Distribution Privacy Under Function Recoverability

Ajaykrishnan Nageswaran and Prakash Narayan, *Life Fellow, IEEE*

***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 query responses upon eliciting them from the user. The user chooses the data probability mass function and devises the random query responses to maximize distribution privacy as gauged by the (Kullback-Leibler) divergence between the former and the querier's best estimate of it based on the n query responses. Considering an arbitrary function, a basic achievable lower bound for distribution privacy is provided that does not depend on n and corresponds to worst-case privacy. Worst-case privacy equals the logsum cardinalities of inverse atoms under the given function, with the number of summands decreasing as the querier recovers the function with improving accuracy. Next, upper (converse) and lower (achievability) bounds for distribution privacy, dependent on n, are developed. The former improves upon worst-case privacy and the latter does so under suitable assumptions; both converge to it as n grows. The converse and achievability proofs identify explicit strategies for the user and the querier.**

***Index Terms*—Distribution privacy, divergence, local differential privacy, locally identical query response, locally uniform estimator, smooth estimator, sparse pmf, worst-case privacy.**

I. Introduction

A USER generates data represented by independent and identically distributed (i.i.d.) repetitions of a finite-valued random variable (rv) with an underlying probability mass function (pmf) that the user selects and seeks to keep private from a querier who wishes to compute a given function of the data. For this purpose, the querier elicits 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.

Specifically, the user chooses a data pmf P_X of the rv X and produces $n \geq 1$ i.i.d.[1] query responses as the outputs of a stochastic matrix W, with inputs being n i.i.d. repetitions of X, such that the querier can recover the function value from each query response with probability at least ρ, $0 \leq \rho \leq 1$. The querier picks an estimator $\widehat{P}_n$ for the pmf P_X based on the n query responses. Our notion of *distribution ρ-privacy for n query responses* entails the (Kullback-Leibler) divergence between P_X and the querier's estimate of it being maximized and minimized, respectively, with respect to (W, P_X) and $\widehat{P}_n$. The order of optimization allows $\widehat{P}_n$ to depend on W, and P_X on $\widehat{P}_n$. This setting can be viewed also as that with n queriers to each of whom the user provides a query response from which the function value can be recovered with probability not less than ρ; the queriers then cooperate to estimate P_X from their pooled n i.i.d. query responses.

A suggestive interpretation of distribution ρ-privacy entails Nature generating its secrets according to a pmf $P_X = P_X^*$, say, that is hardest for a mortal querier to fathom under the function recoverability requirement above. On account of the continuity of $D\left(P_X \middle\| \widehat{P}_n\right)$ with respect to $\left(P_X, \widehat{P}_n\right)$ when the support of P_X is contained in that of $\widehat{P}_n$, a user – constrained unlike Nature – chooses a feasible P_X that is proximate to P_X^*. Potential futuristic applications include: an AI-driven financial trader who reveals trading preferences through daily actions (recoverability of function values) but seeks to guard the workings of an underlying probabilistic algorithm (distribution privacy); and IoT sensors that must recover user commands for execution (recoverability) but without the details of user habits being compromised (distribution privacy). An instance of the second category would occur when a user's predilections for Smart TV [27] programs must not be compromised when program requests are made to a service provider.

In the new problem formulation above, our main results are as follows. Considering an arbitrary function, we first provide a basic achievable lower bound for distribution ρ-privacy that does not depend on n and represents "worst-case" privacy. This worst-case privacy is characterized as a function of ρ and equals the logsum cardinalities of inverse atoms under the given function, with the number of summands decreasing as ρ increases from 0 to 1. We introduce specialized strategies: "sparse pmf" and "locally identical query response" for the user and "locally uniform estimator" for the querier. Primitive forms of these strategies play a role in establishing the characterization of worst-case privacy. We then provide upper (converse) and lower (achievability) bounds for distribution ρ-privacy – the former for every n and the latter for all n suitably large. These bounds are shown to be asymptotically tight, converging to worst-case privacy with increasing n in the worthwhile regime $0.5 < \rho \leq 1$. A key facilitating step in our converse proof is the recognition that with the querier's

Manuscript received March 14, 2021; revised October 22, 2021; accepted December 24, 2021. Date of publication January 4, 2022; date of current version April 21, 2022. This work was supported by the U.S. National Science Foundation under Grant CCF 1527354. *(Corresponding author: Prakash Narayan.)*

The authors are with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: ajayk@umd.edu; prakash@umd.edu).

Communicated by S. Boucheron, Associate Editor for Machine Learning and Statistics.

Digital Object Identifier 10.1109/TIT.2022.3140317

[1]For $n = 1$, clearly "i.i.d." is redundant.

strategy restricted to a locally uniform estimator, the user can make do with a sparse pmf and locally identical query response without sacrificing distribution privacy. The roles of restriction and adequacy are reversed in the achievability proof. Significantly, the converse and achievability proofs spell out specifications of explicit user and querier actions. Preliminary versions of this work are in [30] for binary-valued functions, and in [31].

An extensive body of prior work exists on distribution estimation in the context of data privacy (cf. e.g., [3], [7], [14], [17], [21] and references therein). Privacy constraints, when explicitly present, are dominantly in the sense of differential privacy (cf. [15], [16]). In a series [13], [22], [33], [39], 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 ℓ_2-distance between the user's distribution and the querier's estimate (maximum and minimum, respectively, over possible user distributions and querier estimators), its minimum is examined over all the differentially private randomization mechanisms of the given level. In Section V, we broach the idea of examining our present work in the context of this approach. In another line of work [4], [5], [8], [24], [32], *sans privacy considerations* but relevant to ours, data samples are generated according to a distribution from a given set. The objective is for the user to select a distribution that resists estimation by the best estimator under a divergence cost. Investigated accordingly are the maximum and minimum, respectively, over user distributions and estimators of the expected divergence between the user distribution and the estimate. Also, see [23] for a similar minmax study under other loss measures. These approaches to distribution estimation, with or without privacy, do not require computation of a function of the underlying data.

Data privacy in various forms (rather than privacy of data distribution) is the subject of another vast body of work. Considerations include maximizing data utility under privacy constraints (for instance, differential privacy, privacy based on information measures, and data estimation error probability); examples can be found in [1]–[3], [18], [19], [37]. Likewise, data utility-privacy tradeoffs are analyzed also by maximizing privacy for a given level of utility [6], [26], [35], [20], [25], [36]. Our prior work [29] is of the nature of the latter where, under an explicit constraint on function recoverability, data privacy is maximized. Specifically, for finite-valued data and query responses, upon limiting ourselves to privacy as a probability of error and recoverability as a (pointwise) conditional probability of error, we obtain utility-privacy tradeoffs for single and multiple query responses. Our present work is in this spirit: maximizing the privacy of data distribution under a function recoverability constraint.

Our model for distribution ρ-privacy is described in Section II which then characterizes the resulting worst-case privacy, as demonstrated by an achievability proof. Section III defines specialized user and querier strategies, and states the converse and achievability theorems which are proved in Section IV. The concluding Section V provides a heuristic explanation of the characterization of distribution ρ-privacy, and cites unanswered questions including one that touches on local differential privacy.

II. Preliminaries and Worst-Case Privacy

A user generates data represented by i.i.d. rvs $X_1, \ldots, X_n$, $n \geq 1$, with pmf P_X and with X_1 taking values in a finite set $\mathcal{X}$ of cardinality $|\mathcal{X}| = r \geq 2$. Consider a given mapping $f : \mathcal{X} \to \mathcal{Z} = \{0, 1, \ldots, k-1\}$, $2 \leq k \leq r$. Let f^{-1} denote the corresponding preimage mapping with $f^{-1}(z) = \{x \in \mathcal{X} : f(x) = z\}$, $z \in \mathcal{Z}$. For realizations $X_1 = x_1, \ldots, X_n = x_n$, a querier – who does not know $x^n \triangleq (x_1, \ldots, x_n)$ 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.[2]

Definition 1: Given $0 \leq \rho \leq 1$, a QR Z_t is *ρ-recoverable* (ρ-QR) if

$$P\left(Z_t = f(x) \middle| X_t = x\right) \geq \rho, \quad x \in \mathcal{X}. \tag{1}$$

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

$$W\big(f(x)\,|x\big) \geq \rho, \quad x \in \mathcal{X} \tag{2}$$

and such a W, too, will be termed a ρ-QR. Note that ρ-recoverability in (1), (2) does not depend on P_X.

The ρ-QRs $Z_1, \ldots, Z_n$ are assumed to satisfy

$$\begin{aligned} &P\left(Z^n = z^n | X^n = x^n\right) \\ &\triangleq P\left(Z_1 = z_1, \ldots, Z_n = z_n | X_1 = x_1, \ldots, X_n = x_n\right) \\ &= \prod_{t=1}^{n} P\left(Z_t = z_t | X_t = x_t\right) \\ &= \prod_{t=1}^{n} W\left(z_t | x_t\right), \quad x^n \in \mathcal{X}^n, z^n \in \mathcal{Z}^n, \end{aligned} \tag{3}$$

whereupon since $X_1, \ldots, X_n$ are i.i.d., so too are $Z_1, \ldots, Z_n$, with pmf $\left(P_X W\right)(z) \triangleq \sum_{x \in \mathcal{X}} P_X(x) W(z|x)$, $z \in \mathcal{Z}$. The user chooses the pmf P_X and the ρ-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 a suitable estimator $\widehat{P}_n : \mathcal{Z}^n \to \Delta_r$, where Δ_r is the r-dimensional simplex associated with $\mathcal{X}$.

The measure of discrepancy between the pmf P_X and the querier's estimate $\widehat{P}_n$ is

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n\right) \triangleq \mathbb{E}\left[D\left(P_X \middle|\middle| \widehat{P}_n\left(Z^n\right)\right)\right], \quad 0 \leq \rho \leq 1 \tag{4}$$

where $D(\cdot||\cdot)$ denotes (Kullback-Leibler) divergence[3] and expectation is with respect to the pmf $P_X W$. The user and

[2]As observed in [29, p. 3473, towards the end of Section II], there is no loss of generality in (1), (2) by considering the ρ-QR rvs $Z_1, \ldots, Z_n$ to be $\mathcal{Z}$-valued. If Z_t, $t = 1, \ldots, n$, had an alphabet larger than $\mathcal{Z}$, the querier would *estimate* $f(X)$ based on Z_t. However, the user can emulate any such estimation strategy of the querier to produce another $\mathcal{Z}$-valued ρ-QR.

[3]All logarithms and exponentiations are with respect to the base 2.

querier devise (W, P_X) and $\widehat{P}_n$, respectively, to maximize and minimize $\pi_n\left(\rho, W, P_X, \widehat{P}_n\right)$. 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 $0 \leq \rho \leq 1$; this dependence is not displayed explicitly in the right-side of (4) so as to help contain notational growth.

Definition 2: For $0 \leq \rho \leq 1$, *distribution ρ-privacy* is

$$\pi_n(\rho) \triangleq \sup_{\substack{W: W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \inf_{\widehat{P}_n: \mathcal{Z}^n \to \Delta_r} \sup_{P_X \in \Delta_r} \pi_n\left(\rho, W, P_X, \widehat{P}_n\right), \quad n \geq 1 \tag{5}$$

where W is as in (2) and $\pi_n\left(\rho, W, P_X, \widehat{P}_n\right)$ is given by (4).

Remarks:

(i) The order of maximizations and minimization in (5) accommodates the dependence of $\widehat{P}_n$ on W (and ρ) in providing a conservative measure of distribution privacy. On the other hand, privacy, if gauged by $\inf_{\widehat{P}_n} \sup_{W} \sup_{P_X}$ in (5), 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 (5), if defined instead in terms of $\sup_{W} \sup_{P_X} \inf_{\widehat{P}_n}$, would equal zero unrealistically. Also, reversing the roles of P_X and $\widehat{P}_n(Z^n)$ in $D(\cdot||\cdot)$ in (4), (5) leads to an unrealistic $\pi_n(\rho) = \infty$.

(iii) Clearly, it suffices to restrict the querier's estimators $\widehat{P}_n$ in (5) to those that satisfy $\widehat{P}_n(z^n)(x) > 0, \ z^n \in \mathcal{Z}^n, \ x \in \mathcal{X}$. If the querier were to assign $\widehat{P}_n(z^n)(x) = 0$ to any $x \in \mathcal{X}$, the user can choose $P_X(x) > 0$ for that x (since by (5), P_X can depend on $\widehat{P}_n$), thereby rendering $\pi_n(\rho) = \infty$.

A justification is in order of our model above and choice of divergence as the measure of distribution privacy in (4). First, from a purely heuristic standpoint, for a fixed ρ, any meaningful privacy measure should display the qualitative feature that the associated distribution privacy is nondecreasing with decreasing "atomicity" of a given mapping $f : \mathcal{X} \to \mathcal{Z}$. In other words, the fewer and larger the atoms induced in $\mathcal{X}$ by f^{-1}, the better is the ability of the user to conceal a pmf P_X from the querier. As will be seen below, the concept of distribution ρ-privacy defined in terms of divergence in (4) brings out this behaviour in precise terms and quantifies its dependence on ρ and n. In fact, our main results in Theorems 3, 4 and 5 below depend on $f : \mathcal{X} \to \mathcal{Z}$ only through the sizes $\left|f^{-1}(j)\right|, \ j = 0, 1, \ldots, k-1$. Thus, our divergence formulation is divulgent and also eminently tractable. While other measures of discrepancy between distributions could have been used, any reasonable choice ought to yield answers that do not veer significantly from our divergence-based results that bear out heuristics. We emphasize that our model has features that have been biased deliberately against the user so as to make for a conservative (i.e., diminished) extent of privacy. The recoverability requirement in (1), (2) is imposed stringently for every $t = 1, \ldots, n$, rather than for only over a block of length n ρ-QRs; the latter, in the limit $n \to \infty$, would ask only for *asymptotic* recoverability. Next, as assumed in (3), the ρ-QR W is fixed for $t = 1, \ldots, n$, whereby $Z_1, \ldots, Z_n$ are rendered i.i.d. Moreover, as mentioned before Definition 2, the querier is allowed knowledge of the ρ-QR W. If the user were permitted time-varying ρ-QRs $W_t, \ t = 1, \ldots, n$, it remains open whether a suitably modified definition of distribution ρ-privacy could lead to privacy enhancement.

Two elementary attributes of $\pi_n(\rho)$ are contained in

Proposition 1: For $0 \leq \rho \leq 1$, $\pi_n(\rho)$ is nonincreasing in $n \geq 1$. Furthermore,

$$\pi_n(\rho) \leq \log r, \quad n \geq 1. \tag{6}$$

Proof: To show that $\pi_{n+1}(\rho) \leq \pi_n(\rho), \ n \geq 1$, observe by (4), (5) that in $\pi_{n+1}(\rho)$, for every fixed W,

$$\inf_{\widehat{P}_{n+1}: \mathcal{Z}^{n+1} \to \Delta_r} \sup_{P_X} \mathbb{E}\left[D\left(P_X \middle|\middle| \widehat{P}_{n+1}\left(Z^{n+1}\right)\right)\right] \leq \inf_{\widehat{P}_n: \mathcal{Z}^{n+1} \to \Delta_r} \sup_{P_X} \mathbb{E}\left[D\left(P_X \middle|\middle| \widehat{P}_n\left(Z^{n+1}\right)\right)\right] \tag{7}$$

where, with an abuse of notation, a restricted estimator $\widehat{P_n} : \mathcal{Z}^{n+1} \to \Delta_r$ yields the same estimate for all $z^{n+1} \in \mathcal{Z}^{n+1}$ with common z^n (thereby ignoring z_{n+1}). Then, noting that the expectation in the right-side of (7) with respect to $z^{n+1} \in \mathcal{Z}^{n+1}$ is effectively over $z^n \in \mathcal{Z}^n$, we get from (7) that

$$\inf_{\widehat{P}_{n+1}} \sup_{P_X} \mathbb{E}\left[D\left(P_X \middle|\middle| \widehat{P}_{n+1}\left(Z^{n+1}\right)\right)\right] \leq \inf_{\widehat{P_n}} \sup_{P_X} \mathbb{E}\left[D\left(P_X \middle|\middle| \widehat{P}_n\left(Z^n\right)\right)\right]. \tag{8}$$

Taking $\sup_W$ on both sides of (8) yields $\pi_{n+1}(\rho) \leq \pi_n(\rho)$.

