(\lfloor n\alpha \rfloor - n\alpha \geq n\gamma_n^2) \leq 2e^{-2n\gamma_n^2},
\]
Then, in (22),
\[
\pi_n(\rho) \geq \inf_{\tilde{P}_n \in S_n} \sup_{1 - \rho_0 \leq \alpha \leq \rho_1} \sup_{P_X(\text{Bin}(n, \alpha)) = \alpha} \left[ D\left(P_X \parallel \tilde{P}_n(\lfloor n\alpha \rfloor)\right) - \frac{\gamma_n}{c_n^2\gamma_n} \right] (1 - 2e^{-2n\gamma_n^2}).
\] (23)

The key step hereafter shows that a binary pmf \(P_X^b\) and a locally uniform estimator \(\tilde{P}_n\) attain the extrema in (23). Consequent separate but similar calculations for the cases \(|f^{-1}(1)| \geq |f^{-1}(0)|\) and \(|f^{-1}(1)| < |f^{-1}(0)|\), details of which are omitted, lead to (13).

**REFERENCES**

[1] R. Bassily and A. Smith, “Local, private, efficient protocols for succinct histograms,” in ACM Symposium on Theory of Computing, June 2015.
[2] D. Braess, J. Forster, T. Sauer, and H.U. Simon, “How to achieve minimax expected Kullback-Leibler distance from an unknown finite distribution,” in International Conference on Algorithmic Learning Theory, pp. 380-394, 2002.
[3] D. Braess and T. Sauer, “Bernstein polynomials and learning theory,” in Journal of Approximation Theory, pp. 187-206, 2004.
[4] T. H. Chan, M. Li, E. Shi, and W. Xu, “Differentially private continual monitoring of heavy hitters from distributed streams,” in Privacy Enhancing Technologies, pp. 140–159, Springer, 2012.
[5] T.M. Cover, “Admissibility properties of Gilbert’s encoding for unknown source probabilities,” in IEEE Transactions on Information Theory, pp. 216-217, Jan 1972.
[6] J. C. Duchi, M. I. Jordan and M. J. Wainwright, “Minimax optimal procedures for locally private estimation,” in Journal of the American Statistical Association, pp. 182-201, May 2018.
[7] G. T. Duncan and D. Lambert, “Disclosure-limited data dissemination,” in Journal of the American Statistical Association, 1986.
[8] S. E. Fienberg, U. E. Makov and R. J. Steele, “Disclosure limitation using perturbation and related methods for categorical data,” in Journal of Official Statistics, 1998.
[9] J. Hsu, S. Khanna and A. Roth, “Distributed private heavy hitters,” in Automata, Languages, and Programming, pp. 461-472, 2012.
[10] P. Kairouz, K. Bonawitz and D. Ramage, “Discrete distribution estimation under local privacy,” in International Conference on Machine Learning, pp. 2436-2444, June 2016.
[11] S. Kamath, A. Orlitsky, V. Pichapati, and A. T. Suresh, “On learning distributions from their samples,” in Conference on Learning Theory, pp. 1066-1100, 2015.
[12] R.E. Krichevsky, “The performance of universal encoding,” in IEEE Transactions on Information Theory, pp. 296-303, Jan 1998.
[13] L. Paninski, “Variational minimax estimation of discrete distributions under KL loss,” In Neural Information Processing Systems, 2004.
[14] A. Pastore and M. Gastpar, “Locally differentially-private randomized response for discrete distribution learning,” in Journal on Machine Learning Research, Nov 2018.
[15] M. Ye and A. Barg, “Optimal schemes for discrete distribution estimation under locally differential privacy,” in IEEE Transactions on Information Theory, pp. 5662-5676, Feb 2018.