Turning to (6), upon choosing $\widehat{P}_n(z^n)(x) = 1/r, \ z^n \in \mathcal{Z}^n, \ x \in \mathcal{X}$, we get from (4), (5) that

$$\begin{aligned} \pi_n(\rho) &\leq \sup_W \sup_{P_X} \sum_{z^n \in \mathcal{Z}^n} (P_X W)^n (z^n) (\log r - H(P_X)) \\ &= \log r - \inf_{P_X} H(P_X) = \log r. \end{aligned}$$

■

Given $z^n \in \mathcal{Z}^n$, let $Q^{(n)} = Q^{(n)}(z^n)$ be its n-type, i.e., the empirical pmf on $\mathcal{Z}$ associated with z^n (cf. e.g., [10]). For a given n-type $Q^{(n)}$ on $\mathcal{Z}$, let $\mathcal{T}_{Q^{(n)}}$ be the set of all sequences in $\mathcal{Z}^n$ of type $Q^{(n)}$. Let $\mathcal{Q}^{(n)}$ be the set of all n-types on $\mathcal{Z}$. Denote $(P_X W)^n\left(\mathcal{T}_{Q^{(n)}}\right) \triangleq \sum_{z^n \in \mathcal{T}_{Q^{(n)}}} (P_X W)^n (z^n)$.

As shown next, it is adequate to consider querier estimators $\widehat{P}_n : \mathcal{Q}^{(n)} \to \Delta_r$ that are based on the type $Q^{(n)}$ of z^n in $\mathcal{Z}^n$, with said type serving, in effect, as a sufficient statistic. Then, a convenient representation for $\pi_n(\rho)$ in (5) is provided by

Lemma 2: For $0 \leq \rho \leq 1$,

$$\pi_n(\rho) = \sup_W \inf_{\widehat{P}_n} \sup_{P_X} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} (P_X W)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X \middle|\middle| \widehat{P}_n\left(Q^{(n)}\right)\right) \tag{9}$$

with $\widehat{P}_n\left(Q^{(n)}\right)$ representing identical estimates in Δ_r for all $z^n \in \mathcal{T}_{Q^{(n)}}$.

Proof: Observe that for fixed $W, \widehat{P}_n, P_X$,

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n\right) = \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \sum_{z^n \in \mathcal{T}_{Q^{(n)}}} (P_X W)^n (z^n)\, D\left(P_X \middle\| \widehat{P}_n(z^n)\right). \quad (10)$$

For a fixed $Q^{(n)}$, since $(P_X W)^n(z^n)$ is the same for all $z^n \in \mathcal{T}_{Q^{(n)}}$, if $\widehat{P}_n(z^n)$ were to vary across $z^n \in \mathcal{T}_{Q^{(n)}}$, the querier can pick that $\tilde{z^n}$, say, in $\mathcal{T}_{Q^{(n)}}$ for which $D\left(P_X \middle\| \widehat{P}_n(\tilde{z^n})\right)$ is smallest over $\mathcal{T}_{Q^{(n)}}$ and use $\widehat{P}_n(\tilde{z^n})$ as the estimate of P_X for all $z^n \in \mathcal{T}_{Q^{(n)}}$, denoting it by $\widehat{P}_n\left(Q^{(n)}\right)$; this will only serve to decrease the right-side of (10), bearing in mind the inf with respect to $\widehat{P}_n$ in the left-side of (5). Then the right-side of (10) becomes

$$\sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} (P_X W)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X \middle\| \widehat{P}_n\left(Q^{(n)}\right)\right) \quad (11)$$

leading to (9). ■

We close this section with an achievability result that affords a basic lower bound for $\pi_n(\rho)$ as a function of ρ, and also a characterization of $\pi_n(\rho)$ for low values of ρ; none of these bounds depends on n. This lower bound will be lent additional significance in Section III by the converse and achievability results of Theorems 4 and 5, respectively. Also, the choice of a "sparse" user pmf P_X and a "locally uniform" pmf as the querier's estimate in the proof of the following result will motivate the concepts of a "k-sparse pmf" in Definition 5 and "locally uniform estimator" in Definition 3 below.

For P_X in Δ_r, denote the derived pmf $P_X^l\left(f^{-1}\right)$ on $\mathcal{Z}$, $l = 1, \ldots, k$, by

$$P_X^l\left(f^{-1}\right) \triangleq \Bigg(\underbrace{\frac{P_X\left(\bigcup_{l'=0}^{l-1} f^{-1}(l')\right)}{l}, \ldots, \frac{P_X\left(\bigcup_{l'=0}^{l-1} f^{-1}(l')\right)}{l}}_{l \text{ repetitions}}, P_X\left(f^{-1}(l)\right), \ldots, P_X\left(f^{-1}(k-1)\right)\Bigg). \quad (12)$$

In particular, for $l = 1$ we denote

$$P_X^1\left(f^{-1}\right) \triangleq P_X\left(f^{-1}\right) = \left(P_X\left(f^{-1}(0)\right), P_X\left(f^{-1}(1)\right), \ldots, P_X\left(f^{-1}(k-1)\right)\right). \quad (13)$$

Also, for $l = 1, \ldots, k$, let $\mathcal{Z}_l$ denote a generic l-sized subset of $\mathcal{Z}$, with $\mathcal{Z}_k = \mathcal{Z}$.

We define

$$\omega(\rho) \triangleq \begin{cases} \log\left|\bigcup_{j \in \mathcal{Z}_k} f^{-1}(j)\right| = \log\left|f^{-1}(\mathcal{Z})\right| = \log|\mathcal{X}| = \log r, & 0 \le \rho \le \frac{1}{k} \\ \max_{\mathcal{Z}_l \subset \mathcal{Z}} \log\left|\bigcup_{j \in \mathcal{Z}_l} f^{-1}(j)\right| = \max_{\mathcal{Z}_l \subset \mathcal{Z}} \log \sum_{j \in \mathcal{Z}_l} \left|f^{-1}(j)\right|, & \frac{1}{l+1} < \rho \le \frac{1}{l},\ 1 \le l \le k-1, \end{cases} \quad (14)$$

which, under the assumption

$$|f^{-1}(0)| \ge |f^{-1}(1)| \ge \ldots \ge |f^{-1}(k-1)| \quad (15)$$

yields, for $1/k < \rho \le 1$, the simplification

$$\max_{\mathcal{Z}_l \subset \mathcal{Z}} \log \sum_{j \in \mathcal{Z}_l} \left|f^{-1}(j)\right| = \log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|,\ 1 \le l \le k-1. \quad (16)$$

It is verified readily from (14) that $\omega(\rho)$ is nonincreasing in $0 \le \rho \le 1$.

We show next that $\omega(\rho)$ bears the significance of "worst-case" distribution ρ-privacy.

Theorem 3: For each $n \ge 1$, $\pi_n(\rho)$ is nonincreasing in $0 \le \rho \le 1$, and

$$\pi_n(\rho) \ge \omega(\rho), \quad 0 \le \rho \le 1 \quad (17)$$

and

$$\pi_n(\rho) = \omega(\rho) = \log r, \quad 0 \le \rho \le \frac{1}{k}. \quad (18)$$

Remark: By Theorem 3, for the "single-shot" case $n = 1$, $\pi_1(\rho) = \log r,\ 0 \le \rho \le 1/k$, and $\pi_1(\rho) \ge \omega(\rho),\ 1/k < \rho \le 1$. However, a full characterization of $\pi_1(\rho)$ for $1/k < \rho \le 1$ remains open.

Proof: For each $n \ge 1$, it is obvious by (5) that $\pi_n(\rho)$ is nonincreasing in $0 \le \rho \le 1$.

Turning to (17), we shall show that

$$\pi_n(\rho) \ge \max_{\mathcal{Z}_l \subseteq \mathcal{Z}} \log\left|\bigcup_{j \in \mathcal{Z}_l} f^{-1}(j)\right|, \quad 0 \le \rho \le \frac{1}{l},\ 1 \le l \le k \quad (19)$$

from which (17) is deduced readily.

Assume (15) without loss of essential generality. Fix $l \in \{1, \ldots, k\}$. For $0 \le \rho \le 1/l$, the user selects $W_l : \mathcal{X} \to \mathcal{Z}$ as

$$W_l(j|x) = \begin{cases} \frac{1}{l}, & x \in \bigcup_{l'=0}^{l-1} f^{-1}(l'),\ j = 0, 1, \ldots, l-1 \\ 1, & x \in \bigcup_{l'=l}^{k-1} f^{-1}(l'),\ j = f(x). \end{cases} \quad (20)$$

Clearly, $P_X W_l = P_X^l\left(f^{-1}\right)$ in Δ_k (see (12)). Expressing $\sup_{P_X \in \Delta_r}$ in (5) as

$$\sup_{(\alpha, \alpha_l, \ldots, \alpha_{k-1}) \in \Delta_{k-l+1}} \ \sup_{P_X \in \Delta_r : P_X^l(f^{-1}) = \left(\underbrace{\frac{\alpha}{l}, \ldots, \frac{\alpha}{l}}_{l \text{ repetitions}}, \alpha_l, \ldots, \alpha_{k-1}\right)}$$

we obtain from (5), noting that the expectation in (4) is with respect to

$$P_X W_l = P_X^l\left(f^{-1}\right) = \underline{\alpha}^l \triangleq \left(\underbrace{\frac{\alpha}{l}, \ldots, \frac{\alpha}{l}}_{l \text{ repetitions}}, \alpha_l, \ldots, \alpha_{k-1}\right) \quad (21)$$

that

$$\begin{aligned}
&\pi_n(\rho) \\
&\geq \inf_{\widehat{P}_n} \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \sup_{P_X: P_X^l(f^{-1})=\underline{\alpha}^l} \mathbb{E}_{\underline{\alpha}^l}\left[D\left(P_X \middle|\middle| \widehat{P}_n\left(Z^n\right)\right)\right] \\
&\geq \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \inf_{\widehat{P}_n} \sup_{P_X: P_X^l(f^{-1})=\underline{\alpha}^l} \mathbb{E}_{\underline{\alpha}^l}\left[D\left(P_X \middle|\middle| \widehat{P}_n\left(Z^n\right)\right)\right] \\
&\geq \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \inf_{R\in\Delta_r} \sup_{P_X: P_X^l(f^{-1})=\underline{\alpha}^l} D\left(P_X \middle|\middle| R\right).
\end{aligned} \tag{22}$$

Now, observe in (22) that for a fixed $(\alpha, \alpha_l, \ldots, \alpha_{k-1}) \in \Delta_{k-l+1}$, a "sparse" pmf $P_X \in \Delta_r$ of limited support size $k-l+1$ with probabilities $\alpha, \alpha_l, \ldots, \alpha_{k-1}$, respectively, on (single support) symbols in each of $\bigcup_{l'=0}^{l-1} f^{-1}(l'), f^{-1}(l), \ldots, f^{-1}(k-1)$ satisfies the constraint $P_X^l\left(f^{-1}\right) = \underline{\alpha}^l = (\alpha/l, \ldots, \alpha/l, \alpha_l, \ldots, \alpha_{k-1})$. Furthermore, such a P_X with these support symbols being the lowest R-probability symbols in $\bigcup_{l'=0}^{l-1} f^{-1}(l'), f^{-1}(l), \ldots, f^{-1}(k-1)$, respectively, will serve to maximize $D\left(P_X||R\right)$. Accordingly, the pmf $R \in \Delta_r$ that maximizes said lowest probabilities (without knowledge of P_X) and thereby minimizes $D\left(P_X||R\right)$, is a "locally uniform" pmf, viz.

$$R(x) = \begin{cases} \dfrac{\beta}{\left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right|}, & x \in \bigcup_{l'=0}^{l-1} f^{-1}(l') \\ \dfrac{\beta_j}{|f^{-1}(j)|}, & x \in f^{-1}(j),\ j = l, \ldots, k-1 \end{cases}$$

for some $(\beta, \beta_l, \ldots, \beta_{k-1}) \in \Delta_{k-l+1}$. Then in (22), for a fixed $(\alpha, \alpha_l, \ldots, \alpha_{k-1}) \in \Delta_{k-l+1}$,

$$\begin{aligned}
&\inf_{R\in\Delta_r} \sup_{P_X: P_X^l(f^{-1})=\underline{\alpha}^l} D\left(P_X \middle|\middle| R\right) \\
&= \inf_{(\beta,\beta_l,\ldots,\beta_{k-1})\in\Delta_{k-l+1}} \alpha \log \frac{\alpha}{\frac{\beta}{\left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right|}} + \sum_{j=l}^{k-1} \alpha_j \log \frac{\alpha_j}{\frac{\beta^j}{|f^{-1}(j)|}} \\
&= \inf_{(\beta,\beta_l,\ldots,\beta_{k-1})\in\Delta_{k-l+1}} \alpha \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right| \\
&\quad + \sum_{j=l}^{k-1} \alpha_j \log \left|f^{-1}(j)\right| \\
&\quad + D\left(\left(\alpha, \alpha_l, \ldots, \alpha_{k-1}\right) || \left(\beta, \beta_l, \ldots, \beta_{k-1}\right)\right) \\
&= \alpha \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right| + \sum_{j=l}^{k-1} \alpha_j \log \left|f^{-1}(j)\right|
\end{aligned} \tag{23}$$

with the minimum attained by $(\beta, \beta_l, \ldots, \beta_{k-1}) = (\alpha, \alpha_l, \ldots, \alpha_{k-1})$. Combining (22) and (23),

$$\begin{aligned}
&\pi_n(\rho) \\
&\geq \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \alpha \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right| + \sum_{j=l}^{k-1} \alpha_j \log \left|f^{-1}(j)\right| \\
&= \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right|
\end{aligned} \tag{24}$$

with the maximum attained by

$$\alpha = 1, \alpha_l = \cdots = \alpha_{k-1} = 0 \tag{25}$$

upon recalling (15). This establishes (19) with the obvious replacement by the right-side therein of the right-side of (24).

Turning to (18), observe that with $l = k$ and $0 \leq \rho \leq 1/k$, we get from (24) that $\pi_n(\rho) \geq \log r$. With Proposition 1, (18) follows. ∎

The results of Theorem 3 are interpreted as follows. Theorem 3 guarantees a worst-case (i.e., n-free) level of distribution ρ-privacy $\omega(\rho)$, $0 \leq \rho \leq 1$. Specifically, for $1 \leq l \leq k-1$ determined by ρ according to (14), $\pi_n(\rho)$ is at least $\omega(\rho) = \max_{\mathcal{Z}_l \subset \mathcal{Z}} \log \sum_{j\in\mathcal{Z}_l} \left|f^{-1}(j)\right|$, i.e., the logsum of the sizes of the l largest atoms in the f^{-1}-partition of $\mathcal{X}$. This guaranteed ρ-privacy is achieved by the user's choice of P_X as a point mass on any symbol in the union of these l atoms (cf. passage following (22), and (25)) and ρ-QR W_l as in (20). Then, the resulting pmf $P_X W_l$ on $\mathcal{Z}$ has (restricted) support on the f-images in $\mathcal{Z}$ of these l atoms in $\mathcal{X}$, and is uniform among them (21). This helps explain the form of $\omega(\rho)$. We note at this point that Theorem 5 below will describe an achievability scheme whose privacy, for large and suitable but finite n, can exceed $\omega(\rho)$ while tending to it as $n \to \infty$. Moreover, Theorem 3, together with Theorem 4, will establish that $\lim_n \pi_n(\rho) = \omega(\rho)$ for $0.5 < \rho \leq 1$.

III. Converse and Achievability Theorems

Our main Theorems 4 and 5 constitute, respectively, converse and achievability results for distribution ρ-privacy, and yield n-dependent upper and lower bounds for $\pi_n(\rho)$. Instrumental to their proofs are user and querier strategies that employ special constructs. Among the querier's estimators $\widehat{P}_n : \mathcal{Q}^{(n)} \to \Delta_r$, $n \geq 1$, 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, "k-sparse pmfs P_X^{sp}" and "locally identical ρ-QRs W^{lo}" are material in the converse proof.

Definition 3: Let $\beta^{(n)} = \left\{\beta^{(n)}\left(Q^{(n)}\right)\right\}_{Q^{(n)}\in\mathcal{Q}^{(n)}}$, $n \geq 1$, be a set of pmfs in Δ_k indexed by $Q^{(n)} \in \mathcal{Q}^{(n)}$ with each member pmf being of form $\beta^{(n)}\left(Q^{(n)}\right) = \left(\beta_0^{(n)}\left(Q^{(n)}\right), \beta_1^{(n)}\left(Q^{(n)}\right), \ldots, \beta_{k-1}^{(n)}\left(Q^{(n)}\right)\right)$. A *locally uniform estimator* $\widehat{P}_n^{\beta^{(n)}} : \mathcal{Q}^{(n)} \to \Delta_r$ is defined for each

$Q^{(n)} \in \mathcal{Q}^{(n)}$ by

$$\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)(x) = \frac{\beta_j^{(n)}\left(Q^{(n)}\right)}{|f^{-1}(j)|}, \quad x \in f^{-1}(j),\ j \in \mathcal{Z}.$$

Definition 4: Consider any partition of $\mathcal{Z}$ into $k' \le k$ atoms and, with an abuse of notation, label the atoms by $\mathcal{Z}' = \mathcal{Z}'(k') = \{0, 1, \ldots, k'-1\}$. Let $Q'^{(n)}$ be an n-type on $\mathcal{Z}'$, $\mathcal{T}_{Q'^{(n)}}$ the set of all sequences in $\mathcal{Z}'^n$ of type $Q'^{(n)}$, and $\mathcal{Q}'^{(n)}$ the set of all n-types on $\mathcal{Z}'$. A *smooth estimator* $\widehat{P}_n : \mathcal{Q}'^{(n)} \to \Delta_r,\ n \ge 1$, is such that for some $\gamma_n > 0$, $\hat{\gamma}_n > 0$ and $c_n > 0,\ n \ge 1$, with

$$\lim_n \gamma_n = 0, \quad \lim_n \hat{\gamma}_n = 0, \quad \lim_n c_n = 0 \quad \text{and}$$
$$\frac{\hat{\gamma}_n}{c_n} = o\left(\frac{1}{n}\right) \quad \text{implying} \quad \lim_n \frac{\hat{\gamma}_n}{c_n} = 0, \quad (26)$$

it holds for $Q'^{(n)} \ne Q''^{(n)}$ on $\mathcal{Z}'$ with $\mathrm{var}\big(Q'^{(n)}, Q''^{(n)}\big) \le \gamma_n$ that $\mathrm{var}\Big(\widehat{P}_n\left(Q'^{(n)}\right), \widehat{P}_n\left(Q''^{(n)}\right)\Big) \le \hat{\gamma}_n$, where $\mathrm{var}(\cdot,\cdot)$ denotes variational distance (in $\Delta_{k'}$ or Δ_r); and for each $Q'^{(n)} \in \mathcal{Q}'^{(n)}$, $\widehat{P}_n\left(Q'^{(n)}\right)(x) \ge c_n,\ x \in \mathcal{X}$. Denote the class of all such estimators by $\mathcal{S}_n = \mathcal{S}_n(k'),\ n \ge 1$.

Remark: A smooth estimator has the feature that QRs with neighbouring types lead to proximate pmf estimates by the querier. Its second feature of full support $\mathcal{X}$ is motivated by Remark (iii) following Definition 2.

Definition 5: A *k-sparse pmf* P_X^{sp} on $\mathcal{X}$ is defined by

$$P_X^{sp}(x) = \alpha_j, \quad \text{for some } x \in f^{-1}(j),\ j \in \mathcal{Z},$$

and for some k-pmf $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ in Δ_k.

Definition 6: (i) A *locally identical ρ-QR* $W^{lo} : \mathcal{X} \to \mathcal{Z}$ has the form: for each $j \in \mathcal{Z}$, $W^{lo}(\cdot|x)$ is identical for $x \in f^{-1}(j)$, i.e., W^{lo} has identical rows for all x in $f^{-1}(j)$, $j \in \mathcal{Z}$. Associated with each such W^{lo} is a stochastic matrix $V = V\left(W^{lo}\right) : \mathcal{Z} \to \mathcal{Z}$ given by

$$V\left(W^{lo}\right)(j|j') = W^{lo}(j|x) \text{ for every } x \in f^{-1}(j'),\ j, j' \in \mathcal{Z};$$

in particular $V\left(W^{lo}\right)(j|j) \ge \rho,\ j \in \mathcal{Z}$.

(ii) Let $\mathcal{V}(\rho)$ be the set of all stochastic matrices $V : \mathcal{Z} \to \mathcal{Z}$ with $V(j|j) \ge \rho,\ j \in \mathcal{Z}$. For each $V \in \mathcal{V}(\rho)$, set

$$\Delta_k(V) \triangleq \{\underline{\alpha} \in \Delta_k : \underline{\alpha} = \underline{\beta}V \text{ for some } \underline{\beta} \in \Delta_k\}. \quad (27)$$

Remarks: (i) For $W^{lo} : \mathcal{X} \to \mathcal{Z}$ and $V : \mathcal{Z} \to \mathcal{Z}$ as above and for any P_X in Δ_r, it follows that $P_X W^{lo} = P_X\left(f^{-1}\right)V$, both in Δ_k.
(ii) For $V \in \mathcal{V}(\rho),\ 0.5 < \rho \le 1$, V is diagonally-dominated so that V^{-1} exists [34, Theorem 3.3.9].

The following (information geometric) notion will be pertinent for our converse Theorem 4. For $Q^{(n)}$ in $\mathcal{Q}^{(n)}$, and $V \in \mathcal{V}(\rho),\ 0.5 < \rho \le 1$, let

$$\widetilde{Q}\left(Q^{(n)}\right) \triangleq \arg\min_{Q \in \Delta_k(V)} D\left(Q^{(n)} || Q\right) \quad (28)$$

be the reverse I-projection of $Q^{(n)}$ on $\Delta_k(V)$; and for all $\rho > 0$, the minimum exists by [11, Theorem 3.4] since $\Delta_k(V)$ is a closed convex set in $\mathbb{R}^k$ and contains at least one pmf with support equal to $\mathcal{Z}$ as $V(j|j) \ge \rho,\ j \in \mathcal{Z}$. Noting by (27) that $\widetilde{Q}\left(Q^{(n)}\right)V^{-1}$ lies in Δ_k, let $\kappa_n\left(Q^{(n)}\right)$ be its positivized[4] version in Δ_k defined as

$$\kappa_n\left(Q^{(n)}\right)(j) = \frac{n\left(\widetilde{Q}\left(Q^{(n)}\right)V^{-1}\right)(j) + 1}{n+k}, \quad j \in \mathcal{Z}. \quad (29)$$

Observe that $\kappa_n\left(Q^{(n)}\right)$ is in Δ_k has full support $\mathcal{Z}$.

If the user chooses a locally identical ρ-QR $W : \mathcal{X} \to \mathcal{Z}$ with $V = V(W) : \mathcal{Z} \to \mathcal{Z}$ (see Definition 6 (i)), then $Z_1, \ldots, Z_n$ are i.i.d. with (common) pmf $P_X W = P_X(f^{-1})V$ (see (13)) and $P_X(f^{-1})V$ belongs to $\Delta_k(V)$ (see Definition 6 (ii)). The querier, with full knowledge of V, and having observed a sequence z^n in $\mathcal{Z}^n$ of type $Q^{(n)}$, forms a maximum likelihood estimate of the query response pmf $P_X(f^{-1})V$ as $\widetilde{Q}\left(Q^{(n)}\right)$ (28). Therefore, if the querier is restricted to using a locally uniform estimator (see Definition 3), a natural choice for $\beta^{(n)}$ as an attendant proxy for $P_X(f^{-1})$ is κ_n given by (29) and this plays a role in our converse result below.

We now state Theorems 4 and 5. Hereafter, we make Assumption (15) without loss of essential generality; this assumption is made only for the sake of notational convenience. In particular, the upper bound in Theorem 4 for $\pi_n(\rho)$, $0.5 < \rho \le 1$, tends to the lower bound in Theorem 3 as $n \to \infty$. Theorem 5 gives a lower bound for $\pi_n(\rho),\ 1/k < \rho \le 1$, that approaches, as $n \to \infty$, worst-case privacy in Theorem 3. *A notable characteristic of Theorems 3, 4 and 5 is that for all $0 \le \rho \le 1$, the asymptotically optimal limits in n of $\pi_n(\rho)$ are in terms of the logsum cardinalities of inverse atoms (images) under f, with the number of summands decreasing as ρ increases.*

In the range $0.5 < \rho \le 1$, a converse (upper) bound for $\pi_n(\rho),\ n \ge 1$, and thereby for $\lim_n \pi_n(\rho)$, is given by

Theorem 4: For $0.5 < \rho \le 1$ and every $n \ge 1$,

$$\begin{aligned}\pi_n(\rho) &\le \omega(\rho) + \Gamma_n(\rho) \\ &= \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right| + \Gamma_n(\rho), \quad \text{where} \quad (30)\end{aligned}$$

$$\Gamma_n(\rho) \triangleq \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}V^{-1} || \kappa_n\left(Q^{(n)}\right)\right). \quad (31)$$

Furthermore,

$$\lim_n \Gamma_n(\rho) = 0 \quad \text{and} \quad \lim_n \pi_n(\rho) = \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right|. \quad (32)$$

Remarks: (i) In (30), note that $\omega(\rho) = \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right|$ by (14); and additionally under (15), $\omega(\rho) = \log\left|f^{-1}(0)\right|$.

(ii) In general, a closed-form expression is not available for the reverse I-projection $\widetilde{Q}\left(Q^{(n)}\right)$ in (28); an iterative method for computing it is described in [11, Example 5.1]. Hence, $\kappa_n\left(Q^{(n)}\right)$ in (29) and $\Gamma_n(\rho)$ in (31) lack explicit expressions.

The following achievability result is for $1/k < \rho \le 1$; for $0 \le \rho \le 1/k$, Theorem 3 above already characterizes $\pi_n(\rho)$.

[4]The positivization serves to avoid zeros in $\kappa_n\left(Q^{(n)}\right)$.

Theorem 5: Let $1/k < \rho \le 1$. For appropriate locally identical ρ-QRs $W^{lo} = W^{lo}(\rho)$, it holds that for the (restricted) class of smooth estimators for the querier

$$\inf_{\widehat{P}_n \in \mathcal{S}_n} \sup_{P_X} \pi_n\left(\rho, W^{lo}, P_X, \widehat{P}_n\right) \ge \left(\omega(\rho) + \Lambda_n(\rho)\right)\lambda_n(\rho) = \left(\log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right| + \Lambda_n(\rho)\right)\lambda_n(\rho), \quad \frac{1}{l+1} < \rho \le \frac{1}{l}, \quad 1 \le l \le k-1, \tag{33}$$

for all n large enough, where for $l = l(\rho) \le \left\lfloor \frac{k}{2} \right\rfloor$,

$$\Lambda_n(\rho) \triangleq \begin{cases} \log\left(1 + \dfrac{\sum_{j=l}^{\lfloor \frac{k}{l} \rfloor l-1} \left|f^{-1}(j)\right|}{e \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|} \times \dfrac{\min\left\{ \dfrac{\left\lceil nl\left(\frac{1-l\rho}{\lfloor \frac{k}{l} \rfloor l - l}\right)\right\rceil}{n}, \ l\rho \right\} - l\left(\frac{1-l\rho}{\lfloor \frac{k}{l} \rfloor l - l}\right)}{l\rho - l\left(\frac{1-l\rho}{\lfloor \frac{k}{l} \rfloor l - l}\right)}\right) - \dfrac{\hat{\gamma}_n}{c_n}, \\ \qquad \text{if} \quad \sum_{j=l}^{\lfloor \frac{k}{l} \rfloor l-1} \left|f^{-1}(j)\right| \le \sum_{j=0}^{l-1} \left|f^{-1}(j)\right| \\ \log\left(\dfrac{\sum_{j=l}^{\lfloor \frac{k}{l} \rfloor l-1} \left|f^{-1}(j)\right|}{\sum_{j=0}^{l-1} \left|f^{-1}(j)\right|}\right) \times \dfrac{\min\left\{ \dfrac{\left\lceil nl\left(\frac{1-l\rho}{\lfloor \frac{k}{l} \rfloor l - l}\right)\right\rceil}{n}, \ l\rho \right\} - l\left(\frac{1-l\rho}{l\lfloor \frac{k}{l} \rfloor - l}\right)}{l\rho - l\left(\frac{1-l\rho}{\lfloor \frac{k}{l} \rfloor l - l}\right)} - \dfrac{\hat{\gamma}_n}{c_n}, \\ \qquad \text{if} \quad \sum_{j=l}^{\lfloor \frac{k}{l} \rfloor l-1} \left|f^{-1}(j)\right| > \sum_{j=0}^{l-1} \left|f^{-1}(j)\right| \end{cases} \tag{34}$$

and for $l = l(\rho) > \left\lfloor \frac{k}{2} \right\rfloor$,

$$\Lambda_n(\rho) \triangleq \log\left(1 + \frac{\left|f^{-1}(l)\right|}{e \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|} \frac{\frac{\lceil n(1-l\rho)\rceil}{n} - (1-l\rho)}{l\rho}\right) - \frac{\hat{\gamma}_n}{c_n} \tag{35}$$

and for all $l = l(\rho)$,

$$\lambda_n(\rho) \triangleq 1 - \frac{3e^{\left(\frac{4\left(\lfloor \frac{k}{l} \rfloor + k - \lfloor \frac{k}{l} \rfloor l - 1\right)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}} \quad \text{with } \zeta > 1. \tag{36}$$

Furthermore

$$\lim_n \Lambda_n(\rho) = 0, \quad \lim_n \lambda_n(\rho) = 1, \quad \frac{1}{k} < \rho \le 1 \tag{37}$$

and

$$\lim_n \inf_{\widehat{P}_n \in \mathcal{S}_n} \sup_{P_X} \pi_n\left(\rho, W^{lo}, P_X, \widehat{P}_n\right) \ge \omega(\rho) = \log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|, \quad \frac{1}{l+1} < \rho \le \frac{1}{l}, \quad 1 \le l \le k-1. \tag{38}$$

Remarks: (i) The proof of Theorem 5 will show achievability with the user's choice of P_X taking the form of appropriate sparse pmfs. Note that the left-side of (33) serves as a lower bound for $\pi_n(\rho)$ for the class of smooth querier's estimators.

(ii) In (33) and (38), $\omega(\rho) = \log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|$ by (14) and (15).

(iii) Our result in Theorem 5 must be qualified. In (33), the $\log$ terms in (34), (35) can equal 0 for some values of n. For a larger set of ns, $\Lambda_n(\rho) = O\left(\log\left(1 + \frac{1}{n}\right)\right) = O\left(\frac{1}{n}\right)$. Also, $1 - \lambda_n(\rho) = O\left(\frac{1}{n^{\zeta}}\right)$, $\zeta > 1$. Consequently, the right-side of (33) strictly exceeds $\omega(\rho)$ for all large and suitable (but for those from the mentioned set) n.

The proofs of Theorems 4 and 5 are provided in Sections IV-B and IV-C, respectively.

We close this section by interpreting the results of Theorems 3, 4 and 5 when particularized to $f : \mathcal{X} \to \mathcal{Z} = \mathcal{X}$ being an invertible mapping. Then a ρ-QR $W : \mathcal{X} \to \mathcal{X}$ is an $r \times r$-stochastic matrix with diagonal elements $\ge \rho$. Loosely speaking,

(a) for $0 \le \rho \le 0.5$, it is clear that no accurate estimation of P_X from $Z_1, \ldots, Z_n$ – in the sense of the right-side of (5) tending to 0 as $n \to \infty$ – is possible by the querier;

(b) on the other hand, for $0.5 < \rho \le 1$, strongly consistent estimation of P_X by the querier is possible.

In this context, by Theorem 3, for all $n \ge 1$,

$$\pi_n(\rho) \begin{cases} = \omega(\rho) = \log r, & 0 \le \rho \le \frac{1}{r} \\ \ge \omega(\rho) = \log l, & \frac{1}{l+1} < \rho \le \frac{1}{l}, \quad 1 \le l \le r-1 \end{cases} \tag{39}$$

which, since $\omega(\rho) > 0$ for $0 \le \rho \le 0.5$ by (39), reinforces (a) above. Next, $\omega(\rho) = 0$ for $0.5 < \rho \le 1$ by (39), and Theorem 4 gives that for every $n \ge 1$,

$$\pi_n(\rho) \le \Gamma_n(\rho)$$

by (30), (31), where the inner and outer suprema in (31) are over all $\underline{\alpha}$ in the row space of W and all ρ-QRs $W : \mathcal{X} \to \mathcal{X}$, respectively. Also, $\lim_n \pi_n(\rho) = 0$ by (32), in keeping with (b) above. However, by Theorem 5, for large and suitable but finite n, a positive distribution ρ-privacy of at least $\Lambda_n(\rho)\lambda_n(\rho) > 0$ can be achieved, in effect owing to the querier being unable to estimate P_X accurately from $Z_1, \ldots, Z_n$. Here, $\Lambda_n(\rho)$ and $\lambda_n(\rho)$ are specialized from (34), (35) and (36), respectively, with $k = r$ and $\left|f^{-1}(j)\right| = 1$, $j = 0, \ldots, r-1$.

IV. Proofs of Theorems 4 and 5

A. Technical Lemmas

The following technical Lemmas 6 and 7 are pertinent to Theorems 4 and 5, respectively. Their proofs are relegated to Appendix A.

Lemma 6: Consider a k-partition $\mathcal{A} = (A_0, A_1, \ldots, A_{k-1})$ of $\mathcal{X}$ with $A_j \neq \emptyset,\ j \in \mathcal{Z}$. Let P be a pmf on $\mathcal{X}$ and $P(\mathcal{A}) = (P(A_0), P(A_1), \ldots, P(A_{k-1}))$ the corresponding pmf in Δ_k. Fix $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{k-1}) \in \Delta_k$ and let Q be a pmf on $\mathcal{X}$ given by

$$Q(x) = \frac{\beta_j}{|A_j|},\ x \in A_j,\ j \in \mathcal{Z}.$$

Then

$$D(P||Q) \leq D\left(P(\mathcal{A})\middle|\middle|\underline{\beta}\right) + \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j|$$

with equality iff P is a k-point mass with

$$P(x'_j) = P(A_j) \quad \text{for some } x'_j \in A_j,\ j \in \mathcal{Z}. \tag{40}$$

Lemma 7: Consider pmfs P, Q and Q_o on $\mathcal{X}$ such that $support\ (P) \subseteq support\ (Q)\ \subseteq support\ (Q_o)$. Then

$$D\left(P||Q\right) \geq D\left(P||Q_o\right) - \frac{\text{var}\left(Q, Q_o\right)}{Q_o^{min}}$$

where Q_o^{min} is the smallest nonzero value of Q_o.

B. Proof of Theorem 4

Since the querier's estimator $\widehat{P}_n : \mathcal{Z}^n \to \Delta_r$ of P_X is based on the $\mathcal{Z}$-valued observations $Z_1, \ldots, Z_n$, a reasonable procedure entails the estimation of P_X in two steps, without sacrificing the essence of the infimum in (5). In a first step, $\widehat{P}_n$ estimates $P_X\left(f^{-1}\right)$ from $Z_1, \ldots, Z_n$. Next, $\widehat{P}_n$ estimates P_X by uniformizing $P_X\left(f^{-1}\right)$ over symbols in each inverse atom under f; any nonuniform assignment of $P_X\left(f^{-1}\right)$ would be undesirable as it would enable the user to put the entire P_X-probability on the lowest $\widehat{P}_n$- probability symbol in an inverse atom. This suggests the essential optimality in (5) of locally uniform estimators.

Proceeding with this reasoning, a crucial facilitating step is to show that when the querier uses a locally uniform estimator, the user's actions can be limited to k-sparse pmfs and locally identical ρ-QRs *without loss of distribution privacy.*

Lemma 8: Fix $0 \leq \rho \leq 1$. For every $n \geq 1$ and $\beta^{(n)} = \left\{\beta^{(n)}\left(Q^{(n)}\right)\right\}_{Q^{(n)} \in \mathcal{Q}^{(n)}}$,

$$\begin{aligned}&\sup_{W} \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X} \pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right)\\ &= \sup_{W^{lo}} \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X^{sp}} \pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right).\end{aligned} \tag{41}$$

Proof: Since the suprema in the right-side of (41) are over restricted sets, it suffices to show that (41) holds with "$\leq$." Specifically, we show that for every P_X and W there exist P_X^{sp} and W^{lo} such that

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right) \leq \pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right). \tag{42}$$

To this end, let

$$\begin{aligned}&P_X^{sp}(x) = P_X\left(f^{-1}\left(j\right)\right),\\ &\quad \text{for some } x \in f^{-1}\left(j\right),\ j \in \mathcal{Z}\ \ (\text{see Definition } 5),\end{aligned} \tag{43}$$

and let $W^{lo} : \mathcal{X} \to \mathcal{Z}$ be specified as follows:

- for j with $P_X\left(f^{-1}(j)\right) > 0$: for each $x \in f^{-1}(j)$

$$W^{lo}(j'|x) = \sum_{x' \in f^{-1}(j)} \frac{P_X(x')}{P_X\left(f^{-1}(j)\right)} W(j'|x'), \quad j' \in \mathcal{Z} \tag{44}$$

- for j with $P_X\left(f^{-1}(j)\right) = 0$: for each $x \in f^{-1}(j)$

$$W^{lo}(j'|x) = \begin{cases}\rho, & j' = j\\ \frac{1-\rho}{k-1}, & j' \neq j \in \mathcal{Z}.\end{cases} \tag{45}$$

From (43), (44) and (45), it is clear that for each $j \in \mathcal{Z}$,

$$\begin{aligned}&\left(P_X W\right)(j)\\ &= \sum_{x \in \mathcal{X}} P_X(x) W(j|x)\\ &= \sum_{j' \in \mathcal{Z} : P_X(f^{-1}(j')) > 0}\ \sum_{x \in f^{-1}(j')} P_X(x) W(j|x)\\ &= \sum_{j' \in \mathcal{Z} : P_X(f^{-1}(j')) > 0} P_X\left(f^{-1}(j')\right)\\ &\qquad \times \sum_{x \in f^{-1}(j')} \frac{P_X(x)}{P_X\left(f^{-1}(j')\right)} W(j|x)\\ &= \sum_{j' \in \mathcal{Z} : P_X(f^{-1}(j')) > 0} P_X^{sp}(x')\ W^{lo}(j|x'),\\ &\qquad\qquad \text{for some } x' \in f^{-1}(j')\\ &= \left(P_X^{sp} W^{lo}\right)(j)\end{aligned} \tag{46}$$

where the fourth equality above uses (43) and (44). Then, using (11) and (43) - (46),

$$\begin{aligned}&\pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right)\\ &= \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \left(P_X^{sp} W^{lo}\right)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X\middle|\middle|\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right).\end{aligned} \tag{47}$$

Moreover, by Lemma 6,

$$\begin{aligned}&D\left(P_X\middle|\middle|\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right)\\ &\leq D\left(P_X\left(f^{-1}\right)\middle|\middle|\beta^{(n)}\left(Q^{(n)}\right)\right)\\ &\qquad + \sum_{j \in \mathcal{Z}} P_X\left(f^{-1}(j)\right) \log |f^{-1}(j)|\\ &= D\left(P_X^{sp}\middle|\middle|\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right)\end{aligned} \tag{48}$$

by (43) and Definition 3. By (47) and (48), and recalling (11)

$$\begin{aligned}&\pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right)\\ &\leq \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \left(P_X^{sp} W^{lo}\right)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X^{sp}\middle|\middle|\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right)\\ &= \pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right),\end{aligned}$$

which is (42). ∎

Turning to Theorem 4, note by (5) that upon restricting the querier's choice to locally uniform estimators and using Lemma 8

$$\pi_n(\rho) \le \sup_{W^{lo}} \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X^{sp}} \pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right). \quad (49)$$

For fixed W^{lo} and P_X^{sp}, let

$$\underline{\alpha} = P_X^{sp} W^{lo} = P_X^{sp}\left(f^{-1}\right) V\left(W^{lo}\right) \quad (50)$$

where $V\left(W^{lo}\right): \mathcal{Z} \to \mathcal{Z}$ is as in Definition 6 (i). Since $\rho > 0.5$, $V\left(W^{lo}\right)^{-1}$ exists (see Remark (ii) following Definition 6). Then, upon fixing $\widehat{P}_n^{\beta^{(n)}}$, too, using (11) and (50) we get

$$\begin{aligned}
&\pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right)\\
&= \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X^{sp} \,||\, \widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right)\\
&= \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X^{sp}\left(f^{-1}\right) \,||\, \beta^{(n)}\left(Q^{(n)}\right)\right)\\
&\qquad + \sum_{j \in \mathcal{Z}} P_X^{sp}\left(f^{-1}(j)\right) \log\left|f^{-1}(j)\right| \quad (51)
\end{aligned}$$

by equality in Lemma 6. Next, note from (50) that

$$P_X^{sp}\left(f^{-1}\right) = \underline{\alpha}\ \left(V\left(W^{lo}\right)\right)^{-1}. \quad (52)$$

Then, from (51) and (52),

$$\begin{aligned}
&\pi_n\left(\rho, W^{lo}, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right)\\
&\le \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right| +\\
&\sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\ \left(V\left(W^{lo}\right)\right)^{-1} \Big|\Big| \beta^{(n)}\left(Q^{(n)}\right)\right). \quad (53)
\end{aligned}$$

Hence, in (49) upon using (50) - (53),

$$\begin{aligned}
&\pi_n(\rho)\\
&\le \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right|\\
&+ \sup_{W^{lo}} \inf_{\beta^{(n)}\left(Q^{(n)}\right)} \sup_{\underline{\alpha} \in \Delta_k\left(V\left(W^{lo}\right)\right)}\\
&\quad \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\ \left(V\left(W^{lo}\right)\right)^{-1} \Big|\Big| \beta^{(n)}\left(Q^{(n)}\right)\right)\\
&= \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right|\\
&+ \sup_{\substack{V: \mathcal{Z} \to \mathcal{Z}\\ V\left(j'|j'\right) \ge \rho,\ j' \in \mathcal{Z}}} \inf_{\beta^{(n)}\left(Q^{(n)}\right)} \sup_{\underline{\alpha} \in \Delta_k(V)}\\
&\quad \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\ V^{-1} \,||\, \beta^{(n)}\left(Q^{(n)}\right)\right).
\end{aligned}$$

Upon choosing $\beta^{(n)}\left(Q^{(n)}\right) = \kappa_n\left(Q^{(n)}\right)$ (see (29)) and by Definition 6 (ii), which defines $\mathcal{V}(\rho)$, we get

$$\begin{aligned}
\pi_n(\rho) \le \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right| + \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)}\\
\sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\ V^{-1} \,||\, \kappa_n\left(Q^{(n)}\right)\right)
\end{aligned}$$

which is (31).

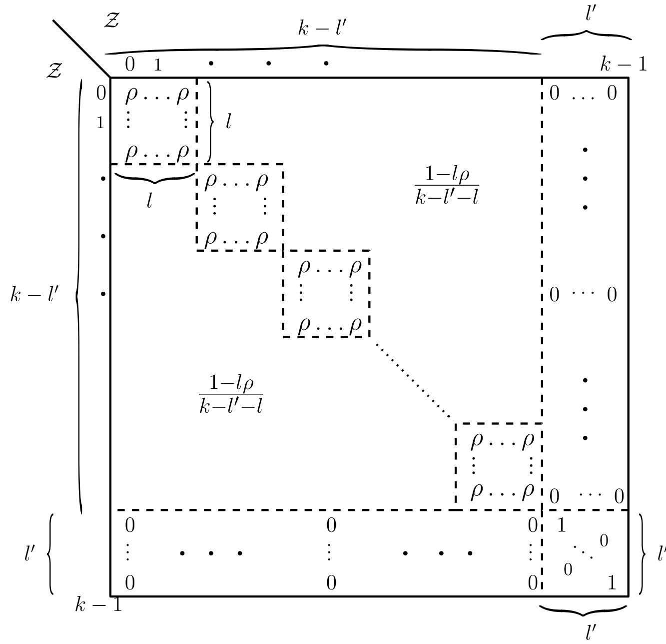

Fig. 1. $V_1 : \mathcal{Z} \to \mathcal{Z}$.

Next, to show (32), observe that

$$\Gamma_n(\rho) = \sup_{V \in \mathcal{V}(\rho)} \sup_{\alpha \in \Delta_k(V)} \mathbb{E}_{\underline{\alpha}}\left[D\left(\underline{\alpha} V^{-1} || \kappa_n\left(T_n\right)\right)\right]$$

where the $\mathcal{Q}^{(n)}$-valued rv T_n has underlying pmf $\underline{\alpha} \in \Delta_k(V)$. Continuing

$$\begin{aligned}
&\Gamma_n(\rho)\\
&= \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \mathbb{E}_{\underline{\alpha}}\left[\sum_{j \in \mathcal{Z}} \left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right]\\
&= \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \sum_{j \in \mathcal{Z}} \mathbb{E}_{\underline{\alpha}}\left[\left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right]\\
&\le \sum_{j \in \mathcal{Z}} \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \mathbb{E}_{\underline{\alpha}}\left[\left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right]. \quad (54)
\end{aligned}$$

Denoting the rvs in $[\cdots]$ in (54) above by

$$\begin{aligned}
\Phi_n^j(\underline{\alpha}, V) &= \Phi_n^j\left(\kappa_n(T_n)(j), \underline{\alpha}, V\right)\\
&\triangleq \left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}, \qquad j \in \mathcal{Z},
\end{aligned}$$

we show in Appendix B that

$$\lim_n \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \mathbb{E}\left[\left|\Phi_n^j(\underline{\alpha}, V)\right|\right] = 0, \quad j \in \mathcal{Z}. \quad (55)$$

Then, by (54) and (55), the first assertion in (32) obtains. The second assertion in (32) follows from (54), (55) and (14), (17) with $l = 1$. ■

C. Proof of Theorem 5

Fix $1/k < \rho \leq 1$. As in the statement of the theorem, $l = l(\rho)$ is determined by

$$\frac{1}{l+1} < \rho \leq \frac{1}{l}, \quad 1 \leq l \leq k-1. \tag{56}$$

We consider separately the cases $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ and $l > \left\lfloor \frac{k}{2} \right\rfloor$.

The proof proceeds in the following four steps for each of the cases $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ and[5] $l > \left\lfloor \frac{k}{2} \right\rfloor$:

1. description of chosen locally identical ρ-QRs $V_1 : \mathcal{Z} \to \mathcal{Z}$ and $V_2 : \mathcal{Z} \to \mathcal{Z}$ for the two cases, respectively (see Definition 6 (i));
2. reduction in the choice of querier estimators induced by V_1 and V_2;
3. selection of a set of sparse pmfs with suitable range cardinality;
4. establishment of the sufficiency of locally uniform querier estimators and identification of a specific such estimator.

These steps are described next with some of the details provided in Appendix C.

Case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ **:**

Step 1: The user selects P_X (to be specified later) and a locally-identical ρ-QR $W_1^{lo} = W_1^{lo}(\rho) : \mathcal{X} \to \mathcal{Z}$ described next in terms of an associated stochastic matrix $V_1 = V_1\left(W_1^{lo}\right) : \mathcal{Z} \to \mathcal{Z}$. It is assumed that the rows of W_1^{lo} are arranged in order, respectively, according to $f^{-1}(0), f^{-1}(1), \ldots, f^{-1}(k-1)$; this entails no loss of generality. Set

$$l' = l'(\rho) \triangleq k - \left\lfloor \frac{k}{l} \right\rfloor l. \tag{57}$$

Clearly $0 \leq l' < l$. Then, as illustrated in Fig. 1, $V_1 : \mathcal{Z} \to \mathcal{Z}$ is chosen as follows:

- the top-left $(k-l') \times (k-l')$-subblock of V_1 consists of $\left\lfloor \frac{k}{l} \right\rfloor = \frac{k-l'}{l}$ diagonal blocks of $l \times l$-matrices with all entries equal to ρ, and with the remaining entries being $\frac{1-l\rho}{k-l'-l}$;
- the bottom-right $l' \times l'$-subblock is an identity matrix;
- the bottom-left $l' \times (k-l')$-subblock and the top-right $(k-l') \times l'$-subblock consist of zeros.

In the specification of V_1 above, note that $k - l' - l \geq 1$ since

$$\left\lfloor \frac{k}{l} \right\rfloor \geq \left\lfloor \frac{k}{\left\lfloor \frac{k}{2} \right\rfloor} \right\rfloor \geq \left\lfloor \frac{k}{\frac{k}{2}} \right\rfloor = 2 \quad \text{so that}$$

$$k - l' - l = \left\lfloor \frac{k}{l} \right\rfloor l - l \geq 2l - l = l \geq 1. \tag{58}$$

The rationale for our specific choice of $V_1 : \mathcal{Z} \to \mathcal{Z}$ is guided by two features. First, it is advantageous for the user if V_1 has as few distinct rows as possible. Second, each diagonal element must be at least ρ, by the ρ-recoverability constraint. Thus, the chosen $V_1 : \mathcal{Z} \to \mathcal{Z}$ has $\left\lfloor \frac{k}{l} \right\rfloor$ blocks of l rows that are identical (and distinct among such blocks), with $\left\lfloor \frac{k}{l} \right\rfloor$ $l \times l$ ρ-blocks along the diagonal, except for boundary fillers.

Step 2: With $V_1 : \mathcal{Z} \to \mathcal{Z}$ as above and for any P_X in Δ_r, $P_X(f^{-1})V_1 \in \Delta_k$ has identical entries in each of $\left\lfloor \frac{k}{l} \right\rfloor = \frac{k-l'}{l}$ blocks (each with l entries); and possibly l' distinct entries $P_X\left(f^{-1}(k-l')\right), \ldots, P_X\left(f^{-1}(k-1)\right)$. Accordingly, consider a reduced set resulting from $\mathcal{Z}$, namely

$$\mathcal{Z}' \triangleq \left\{0, 1, \ldots, \frac{k-l'}{l} - 1, \frac{k-l'}{l}, \ldots \frac{k-l'}{l} + l' - 1\right\} \tag{59}$$

obtained by merging those symbols in $\mathcal{Z}$ that lie within each of the mentioned blocks, and thereby of diminished cardinality

$$k' = k'(\rho) \triangleq \frac{k-l'}{l} + l' = \left\lfloor \frac{k}{l} \right\rfloor + l' \leq k \tag{60}$$

on which $P_X\left(f^{-1}\right)V_1$ can have possibly different probability values. The resulting merged probabilities on $\mathcal{Z}'$ are obtained as $P_X\left(f^{-1}\right)V_1'$, where $V_1' = V_1'(V_1) : \mathcal{Z} \to \mathcal{Z}'$ is obtained by merging blocks of l columns of V_1 (and their elements). Then, $V_1' : \mathcal{Z} \to \mathcal{Z}'$ is as illustrated in Fig. 2, and is described as follows.

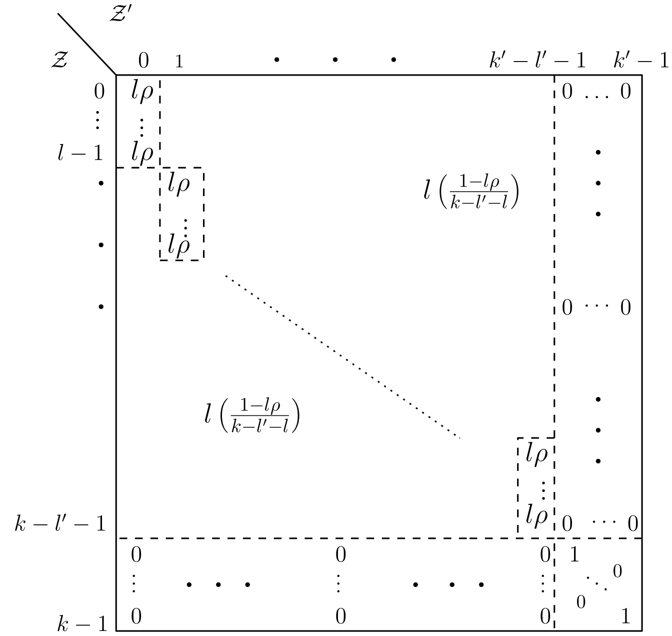

Fig. 2. $V_1' : \mathcal{Z} \to \mathcal{Z}'$.

For $0 \leq j \leq k-1$ and $0 \leq j' \leq k'-1$,

$$V_1'(j'|j) = \begin{cases} l\rho, & j' = 0, 1, \ldots, k'-l'-1, \\ & j = j' \cdot l, \ldots, (j'+1)l - 1 \\ l\left(\frac{1-l\rho}{k-l'-l}\right), & j' = 0, 1, \ldots, k'-l'-1, \\ & j \neq j' \cdot l, \ldots, (j'+1)l - 1, \quad j \leq k-l'-1 \\ 1, & (j' = k'-l', j = k-l'), \\ & \ldots, (j' = k'-1, j = k-1) \\ 0, & \text{otherwise.} \end{cases} \tag{61}$$

For the user's choice of $V_1 = V_1\left(W_1^{lo}\right) : \mathcal{Z} \to \mathcal{Z}$ as above, its effect on the querier's estimation of P_X is governed by $V_1' = V_1'(V_1) : \mathcal{Z} \to \mathcal{Z}'$ in (61). Let $\mathcal{Q}'^{(n)}$ denote the set of

[5]For $k = 2$, only the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ occurs.

all types on $\mathcal{Z}'^n$. Then precisely, referring to (11), we claim that

$$\inf_{\widehat{P}_n:\mathcal{Q}^{(n)}\to\Delta_r}\sup_{P_X}\sum_{Q^{(n)}\in\mathcal{Q}^{(n)}}\left(P_X\left(f^{-1}\right)V_1\right)^n\left(\mathcal{T}_{Q^{(n)}}\right)\times D\left(P_X\middle|\middle|\widehat{P}_n\left(Q^{(n)}\right)\right)$$
$$=\inf_{\widehat{P}_n:\mathcal{Q}'^{(n)}\to\Delta_r}\sup_{P_X}\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}}\left(P_X\left(f^{-1}\right)V_1'\right)^n\left(\mathcal{T}_{Q'^{(n)}}\right)\times D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right) \quad (62)$$

with an obvious abuse of notation of $\widehat{P}_n$ in the right-side. To this end, observe that all $z^n\in\mathcal{T}_{Q^{(n)}}$ for some (fixed) $Q^{(n)}\in\mathcal{Q}^{(n)}$ result in (possibly different) $z'^n\in\mathcal{Z}'^n$ but of a common type $Q'^{(n)}\in\mathcal{Q}'^{(n)}$, by the merge described in the passage preceding (59); furthermore, different $Q^{(n)}\in\mathcal{Q}^{(n)}$ can map into the same $Q'^{(n)}\in\mathcal{Q}'^{(n)}$. Using this observation and mimicking the proof of Lemma 2, the claim in (62) follows.

Hereafter in this proof, we restrict attention in (62) to smooth estimators $\widehat{P}_n:\mathcal{Q}'^{(n)}\to\Delta_r$. Then, recalling (11), we get from (62) that

$$\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{P_X}\pi_n\left(\rho,W_1^{lo},P_X,\widehat{P}_n\right)$$
$$=\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{P_X}\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}}\left(P_X(f^{-1})V_1'\right)^n\left(\mathcal{T}_{Q'^{(n)}}\right)\times D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right)$$
$$=\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\underline{\alpha}\in\Delta_{k'}}\sup_{P_X:P_X(f^{-1})V_1'=\underline{\alpha}}\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)\ D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right). \quad (63)$$

The sum in the right-side of (63) is bounded below further as follows: for each $\underline{\alpha}\in\Delta_{k'}$, we restrict attention to those types $Q'^{(n)}\in\mathcal{Q}'^{(n)}$ that are close to types $Q'^{(n)}(\underline{\alpha})$ which approximate $\underline{\alpha}$. Then,

$$\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)\ D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right)$$
$$\geq\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}:\ \mathrm{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)\times D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right) \quad (64)$$

where

$$Q'^{(n)}(\underline{\alpha})(j')=\frac{\lceil n\underline{\alpha}(j')\rceil}{n},\quad j'=1,\ldots,k'-1$$
$$\text{and}\quad Q'^{(n)}(\underline{\alpha})(0)=1-\sum_{j'\neq 0}\frac{\lceil n\underline{\alpha}(j')\rceil}{n} \quad (65)$$

and γ_n will be specified below. For $Q'^{(n)}(\underline{\alpha})$ in (65) to be a pmf in $\Delta_{k'}$, it suffices for $\underline{\alpha}\in\Delta_{k'}$ and n to satisfy

$$1-\sum_{j'\neq 0}\frac{\lceil n\underline{\alpha}(j')\rceil}{n}\geq 0$$

which, in turn, is implied if

$$1-\sum_{j'\neq 0}\frac{n\underline{\alpha}(j')+1}{n}=\underline{\alpha}(0)-\frac{k'-1}{n}\geq 0. \quad (66)$$

In Appendix C, we shall show that $\underline{\alpha}\in\Delta_{k'}$ can be restricted further and n chosen large enough with

$$n\geq N_0(k')=2k', \quad (67)$$

so that (66) holds (without any dependence of N_0 on $\underline{\alpha}$).

Since $\widehat{P}_n$ is a smooth estimator in $\mathcal{S}_n(k')$, $\mathrm{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n$ implies $\mathrm{var}\left(\widehat{P}_n\left(Q'^{(n)}\right),\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)\leq\hat{\gamma}_n$ and $\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)\geq c_n>0,\ x\in\mathcal{X}$ (see Definition 4).

Then in the right-side of (64), by Lemma 7

$$D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right)$$
$$\geq D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)-\frac{\mathrm{var}\left(\widehat{P}_n\left(Q'^{(n)}\right),\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)}{\min_{x\in\mathcal{X}}\ \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}$$
$$\geq D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)-\frac{\hat{\gamma}_n}{c_n}. \quad (68)$$

Hence in (64), using (68),

$$\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)\ D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}\right)\right)$$
$$\geq\left[D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)-\frac{\hat{\gamma}_n}{c_n}\right]\times\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}:\ \mathrm{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right). \quad (69)$$

Next, in the right-side of (69), with T_n' denoting a $\mathcal{Q}'^{(n)}$-valued rv with underlying pmf $\underline{\alpha}\in\Delta_{k'}$, we get

$$\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}:\ \mathrm{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n}\underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)$$
$$=P\left(\mathrm{var}\left(T_n',Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n\right) \quad (70)$$
$$=1-P\left(\mathrm{var}\left(T_n',Q'^{(n)}(\underline{\alpha})\right)>\gamma_n\right)$$
$$\geq 1-P\left(\mathrm{var}\left(T_n',\underline{\alpha}\right)+\mathrm{var}\left(\underline{\alpha},Q'^{(n)}(\underline{\alpha})\right)\geq\gamma_n\right) \quad (71)$$
$$\geq 1-P\left(\mathrm{var}\left(T_n',\underline{\alpha}\right)\geq\gamma_n-\frac{2(k'-1)}{n}\right) \quad (72)$$

where (71) is by the triangle inequality for $\mathrm{var}(\cdot,\cdot)$, and (72) holds since $\mathrm{var}\left(\underline{\alpha},Q'^{(n)}(\underline{\alpha})\right)\leq\frac{2(k'-1)}{n}$ by (65). Denoting

$$\epsilon_n=\gamma_n-\frac{2(k'-1)}{n}, \quad (73)$$

we obtain by [12, Lemma 3] that

$$P\left(\mathrm{var}\left(T'_n,\underline{\alpha}\right)\geq\epsilon_n\right)\leq 3e^{\left(-n\frac{\epsilon_n^2}{25}\right)} \tag{74}$$

for all n such that

$$\epsilon_n>0 \quad\text{and}\quad n\epsilon_n^2\geq 20k'. \tag{75}$$

Now, pick

$$\gamma_n=5\sqrt{\frac{\zeta\ln 2\log n}{n}},\quad n\geq 1 \text{ and } \zeta>1 \tag{76}$$

so that $\lim_n \gamma_n=0$. Then (75) holds for all $n\geq N_1(k')$ determined by

$$5\sqrt{n\zeta\ln 2\log n}>2(k'-1),$$

and for all $n\geq N_2(k')$ determined by

$$25\zeta\ln 2\log n+\frac{4(k'-1)^2}{n}-20(k'-1)\sqrt{\frac{\zeta\ln 2\log n}{n}}\geq 20k'.$$

Then for $n\geq\max\{N_1(k'),N_2(k')\}$, (74) holds, and thereby by (73) and (76),

$$P\left(\mathrm{var}\left(T'_n,\underline{\alpha}\right)\geq\gamma_n-\frac{2(k'-1)}{n}\right)\leq \frac{3e^{\left(\frac{-4(k'-1)^2}{25n}\right)}e^{\left(\frac{4(k'-1)}{5}\sqrt{\frac{\zeta\ln 2\log n}{n}}\right)}}{n^\zeta}\leq\frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^\zeta} \tag{77}$$

so that in (70)

$$P\left(\mathrm{var}\left(T'_n,Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n\right)\geq 1-\frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^\zeta}, \tag{78}$$

where the right-side above is nonnegative for $n\geq N_3(k')$. Upon gathering (63), (64), (69), (70) and (78), we get that for all $n\geq\max\{N_0(k'),N_1(k'),N_2(k'),N_3(k')\}$,

$$\begin{aligned}&\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{P_X}\pi_n\left(\rho,W_1^{lo},P_X,\widehat{P}_n\right)\\ &\geq\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\underline{\alpha}\in\Delta_{k'}}\sup_{P_X:P_X(f^{-1})V_1'=\underline{\alpha}}\\ &\left[D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)-\frac{\hat{\gamma}_n}{c_n}\right]\left(1-\frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^\zeta}\right).\end{aligned} \tag{79}$$

Step 3: It remains to reduce the right-side of (79) to (33), (34), (36). The main steps are outlined below and the details are given in Appendix C. First, for $\underline{\alpha}\in\Delta_{k'}$, a straightforward manipulation using (61) shows that $P_X(f^{-1})V_1'=\underline{\alpha}$ can be written as

$$\begin{aligned}&l\rho P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1}f^{-1}(j)\right)\\ &+\left(1-P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1}f^{-1}(j)\right)-P_X\left(\bigcup_{j=k'-l'}^{k'-1}f^{-1}(j)\right)\right)\\ &\times l\left(\frac{1-l\rho}{k-l'-l}\right)=\underline{\alpha}(j'),\quad j'=0,1,\ldots,k'-l'-1,\end{aligned} \tag{80}$$

$$\text{and}\qquad P_X\left(f^{-1}(j')\right)=\underline{\alpha}(j'),\quad j'=k'-l',\ldots,k'-1. \tag{81}$$

Combining (80) and (81), we get

$$\begin{aligned}&P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1}f^{-1}(j)\right)\\ &=\frac{\underline{\alpha}(j')-l\left(\frac{1-l\rho}{k-l'-l}\right)\left(1-\sum_{j=k'-l'}^{k'-1}\underline{\alpha}(j)\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)},\\ &\qquad j'=0,1,\ldots,k'-l'-1.\end{aligned} \tag{82}$$

Then in (79), fixing $\widehat{P}_n\in\mathcal{S}_n(k')$ and $\underline{\alpha}\in\Delta_{k'}$,

$$\begin{aligned}&\sup_{P_X:P_X(f^{-1})V_1'=\underline{\alpha}}D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)\\ &=\sup_{P_X:P_X\sim\text{ (81), (82)}}D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)\end{aligned} \tag{83}$$

where $P_X\sim(81),(82)$ connotes P_X consistent with (81) and (82). Next, consider a derived mapping $f'^{-1}:\mathcal{Z}'\to\mathcal{X}$ defined in terms of $f^{-1}:\mathcal{Z}\to\mathcal{X}$ as follows:

$$f'^{-1}(j')=\begin{cases}\bigcup_{j=j'l}^{j'(l+1)-1}f^{-1}(j), & j'=0,1,\ldots,k'-l'-1\\ f^{-1}(k-k'+j'), & j'=k'-l',\ldots,k'-1\end{cases} \tag{84}$$

and define a k'-sparse pmf P_X^{sp} on $\mathcal{X}$ as in Definition 5 with k', $j'\in\mathcal{Z}'$ and f'^{-1} in lieu of k, $j\in\mathcal{Z}$ and f^{-1} therein. The right-side of (83) is bounded below further by a restriction to k'-sparse pmfs P_X^{sp} on $\mathcal{X}$ whose support symbols are the lowest $\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)$-probability symbols within $f'^{-1}(j')$, $j'=0,1,\ldots,k'-1$. Additionally, pick $\underline{\alpha}\in\Delta_{k'}$ in (79) with $\underline{\alpha}(j')=0$, $j'=k'-l',\ldots,k'-1$. Then a straightforward substitution in (79) using (83) and (84) yields that

$$\begin{aligned}&\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\underline{\alpha}\in\Delta_{k'}}\sup_{P_X:P_X\sim(81),\ (82)}D\left(P_X\middle|\middle|\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)\\ &\geq\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ \underline{\alpha}(j')=0,\ j'=k'-l',\ldots,k'-1}}\\ &\sum_{j'=0}^{k'-l'-1}\frac{\underline{\alpha}(j')-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}\end{aligned}$$

$$\times \log \left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{1}{\min\limits_{x \in f'^{-1}(j')} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)} \right), \tag{85}$$

where the coefficient of each log term is in $[0, 1]$.

Step 4: In (85), observe that for every $\widehat{P}_n : \mathcal{Q}'^{(n)} \to \mathcal{X}$, there exists a locally uniform estimator (see Definition 3, with k' replacing k and f'^{-1} replacing f^{-1}), depending on $\widehat{P}_n$, and specified by

$$\beta^{(n)} = \left\{\beta^{(n)}\left(Q'^{(n)}\right)\right\}_{Q'^{(n)} \in \mathcal{Q}'^{(n)}}, \qquad n \geq 1,$$

with $\beta^{(n)}\left(Q'^{(n)}\right) = \left(\beta_0^{(n)}\left(Q'^{(n)}\right), \beta_1^{(n)}\left(Q'^{(n)}\right), \ldots, \beta_{k'-1}^{(n)}\left(Q'^{(n)}\right)\right) \in \Delta_{k'}$ and

$$\begin{aligned} &\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}\right)(x) \\ &= \frac{\beta_{j'}^{(n)}\left(Q'^{(n)}\right)}{\left|f'^{-1}(j')\right|}, \quad x \in f'^{-1}(j'), \quad j' \in \mathcal{Z}' \\ &= \frac{\widehat{P}_n\left(Q'^{(n)}\right)\left(f'^{-1}(j')\right)}{\left|f'^{-1}(j')\right|}, \quad x \in f'^{-1}(j'), \quad j' \in \mathcal{Z}' \end{aligned}$$

and with the obvious property that

$$\frac{1}{\min\limits_{x \in f'^{-1}(j')} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)} \geq \frac{\left|f'^{-1}(j')\right|}{\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)}, \quad j' \in \mathcal{Z}'.$$

Hence, $\inf\limits_{\widehat{P}_n}$ in the right-side of (85) can be restricted to $\inf\limits_{\widehat{P}_n^{\beta^{(n)}}}$, and becomes

$$\inf_{\widehat{P}_n^{\beta^{(n)}} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=k'-l',\ldots,k'-1}} \sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \times \log \left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{\left|f'^{-1}(j')\right|}{\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)} \right). \tag{86}$$

Finally, a further lower bound for (86) in Appendix C, taken together with (79), yields

$$\pi_n(\rho) \geq \left(\log\left|f'^{-1}(0)\right| + \Lambda_n(\rho)\right)\lambda_n(\rho) \tag{87}$$

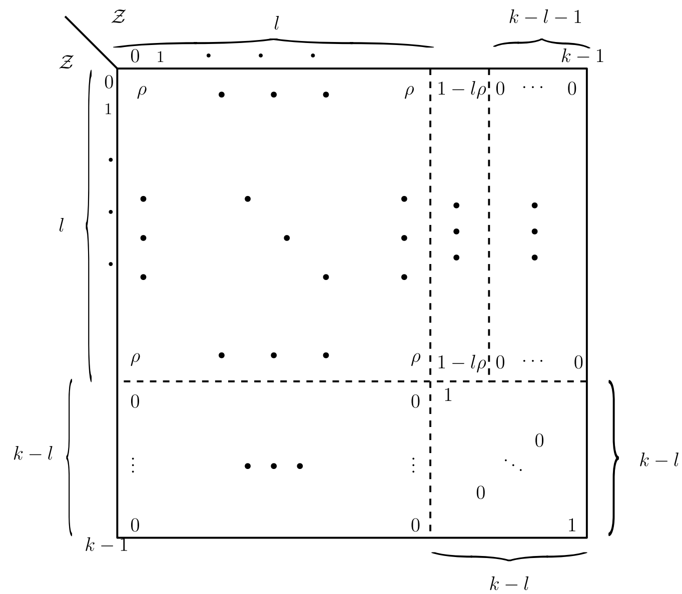

Fig. 3. $V_2 : \mathcal{Z} \to \mathcal{Z}$.

where

$$\Lambda_n(\rho) \triangleq \begin{cases} \log\left(1 + \frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{e\left|f'^{-1}(0)\right|} \times \frac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)}\right) - \frac{\hat{\gamma}_n}{c_n}, \\ \qquad \text{if} \quad \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right| \leq \left|f'^{-1}(0)\right| \\ \log\left(\frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}\right) \times \frac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} - \frac{\hat{\gamma}_n}{c_n}, \\ \qquad \text{if} \quad \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right| > \left|f'^{-1}(0)\right| \end{cases} \tag{88}$$

and

$$\lambda_n(\rho) \triangleq 1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}. \tag{89}$$

From (84), the passage following it, and (85), we have that the user-selected P_X is a k'-sparse pmf with associated mapping f' described by (84). Additional details of the specific k'-sparse pmf chosen by the user are provided in Appendix C.

Thus, for the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$, (33) with (34), (36) follow from (87), (88), (89) upon recalling (57), (60) and (84).

Case $l > \left\lfloor \frac{k}{2} \right\rfloor$:

Step 1: The user selects a locally-identical ρ-QR $W_2^{lo} = W_2^{lo}(\rho) : \mathcal{X} \to \mathcal{Z}$ described in terms of an associated stochastic matrix $V_2 = V_2\left(W_2^{lo}\right) : \mathcal{Z} \to \mathcal{Z}$ and under the assumption that the rows of W_2^{lo} are arranged in order, as in the previous case, according to $f^{-1}(0), f^{-1}(1), \ldots, f^{-1}(k-1)$. The user-selected P_X will be specified later. Let $l' = l'(\rho)$, $\mathcal{Z}'$ and $k' = k'(\rho)$ be as in (57), (59) and (60), respectively. Note that

$$\frac{k}{l} \le \frac{k}{\left\lfloor \frac{k}{2} \right\rfloor + 1} \le \frac{k}{\frac{k+1}{2}} = \frac{2}{1+\frac{1}{k}} < 2 \quad \text{and} \quad \frac{k}{l} \ge \frac{k}{k-1} \ge 1 \quad \text{implies} \quad \left\lfloor \frac{k}{l} \right\rfloor = 1.$$

Hence, $l' = k - l \ge 1$ and $k' = 1 + k - l$. As illustrated in Fig. 3, $V_2 : \mathcal{Z} \to \mathcal{Z}$ is chosen as follows:

- all the entries of the top-left $l \times l$-subblock are ρ;
- the bottom-right $(k-l) \times (k-l)$-subblock is an identity matrix;
- the bottom-left $(k-l) \times l$-subblock and the top-right $l \times (k-l-1)$-subblock consist of zeros;
- the remaining entries are $1 - l\rho$.

The rationale for this structure of $V_2 : \mathcal{Z} \to \mathcal{Z}$ is similar to that for the case $l \le \left\lfloor \frac{k}{2} \right\rfloor$ (see passage following (58)), noting that $\left\lfloor \frac{k}{l} \right\rfloor = 1$ gives a single ρ-block.

Step 2: Consider the stochastic matrix $V_2' = V_2'(V_2) : \mathcal{Z} \to \mathcal{Z}'$, obtained by merging the first l columns of V_2, and described next.

For $0 \le j \le k-1$ and $0 \le j' \le k'-1$,

$$V_2'(j'|j) = \begin{cases} l\rho, & j' = 0, \quad j = 0, 1, \ldots, l-1 \\ 1 - l\rho, & j' = 1, \quad j = 0, 1, \ldots, l-1 \\ 1, & (j' = 1, j = l), \ldots, (j' = k'-1, j = k-1) \\ 0, & \text{otherwise.} \end{cases} \tag{90}$$

Using identical arguments as in the case $l \le \left\lfloor \frac{k}{2} \right\rfloor$ with V_1 and V_1' replaced by V_2 and V_2', respectively, the claim (62) holds and we get

$$\begin{aligned} &\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \pi_n\left(\rho, W_2^{lo}, P_X, \widehat{P}_n\right) \\ &= \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \left(P_X(f^{-1})V_2'\right)^n \left(\mathcal{T}_{Q'^{(n)}}\right) \\ &\qquad \times D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}\right)\right) \\ &= \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} \\ &\qquad \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q'^{(n)}}\right) \; D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}\right)\right). \end{aligned}$$

Following the same steps from (63) - (79), we get that for all $n \ge \max\{N_0(k'), N_1(k'), N_2(k'), N_3(k')\}$

$$\begin{aligned} &\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \pi_n\left(\rho, W_2^{lo}, P_X, \widehat{P}_n\right) \\ &\ge \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} \\ &\left[D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\hat{\gamma}_n}{c_n}\right] \left(1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}\right), \end{aligned} \tag{91}$$

where $N_0(k'), N_1(k'), N_2(k'), N_3(k')$ are described in (67), (75) - (79).

Step 3: In the right-side of (91),

$$\begin{aligned} &\sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \\ &\ge \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} \\ &\qquad D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right). \end{aligned} \tag{92}$$

If $\underline{\alpha} \in \Delta_{k'}$ is such that[6] $\underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1$, then $P_X(f^{-1})V_2' = \underline{\alpha}$, using (90), gives

$$P_X\left(f'^{-1}(0)\right) = \frac{\underline{\alpha}(0)}{l\rho} \tag{93}$$

$$P_X\left(f'^{-1}(1)\right) = \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \tag{94}$$

$$P_X\left(f'^{-1}(j')\right) = 0, \qquad j' = 2, \ldots, k'-1, \tag{95}$$

where $f'^{-1} : \mathcal{Z}' \to \mathcal{X}$ is defined in (84). Then in the right-side of (92),

$$\begin{aligned} &\sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} \\ &\qquad D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \\ &= \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1}} \sup_{P_X : P_X \sim \text{(93), (94), (95)}} \\ &\qquad D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right). \end{aligned} \tag{96}$$

The right-side of (96) is bounded below further by a restriction to k'-sparse pmfs P_X^{sp} on $\mathcal{X}$ whose support symbols are the lowest $\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)$-probability symbols within $f'^{-1}(j'), \; j' = 0, 1, \ldots, k'-1$, and we get

$$\begin{aligned} &\sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1}} \sup_{P_X : P_X \sim \text{(93), (94), (95)}} \\ &\qquad D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \\ &\ge \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0, \; j' = 2, \ldots, k'-1}} \\ &\qquad \frac{\underline{\alpha}(0)}{l\rho} \log\left(\frac{\underline{\alpha}(0)}{l\rho} \frac{1}{\min\limits_{x \in f'^{-1}(0)} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right) \\ &+ \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \\ &\qquad \times \log\left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{1}{\min\limits_{x \in f'^{-1}(1)} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right). \end{aligned} \tag{97}$$

[6]For $l = k - 1$, i.e., $l' = 1, \; k' = 2$, there are no constraints on $\underline{\alpha}$.

Using (97) in (91), we obtain

$$\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1}) V_2' = \underline{\alpha}} D\left(P_X \middle\| \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)$$
$$\geq \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \log\left(\frac{\underline{\alpha}(0)}{l\rho} \frac{1}{\min_{x \in f'^{-1}(0)} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right)$$
$$+ \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \times \log\left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{1}{\min_{x \in f'^{-1}(1)} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right).$$

Step 4: Using the same reasoning as in the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$, we can restrict $\inf_{\widehat{P}_n \in \mathcal{S}_n(k')}$ above to locally uniform estimators $\inf_{\widehat{P}_n^{\beta(n)} \in \mathcal{S}_n(k')}$ (see Definition 3) so that

$$\inf_{\widehat{P}_n^{\beta(n)} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \log\left(\frac{\underline{\alpha}(0)}{l\rho} \frac{\left|f'^{-1}(0)\right|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(0)\right)}\right)$$
$$+ \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \times \log\left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{\left|f'^{-1}(1)\right|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(1)\right)}\right). \tag{98}$$

A further lower bound for (98) in Appendix C, taken together with (91), yields (87) where

$$\Lambda_n(\rho) \triangleq \log\left(1 + \frac{\left|f'^{-1}(1)\right|}{e\left|f'^{-1}(0)\right|} \frac{\frac{\lceil n(1-l\rho)\rceil}{n} - (1 - l\rho)}{l\rho}\right) - \frac{\hat{\gamma}_n}{c_n} \tag{99}$$

and

$$\lambda_n(\rho) \triangleq 1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}. \tag{100}$$

From (98), we have that the user-selected P_X is a k'-sparse pmf with associated mapping f' described by (84). Additional details of the specific k'-sparse pmf chosen by the user are provided in Appendix C.

Hence, when $l > \left\lfloor \frac{k}{2} \right\rfloor$, we get (33) along with (35), (36) from (87), (99), (100) upon recalling (57), (60) and (84).

Finally, in both cases $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ and $l > \left\lfloor \frac{k}{2} \right\rfloor$, (37) follows from (34) - (36) and (26); in particular, in the former case, observe in (34) that

$$l\left(\frac{1 - l\rho}{\left\lfloor \frac{k}{l} \right\rfloor l - l}\right) = l\left(\frac{1 - l\rho}{k - l' - l}\right), \quad \text{by (57)}$$
$$\leq l\rho, \quad \text{by (121) (in Appendix C).}$$

Also, (38) is immediate from (33) and (37). ■

V. Discussion

A minimum level of distribution ρ-privacy equal to worst-case privacy $\omega(\rho)$, $0 \leq \rho \leq 1$, is guaranteed by Theorem 3 since $\pi_n(\rho) \geq \omega(\rho)$ for every $n \geq 1$, with $\omega(\rho)$ being achievable. Under Assumption (15), $\omega(\rho) = \log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|$, where l is determined by ρ (see (14)). For low recoverability, i.e., $\rho \leq 1/k$, the user can pick a ρ-QR $W : \mathcal{X} \rightarrow \mathcal{Z}$ with all entries $= 1/k$, which renders $P_X W$ to be the uniform pmf on $\mathcal{Z}$ for any P_X. Clearly, the querier's best estimate for P_X is the uniform pmf on $\mathcal{X}$, with a resulting distribution ρ-privacy of $\log r$, which also equals $\omega(\rho)$ for $\rho \leq 1/k$. On the other hand, for high recoverability, i.e., $\rho > 0.5$, for the user's choice of any pmf P_X and ρ-QR W, standard estimation methods show that the querier can estimate exactly $P_X\left(f^{-1}\right)$ in Δ_k (see (13)) from Z^n as $n \rightarrow \infty$. Then, for $\rho > 0.5$, distribution ρ-privacy informally equals $\inf_{g:\Delta_k \rightarrow \Delta_r} \sup_{P_X \in \Delta_r} D\left(P_X \middle\| g\left(P_X\left(f^{-1}\right)\right)\right)$, where g is an "estimator" of P_X on the basis of $P_X\left(f^{-1}\right)$. It is shown in Appendix D that

$$\inf_{g:\Delta_k \rightarrow \Delta_r} \sup_{P_X \in \Delta_r} D\left(P_X \middle\| g\left(P_X\left(f^{-1}\right)\right)\right) = \max_{j \in \mathcal{Z}} \log\left|f^{-1}(j)\right| \tag{101}$$

thereby explaining the value of $\omega(\rho)$ for $\rho > 0.5$ in (14) with $l = 1$. Intermediate increasing values of ρ in $(1/k, 0.5]$ give $\omega(\rho) = \log \sum_{j=0}^{l-1} \left|f^{-1}(j)\right|$ with l decreasing from $k - 1$ to 2 in (14), (16).

Theorem 5 shows how achievable distribution ρ-privacy can be improved beyond worst-case privacy $\omega(\rho)$ for large and suitable but finite n. The underlying heuristic that governs appropriate user and querier strategies is as follows. Under the function ρ-recoverability constraint, the user picks a sparse pmf for the data and a locally identical ρ-QR that serve to smear the resulting pmf on $\mathcal{Z}$ to be nearly uniform, at least over a subset corresponding to the images of the largest atoms in $\mathcal{X}$ induced by f^{-1}. The querier thereby is able to recover the function value with probability at least ρ, but the attendant estimate of the data is forced to be nearly uniform over such atoms. The resulting gain in achievable distribution ρ-privacy over $\omega(\rho)$ is specified by Theorem 5.

The preceding observations show why distribution ρ-privacy defined in terms of divergence in (4) leads to useful insights in Theorems 3 and 5, complemented by the converse Theorem 4 that is valid in the practically interesting regime $\rho > 0.5$.

However, our analysis techniques suffer from shortcomings, too, suggesting room for improvement. Specifically, our approach fails to deliver a converse when $1/k < \rho \leq 0.5$ (owing to a potential noninvertibility of V^{-1} for $\rho \leq 0.5$; see Remark (ii) after Definition 6). On a related note, Theorems 3 and 4 imply that

$$\lim_n \pi_n(\rho) = \omega(\rho), \quad 0 \leq \rho \leq 1/k \ \text{ and } \ 0.5 < \rho \leq 1.$$

It remains unknown if the limit above holds also for $1/k < \rho \leq 0.5$. Next, in the proof of Theorem 5, our approach resorts to a smooth estimator for the querier (see Definition 4, especially its properties in (26)) in order to evade a divergence-borne fly in the ointment in (63)-(68). However, this raises the question of whether the converse Theorem 4, if restricted to such smooth querier's estimators, could lead to an increased upper bound than in (30), (31). This, too, remains unanswered. Furthermore, the additional restriction placed on large n in Theorem 5, as mentioned in Remark (iii) after the statement of the theorem, is a weakness. We conjecture that the ρ-QRs $W_1^{lo} : \mathcal{X} \to \mathcal{Z}$ and $W_2^{lo} : \mathcal{X} \to \mathcal{Z}$ in the proof of Theorem 5 in Section IV-C are adequate even without this restriction.

We close with a suggested framework for examining our work in the context of differential privacy and affiliated approaches to data distribution estimation [13], [22], [33], [39]. Consider a database that hosts multiple users' data that, in our setting, constitutes a data vector. Differential privacy stipulates that altering a data vector slightly leads only to a near-imperceptible change in the corresponding probability distribution of the output of the privacy mechanism, i.e., query responses that are randomized functions of data vectors. An altered formulation would seek to adhere to the function recoverability requirement and additionally guarantee differential privacy for the data vector, while simultaneously maximizing distribution privacy. The user selects the data pmf and the randomization mechanism, the latter enabling function recoverability while simultaneously being locally differentially private (ϵ-LDP) [13], [22], [33], [39]. Specifically, ϵ-LDP, $\epsilon > 0$, requires a QR $W : \mathcal{X} \to \mathcal{Z}$ to satisfy

$$\frac{W(j|x')}{W(j|x)} \le e^{\epsilon}, \qquad x, x' \in \mathcal{X}, \quad j \in \mathcal{Z}. \tag{102}$$

For each $j \in \mathcal{Z}$, ρ-recoverability in (2) and (102) with $x' \in f^{-1}(j)$ imply that

$$W(j|x) \ge \begin{cases} \rho, & x \in f^{-1}(j) \\ \frac{\rho}{e^{\epsilon}}, & x \notin f^{-1}(j). \end{cases}$$

Furthermore, we must have

$$1 = \sum_{j \in \mathcal{Z}} W(j|x) \ge \rho + (k-1)\frac{\rho}{e^{\epsilon}}, \quad x \in \mathcal{X}$$

whence

$$\rho \le \frac{1}{1 + (k-1)e^{-\epsilon}} < 1. \tag{103}$$

Thus, an ϵ-LDP QR $W : \mathcal{X} \to \mathcal{Z}$ will be a ρ-QR for ρ as in (103), implying that f cannot be ρ-recoverable for ρ violating (103). Also, it is significant that the ϵ-LDP requirement (102) would preclude the ρ-QRs used in the proofs of Theorems 3 and 5 (with zeros in the associated stochastic matrices). In effect, a characterization of distribution privacy in (5) under the additional requirement that the ρ-QR be locally differentially private of a given level, is open.

APPENDIX A
PROOFS OF LEMMAS 6 AND 7

Proof of Lemma 6: Assume first that

$$0 < \beta_j < 1 \ \text{ and } \ 0 < P(A_j) < 1, \quad j \in \mathcal{Z}.$$

Then

$$\begin{aligned} &D(P||Q) \\ &= \sum_{j \in \mathcal{Z}} \sum_{x \in A_j} P(x) \log \frac{P(x)}{\frac{\beta_j}{|A_j|}} \\ &= \sum_{j \in \mathcal{Z}} \sum_{x \in A_j} P(x) \log \frac{P(x)}{\beta_j} + \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j| \\ &= \sum_{j \in \mathcal{Z}} \sum_{x \in A_j} P(x) \log \frac{P(x)}{\beta_j} \frac{P(A_j)}{P(A_j)} + \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j| \\ &= \sum_{j \in \mathcal{Z}} \sum_{x \in A_j} P(x) \log \frac{P(x)}{P(A_j)} + \sum_{j \in \mathcal{Z}} P(A_j) \log \frac{P(A_j)}{\beta_j} \\ &+ \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j| \\ &= -\left[H(P) - H\left(P(\mathcal{A})\right)\right] + D\left(P(\mathcal{A}) \middle|\middle| \underline{\beta}\right) \\ &\qquad\qquad + \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j| \\ &\le D\left(P(\mathcal{A}) \middle|\middle| \underline{\beta}\right) + \sum_{j \in \mathcal{Z}} P(A_j) \log |A_j|. \end{aligned}$$

Equality holds above iff $H\left(P(\mathcal{A})\right) = H(P)$ which is tantamount to (40).

Next, if $P(A_j) = 0$ for some $j \in \mathcal{Z}$, the claim holds upon replacing $\sum_{j \in \mathcal{Z}}$ throughout by $\sum_{j \in \mathcal{Z}: P(A_j) \neq 0}$. Finally, if $\beta_j = 0$ for some $j \in \mathcal{Z}$, the only nontrivial case (when the right-side does not become ∞) is when $\beta_j = 0$ implies $P(A_j) = 0$; then the claim holds with the same replacement as above. ■

Proof of Lemma 7: We have

$$\begin{aligned} &D\left(P||Q\right) - D\left(P||Q_o\right) \\ &\quad = \sum_{x \in support\ (Q_o)} P(x)\ \log \frac{Q(x)}{Q_o(x)} \\ &\quad \le \sum_{x \in support\ (Q_o)} P(x) \ \left(\frac{Q(x)}{Q_o(x)} - 1\right) \\ &\quad = \sum_{x \in support\ (Q_o)} P(x) \ \left(\frac{Q(x) - Q_o(x)}{Q_o(x)}\right). \end{aligned}$$

Hence,

$$\begin{aligned} &\left|D\left(P||Q\right) - D\left(P||Q_o\right)\right| \\ &\quad \le \sum_{x \in support\ (Q_o)} \frac{P(x)}{Q_o(x)} \ \left|Q(x) - Q_o(x)\right| \\ &\quad \le \ \frac{1}{Q_o^{min}} \ \mathrm{var}\left(Q, Q_o\right) \end{aligned}$$

so that

$$-\frac{\mathrm{var}\left(Q, Q_o\right)}{Q_o^{min}} \le D\left(P||Q\right) - D\left(P||Q_o\right) \le \frac{\mathrm{var}\left(Q, Q_o\right)}{Q_o^{min}}$$

whence

$$D(P||Q) \geq D(P||Q_o) - \frac{\mathrm{var}(Q, Q_o)}{Q_o^{min}}.$$

∎

Appendix B
Proof of (55)

To establish (55), we write for any $\epsilon > 0$,

$$\begin{aligned}
&\sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}\left[\left|\Phi_n^j(\underline{\alpha}, V)\right|\right] \\
&\leq \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}\left[\left|\Phi_n^j(\underline{\alpha}, V)\right| \mathbb{1}\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| > \epsilon\right)\right] \\
&+ \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}\left[\left|\Phi_n^j(\underline{\alpha}, V)\right| \mathbb{1}\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| \leq \epsilon\right)\right] \\
&\leq \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}\left[\left|\Phi_n^j(\underline{\alpha}, V)\right| \mathbb{1}\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| > \epsilon\right)\right] + \epsilon \\
&\leq \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \log(n+k) P\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| > \epsilon\right) + \epsilon
\end{aligned} \tag{104}$$

since

$$\begin{aligned}
\left|\Phi_n^j(\underline{\alpha}, V)\right| &\leq \left|\left(\underline{\alpha}V^{-1}\right)(j) \log \frac{\left(\underline{\alpha}V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right| \\
&\leq 1.\log \frac{1}{1/(n+k)} = \log(n+k), \quad \text{by (29)}.
\end{aligned}$$

Since $\epsilon > 0$ is arbitrary, (55) will follow from (104) if for any $\epsilon > 0$,

$$\lim_n \log(n+k) \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| > \epsilon\right) = 0.$$

For $V \in \mathcal{V}(\rho)$, let ν_j denote the j^{th} column of V^{-1}, $j \in \mathcal{Z}$. Noting that $\left(\underline{\alpha}V^{-1}\right)(j) = \underline{\alpha}\nu_j$, we write

$$\begin{aligned}
&\log(n+k) \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\left|\Phi_n^j(\underline{\alpha}, V)\right| > \epsilon\right) \\
&= \log(n+k) \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\left|\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}\right| > \epsilon\right) \\
&\leq \log(n+k) \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \\
&+ \log(n+k) \\
&\quad \times \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(-\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right).
\end{aligned} \tag{105}$$

Considering the first term in the right-side above and noting by (29) that $\kappa_n(T_n)(j) \geq 1/(n+k)$, clearly the probability equals 0 if $\epsilon \geq \underline{\alpha}\nu_j \log(n+k)$ so that it suffices to consider

$$\underline{\alpha}\nu_j \log(n+k) > \epsilon \quad \text{or} \quad \underline{\alpha}\nu_j > \frac{\epsilon}{\log(n+k)}. \tag{106}$$

Then, in (105),

$$\begin{aligned}
&P\left(\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \\
&= P\left(\kappa_n(T_n)(j) < \underline{\alpha}\nu_j 2^{-\frac{\epsilon}{\underline{\alpha}\nu_j}}\right) \\
&\leq P\left(\kappa_n(T_n)(j) < \underline{\alpha}\nu_j 2^{-\epsilon}\right) \\
&\leq P\left(\widetilde{Q}(T_n)\nu_j < \underline{\alpha}\nu_j 2^{-\epsilon}\left(1 + \frac{k}{n}\right)\right), \quad \text{by (29)} \\
&\leq P\left(\left|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j\right| \geq \underline{\alpha}\nu_j\left(1 - 2^{-\epsilon}\left(1 + \frac{k}{n}\right)\right)\right) \\
&= P\left(\left|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j\right| \geq \underline{\alpha}\nu_j\left(1 - 2^{-\epsilon}\left(1 + \frac{k}{n}\right)\right)^+\right)
\end{aligned} \tag{107}$$

where $x^+ \triangleq \max\{0, x\},\ x \in \mathbb{R}$. Denote for $\underline{\alpha} \in \mathbb{R}^k,\ \|\underline{\alpha}\|_1 \triangleq \sum_{j=1}^k |\alpha_j|$; and for $V \in \mathcal{V}(\rho)$, $\left\|V^{-1}\right\|_1 \triangleq \max_{1\leq j\leq k} \|\nu_j\|_1$. Then, in (107),

$$\begin{aligned}
&\left|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j\right| \leq \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \|\nu_j\|_1 \\
&\leq \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \left\|V^{-1}\right\|_1 \leq \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \frac{k}{2\rho - 1}
\end{aligned} \tag{108}$$

since for a strictly diagonally-dominated $V \in \mathcal{V}(\rho)$, we have by [38, Theorem 1] and [28, Section 3, Theorem 1] that $\left\|V^{-1}\right\|_1 \leq k/(2\rho - 1)$, noting that $\rho > 0.5$. Furthermore,

$$\begin{aligned}
&\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \\
&\leq \left\|\widetilde{Q}(T_n) - T_n\right\|_1 + \|T_n - \underline{\alpha}\|_1 \\
&\leq \sqrt{2\ln 2}\left(\sqrt{D\left(T_n||\widetilde{Q}(T_n)\right)} + \sqrt{D\left(T_n||\alpha\right)}\right), \\
&\qquad \text{by [9, Lemma 11.6.1]} \\
&\leq 2\sqrt{2\ln 2\ D\left(T_n||\alpha\right)}, \quad \text{by (28)}.
\end{aligned} \tag{109}$$

Hence, in (107), by (108), (109),

$$\begin{aligned}
&P\left(\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \\
&\leq P\Bigg(\sqrt{D\left(T_n||\underline{\alpha}\right)} \geq \frac{(2\rho - 1)}{2k\sqrt{2\ln 2}}\underline{\alpha}\nu_j \\
&\qquad\qquad \times \left(1 - 2^{-\epsilon}\left(1 + \frac{k}{n}\right)\right)^+\Bigg) \\
&\leq P\Bigg(D\left(T_n||\underline{\alpha}\right) \geq \frac{(2\rho - 1)^2}{8k^2\ln 2}\frac{\epsilon^2}{\log^2(n+k)} \\
&\qquad\qquad \times \left(\left(1 - 2^{-\epsilon}\left(1 + \frac{k}{n}\right)\right)^+\right)^2\Bigg)
\end{aligned} \tag{110}$$

using (106). Denoting the threshold above by $\tau_1(\rho, \epsilon, n)$, straightforward manipulation yields that

$$\tau_1(\rho, \epsilon, n) \geq \frac{c_1(\rho, \epsilon)}{\log^2(n+k)} > 0$$

with

$$c_1(\rho, \epsilon) = \frac{(2\rho-1)^2\epsilon^2 c^2}{8k^2\ln 2}, \quad \left(1 - 2^{-\epsilon}(1+k)\right)^+ < c < 1 - 2^{-\epsilon}$$

for all $n \geq N_1(\epsilon, k, c) = k/\left((1-c)2^{\epsilon}-1\right)$. Then, in (110) for all $n \geq N_1(\epsilon, k, c)$, by [9, Theorem 11.2.1], the first term in the right-side of (105) is

$$\begin{aligned} &\leq \log(n+k) P\left(D\left(T_n \| \underline{\alpha}\right) \geq \frac{c_1(\rho,\epsilon)}{\log^2(n+k)}\right) \\ &\leq \log(n+k)\exp\left[-n\left(\frac{c_1(\rho,\epsilon)}{\log^2(n+k)} - k\frac{\log(n+1)}{n}\right)\right] \\ &\leq \exp\left[-\left(c_1(\rho,\epsilon)\frac{n}{\log^2(n+k)} - (k+1)\log(n+k)\right)\right] \end{aligned} \tag{111}$$

since $\log(n+k) \leq (n+k)$ whereby because

$$\lim_n \; c_1(\rho,\epsilon)\frac{n}{\log^2(n+k)} - (k+1)\log(n+k) = \infty,$$

we get

$$\begin{aligned} &\lim_n \; \log(n+k) \\ &\quad \times \sup_{V\in\mathcal{V}(\rho)} \; \sup_{\underline{\alpha}\in\Delta_k(\rho)} \; P\left(\underline{\alpha}\nu_j \log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) = 0. \end{aligned} \tag{112}$$

Turning to the second term in the right-side of (105), and considering

$$\sup_{V\in\mathcal{V}(\rho)} \; \sup_{\underline{\alpha}\in\Delta_k(V)} \; P\left(-\underline{\alpha}\nu_j \log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right),$$

note that the probability is 0 for $\epsilon \geq -\underline{\alpha}\nu_j\log\underline{\alpha}\nu_j$. Then, since $-\underline{\alpha}\nu_j\log\underline{\alpha}\nu_j \leq 0.5$, considering

$$-\underline{\alpha}\nu_j\log\underline{\alpha}\nu_j > \epsilon \quad \text{for} \quad 0<\epsilon<0.5, \tag{113}$$

we get

$$\begin{aligned} &P\left(-\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \leq P\left(\kappa_n(T_n)(j) > \underline{\alpha}\nu_j 2^{\epsilon}\right) \\ &= P\left(\widetilde{Q}(T_n)\nu_j > \underline{\alpha}\nu_j 2^{\epsilon}\left(1+\frac{k}{n}\right) - \frac{1}{n}\right) \\ &\leq P\left(\left|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j\right| \geq \underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right)-\frac{1}{n}\right) \\ &\leq P\left(\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \left\|V^{-1}\right\|_1 \right.\\ &\qquad \left. \geq \underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right)-\frac{1}{n}\right), \\ &\qquad \text{by the first inequality in (108)} \\ &\leq P\left(\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \right.\\ &\qquad \left. \geq \left(\underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right)-\frac{1}{n}\right)\frac{2\rho-1}{k}\right), \\ &\qquad \text{by the last inequality in (108)} \\ &\leq P\left(\sqrt{D\left(T_n\|\underline{\alpha}\right)} \right.\\ &\qquad \left. \geq \frac{(2\rho-1)}{2k\sqrt{2\ln 2}}\left(t^*(\epsilon)\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right)-\frac{1}{n}\right)^+\right), \\ &\qquad \text{by (109) and (113)} \end{aligned} \tag{114}$$

$$\begin{aligned} &= P\left(D\left(T_n\|\underline{\alpha}\right) \right.\\ &\qquad \left. \geq \frac{(2\rho-1)^2}{8k^2\ln 2}\left(\left(t^*(\epsilon)\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right)-\frac{1}{n}\right)^+\right)^2\right) \end{aligned} \tag{115}$$

where $t^*(\epsilon)$ in (114) is the solution of $-t\log t = \epsilon$ for $t \in [0, 0.5)$. Denoting by $\tau_2(\rho,\epsilon,n)$ the threshold in (115), we observe that $\tau_2(\rho,\epsilon,n) \geq c_2(\rho,\epsilon) > 0$ with

$$c_2(\rho,\epsilon) = \frac{(2\rho-1)^2 d^2}{8k^2\ln 2}, \quad 0<d<t^*(\epsilon)\left(2^{\epsilon}-1\right)$$

for all $n \geq N_2(\epsilon,k,d) = \left(1-kt^*(\epsilon)2^{\epsilon}\right)^+ / \left(t^*(\epsilon)\left(2^{\epsilon}-1\right)-d\right)$. Then, bounding above the second term in (105) upon treating the probability in (115) in the manner of (111), and observing that

$$\lim_n \; c_2(\rho,\epsilon)n - (k+1)\log(n+k) = \infty,$$

we have

$$\begin{aligned} &\lim_n \; \log(n+k) \\ &\quad \times \sup_{V\in\mathcal{V}(\rho)} \; \sup_{\underline{\alpha}\in\Delta_k(V)} \; P\left(-\underline{\alpha}\nu_j \log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) = 0. \end{aligned} \tag{116}$$

Upon combining (112) and (116), we get (55).

Appendix C
Lower Bound for (86), (98) and Proof of (66), (67)

Lower bound for (86):

We first bound (86) below by restricting the supremum further according to

$$\begin{aligned} &\inf_{\widehat{P}_n^{\beta(n)}\in\mathcal{S}_n(k')} \; \sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ \underline{\alpha}(j')=0,\; j'=k'-l',\ldots,k'-1}} \\ &\sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \\ &\times \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{\left|f'^{-1}(j')\right|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)}\right) \\ &\geq \inf_{\widehat{P}_n^{\beta(n)}\in\mathcal{S}_n(k')} \\ &\qquad \sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ l\left(\frac{1-l\rho}{k-l'-l}\right)\leq\underline{\alpha}(j')\leq\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\; l\rho\right\},\; j'=1,\ldots,k'-l'-1 \\ \underline{\alpha}(j')=0,\; j'=k'-l',\ldots,k'-1}} \end{aligned}$$

$$\sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \times \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{\left|f'^{-1}(j')\right|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)}\right). \tag{117}$$

Observe from (65) that $Q'^{(n)}(\underline{\alpha}) \in \mathcal{Q}'^{(n)}$ is the same for all $\underline{\alpha} \in \Delta_{k'}$ satisfying the constraints in the right-side of (117). Hence, with

$$\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right) = \beta_{j'}, \qquad j' \in \mathcal{Z}',$$

for some $\underline{\beta} = \{\beta_0, \beta_1, \ldots, \beta_{k'-1}\} \in \Delta_{k'}$, the right-side of (117)

$$\geq \inf_{\underline{\beta}\in\Delta_{k'}} \sup_{\underline{\alpha}\in\Delta_{k'}\sim\text{right-side of (117)}} \left\{ \sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \times \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}}\right)\right\}. \tag{118}$$

For each fixed $\underline{\beta} \in \Delta_{k'}$, we further bound below the expression in (118) by limiting the supremum to a maximum over a finite set $\{\underline{\alpha}_t : t = 1, \ldots, k'-l'\}$ made up of $k'-l' = \left\lfloor \frac{k}{l} \right\rfloor \geq 2$ elements (see (58), (59)) specified by

$$\underline{\alpha}_1 = \left(l\rho, l\left(\frac{1-l\rho}{k-l'-l}\right), \ldots, l\left(\frac{1-l\rho}{k-l'-l}\right), 0, \ldots, 0\right) \tag{119}$$

with $k'-l'$ nonzero elements; and for $t = 2, \ldots, k'-l'$, $\underline{\alpha}_t = (\underline{\alpha}_t(0), \underline{\alpha}_t(1), \ldots, \underline{\alpha}_t(k'-1))$ specified by

$$\underline{\alpha}_t(j') = \begin{cases} l\rho - \left(\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)\right), & j' = 0 \\ l\left(\frac{1-l\rho}{k-l'-l}\right), & j' = 1, \ldots, t-2, t, \ldots, k'-l'-1 \\ \min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\}, & j' = t-1 \\ 0, & j' \geq k'-l'. \end{cases} \tag{120}$$

A description of the $k'-l'-1$ values above is as follows: For $t = 2, \ldots, k'-l'$, $\underline{\alpha}_t(t-1) = \min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\}$, $\underline{\alpha}_t(1) = \cdots = \underline{\alpha}_t(t-2) = \underline{\alpha}_t(t) = \cdots = \underline{\alpha}_t(k'-l'-1) = l\left(\frac{1-l\rho}{k-l'-l}\right)$ and $\underline{\alpha}_t(j') = 0,\ j' \geq k'-l'$. We now check that when $\underline{\alpha}$ is from the set $\{\underline{\alpha}_t : t = 1, \ldots, k'-l'\}$, the coefficients of the log terms in (118), i.e., the right-side of (80) under (119), (120), take values in $[0, 1]$. For this, it suffices to verify that $l\left(\frac{1-l\rho}{k-l'-l}\right) \leq \underline{\alpha}_t(0) \leq l\rho,\ t = 2, \ldots, k'-l'$. Observe that

$$l\left(\frac{1-l\rho}{k-l'-l}\right) \leq l\frac{(1-l\rho)}{l}, \quad \text{since from (58), } k-l'-l \geq l$$
$$\leq l\rho, \quad \text{using } l\rho \geq l/(l+1) \geq 1/2 \text{ from (56)}, \tag{121}$$

so that $\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n}, l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right) \geq 0$. Therefore,

$$\underline{\alpha}_t(0) = l\rho - \left(\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n}, l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)\right) \leq l\rho, \qquad t = 2, \ldots, k'-l',$$

and

$$\begin{aligned}\underline{\alpha}_t(0) &= l\rho - \left(\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n}, l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)\right) \\ &\geq l\rho - \left(l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)\right) \\ &= l\left(\frac{1-l\rho}{k-l'-l}\right), \qquad t = 2, \ldots, k'-l'.\end{aligned}$$

This completes the verification.

Now set

$$\mu_n \triangleq \frac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)}. \tag{122}$$

Then the supremum in (118) reduces to a maximum over $k'-l'$ choices of $\underline{\alpha}_t,\ t = 1, \ldots, k'-l'$, given by (119), (120). Then, with μ_n as in (122), the right-side of (118) is bounded below as

$$\geq \inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{\log\frac{\left|f'^{-1}(0)\right|}{\beta_0},\ \mu_n \log\left(\mu_n\frac{\left|f'^{-1}(1)\right|}{\beta_1}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right), \ldots, \mu_n \log\left(\mu_n\frac{\left|f'^{-1}(k'-l'-1)\right|}{\beta_{k'-l'-1}}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right)\right\} \tag{123}$$

where the tth term, $1 \leq t \leq k'-l'$ is obtained by evaluating the expression within $\{\cdot\}$ in (118) at $\underline{\alpha}_t$. Moreover, the right-side of (123) is

$$= \inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{\log\frac{\left|f'^{-1}(0)\right|}{\beta_0},\ \max_{1\leq j'\leq k'-l'-1}\left\{\mu_n\log\left(\mu_n\frac{\left|f'^{-1}(j')\right|}{\beta_{j'}}\right)\right.\right.$$

$$+ (1-\mu_n)\log\left((1-\mu_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right)\Bigg\}\Bigg\}. \tag{124}$$

Hence, for the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$, the user-selected pmf P_X is one among a set of $k'-l'$ k'-sparse pmfs with associated mapping f' (84) and $P_X\left(f'^{-1}\right) = \underline{\alpha}_t,\ t = 1,\ldots,k'-l'$.

Since for each $\underline{\beta} \in \Delta_{k'}$, $\beta_{k'-l'},\ldots,\beta_{k'-1}$ do not appear in (124), it is sufficient to consider $\underline{\beta} \in \Delta_{k'}$ such that

$$\beta_{k'-l'} = \cdots = \beta_{k'-1} = 0. \tag{125}$$

For every $0 \leq \beta_0 \leq 1$, we solve the inner $\inf\ \max$ in (124), which, using (125), is equivalent to

$$\inf_{\substack{\beta_1,\ldots,\beta_{k'-l'-1}:\\ \beta_{j'}\geq 0,\ j'=1,\ldots,k'-l'-1\\ \sum_{j'=1}^{k'-l'-1}\beta_{j'}=1-\beta_0}} \max_{1\leq j'\leq k'-l'-1} \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}}. \tag{126}$$

We claim that

$$\max_{1\leq j'\leq k'-l'-1} \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}} \geq \frac{\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|}{1-\beta_0} \tag{127}$$

since, if

$$\max_{1\leq j'\leq k'-l'-1} \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}} < \frac{\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|}{1-\beta_0}$$

$$\text{i.e., } \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}} < \frac{\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|}{1-\beta_0},\quad j'=1,\ldots,k'-l'-1$$

$$\left|f'^{-1}(j')\right| < \frac{\beta_{j'}}{1-\beta_0}\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|,\quad j'=1,\ldots,k'-l'-1,$$

and by summing over $j' = 1,\ldots,k'-l'-1$ on both sides

$$\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right| < \frac{\sum_{j'=1}^{k'-l'-1}\beta_{j'}}{1-\beta_0}\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right| = \sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|$$

which is a contradiction. Also, by choosing

$$\beta_{j'} = \frac{\left|f'^{-1}(j')\right|}{\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|}(1-\beta_0),\quad j'=1,\ldots,k'-l'-1,$$

we get

$$\inf_{\substack{\beta_1,\ldots,\beta_{k'-l'-1}:\\ \beta_{j'}\geq 0,\ j'=1,\ldots,k'-l'-1\\ \sum_{j'=1}^{k'-l'-1}\beta_{j'}=1-\beta_0}} \max_{1\leq j'\leq k'-l'-1} \frac{\left|f'^{-1}(j')\right|}{\beta_{j'}} \leq \frac{\sum_{j''=1}^{k'-l'-1}\left|f'^{-1}(j'')\right|}{1-\beta_0}. \tag{128}$$

Thus, the expression in (126) equals the (common) right-sides of (127), (128), using which the lower bound in (124) becomes

$$\inf_{0\leq\beta_0\leq 1}\max\Bigg\{\log\frac{\left|f'^{-1}(0)\right|}{\beta_0},\ \mu_n\log\left(\mu_n\frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{1-\beta_0}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right)\Bigg\}. \tag{129}$$

The first term in (129) is decreasing in $0 \leq \beta_0 \leq 1$ and the second term is convex in $0 \leq \beta_0 \leq 1$ since it can be written as

$$D\left(\text{Ber}(\mu_n)||\text{Ber}(1-\beta_0)\right) + \mu_n\log\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right| + (1-\mu_n)\log\left|f'^{-1}(0)\right| \tag{130}$$

with the minimum being attained at $\beta_0 = \beta_0' \triangleq 1-\mu_n$. Straightforward but tedious calculations show that the terms intersect exactly once at

$$\beta_0 = \beta_0'' \triangleq \left(1 + \frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}}\mu_n\right)^{-1},$$

and[7] the first term is larger than the second when $\beta_0 < \beta_0''$ and smaller when $\beta_0 > \beta_0''$. We now distinguish between the cases $\left|f'^{-1}(0)\right| \geq \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|$ and $\left|f'^{-1}(0)\right| < \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|$.

(i) $\left|f'^{-1}(0)\right| \geq \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|$: It holds that

$$\beta_0'' \geq \beta_0'$$

i.e.,

$$\left(1 + \frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}}\mu_n\right)^{-1} \geq 1-\mu_n$$

which is

$$\left|f'^{-1}(0)\right| \geq \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|(1-\mu_n)^{\frac{1}{\mu_n}}$$

[7]When $\mu_n = 0,\ \beta_0'' = 1$.

because $(1-\mu_n)^{\frac{1}{\mu_n}} \le 1$ and $\left|f'^{-1}(0)\right| \ge \sum_{j'=1}^{k'-l'-1} \left|f'^{-1}(j')\right|$. Then $\inf_{0\le\beta_0\le 1}$ in (129) is attained as a minimum at $\beta_0 = \beta_0''$, and becomes

$$\log\left|f'^{-1}(0)\right| + \log\left(1 + \frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}}\mu_n\right), \quad (131)$$

with μ_n as in (122).

(ii) $\left|f'^{-1}(0)\right| < \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|$: We have that (129) is bounded below as

$$\ge \inf_{0\le\beta_0\le 1} D\left(\mathrm{Ber}(1-\mu_n)||\mathrm{Ber}(\beta_0)\right) + \mu_n \log \sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right| + (1-\mu_n)\log\left|f'^{-1}(0)\right|$$
$$= \log\left|f'^{-1}(0)\right| + \mu_n \log \frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}. \quad (132)$$

Note that the second $\log$ term in (132) is positive.

From (131) along with the observation that $(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}} \ge 1/e$ and (132), we obtain the desired lower bound for (86) which along with (79) and (122) gives (87), (88), (89).

Lower bound for (98)*:*

Turning next to the task of bounding (98) below, we have

$$\inf_{\widehat{P}_n^{\beta^{(n)}}\in\mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ \underline{\alpha}(j')=0,\ j'=2,\dots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \times \log\left(\frac{\underline{\alpha}(0)}{l\rho}\frac{\left|f'^{-1}(0)\right|}{\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(0)\right)}\right)$$
$$+ \frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho} \times \log\left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\frac{\left|f'^{-1}(1)\right|}{\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(1)\right)}\right)$$
$$\ge \inf_{\widehat{P}_n^{\beta^{(n)}}\in\mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ 1-l\rho\le\underline{\alpha}(1)\le\frac{\lceil n(1-l\rho)\rceil}{n}\\ \underline{\alpha}(j')=0,\ j'=2,\dots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \times \log\left(\frac{\underline{\alpha}(0)}{l\rho}\frac{\left|f'^{-1}(0)\right|}{\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(0)\right)}\right)$$
$$+ \frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho} \times \log\left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\frac{\left|f'^{-1}(1)\right|}{\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(1)\right)}\right). \quad (133)$$

In this case, too, observe from (65) that $Q'^{(n)}(\underline{\alpha}) \in \mathcal{Q}'^{(n)}$ remains unchanged for all $\underline{\alpha}\in\Delta_{k'}$ satisfying the constraints in the right-side of (133). Hence, with

$$\widehat{P}_n^{\beta^{(n)}}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right) = \beta_{j'}, \qquad j'\in\mathcal{Z}',$$

for some $\underline{\beta} = \{\beta_0,\beta_1,\dots,\beta_{k'-1}\} \in \Delta_{k'}$, the right-side of (133)

$$\ge \inf_{\underline{\beta}\in\Delta_{k'}} \sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ 1-l\rho\le\underline{\alpha}(1)\le\frac{\lceil n(1-l\rho)\rceil}{n}\\ \underline{\alpha}(j')=0,\ j'=2,\dots,k'-1}} \left\{\frac{\underline{\alpha}(0)}{l\rho}\log\left(\frac{\underline{\alpha}(0)}{l\rho}\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right) + \frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\log\left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\frac{\left|f'^{-1}(1)\right|}{\beta_1}\right)\right\}. \quad (134)$$

We further bound (134) below by replacing the supremum by a maximum of the expression within $\{\cdot\}$ in (134) evaluated at two points $\underline{\alpha}_1, \underline{\alpha}_2$ given by

$$\underline{\alpha}_1 = (l\rho, 1-l\rho, 0, \dots, 0)$$
$$\underline{\alpha}_2 = \left(1-\frac{\lceil n(1-l\rho)\rceil}{n}, \frac{\lceil n(1-l\rho)\rceil}{n}, 0, \dots, 0\right). \quad (135)$$

When $\underline{\alpha} = \underline{\alpha}_1$, the coefficients of the $\log$ terms in (134) are in $[0,1]$; and when $\underline{\alpha} = \underline{\alpha}_2$, the same holds upon observing that $0 \le \underline{\alpha}_2(0) \le l\rho$. Then with

$$\theta_n = \frac{\frac{\lceil n(1-l\rho)\rceil}{n} - (1-l\rho)}{l\rho}, \quad (136)$$

the expression in (134) is bounded below by

$$\inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{\log\frac{\left|f'^{-1}(0)\right|}{\beta_0}, \theta_n\log\left(\theta_n\frac{\left|f'^{-1}(1)\right|}{\beta_1}\right) + (1-\theta_n)\log\left((1-\theta_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right)\right\}, \quad (137)$$

where the two terms within $\{\cdot\}$ in (137) are obtained by evaluating the term within $\{\cdot\}$ in (134) at $\underline{\alpha}_1$ and $\underline{\alpha}_2$, respectively. Hence, for the case $l > \left\lfloor\frac{k}{2}\right\rfloor$, the user-selected pmf P_X is one among two k'-sparse pmfs with associated mapping f' (84) and $P_X\left(f'^{-1}\right) = \underline{\alpha}_t,\ t=1,2$.

For every $\underline{\beta}\in\Delta_{k'},\ \beta_2,\dots,\beta_{k'-1}$ do not appear in (137), so that it suffices to consider $\underline{\beta}\in\Delta_{k'}$ that satisfies

$$\beta_2 = \cdots = \beta_{k'-1} = 0$$

whereby (137) becomes

$$\inf_{0\le\beta_0\le 1} \max\left\{\log\frac{\left|f'^{-1}(0)\right|}{\beta_0}, \theta_n\log\left(\theta_n\frac{\left|f'^{-1}(1)\right|}{1-\beta_0}\right) + (1-\theta_n)\log\left((1-\theta_n)\frac{\left|f'^{-1}(0)\right|}{\beta_0}\right)\right\}. \quad (138)$$

Observe that (138) is the same as (129) with μ_n replaced by θ_n and $\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|$ by $\left|f'^{-1}(1)\right|$. Since, by the assumption in (15), $\left|f'^{-1}(0)\right| \geq \left|f'^{-1}(1)\right|$, applying the same steps from (129) - (131) for the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ and $\left|f'^{-1}(0)\right| \geq \sum_{j'=1}^{k'-l'-1} \left|f'^{-1}(j')\right|$, we get that (138) equals

$$\log\left|f'^{-1}(0)\right| + \log\left(1 + \frac{\left|f'^{-1}(1)\right|}{\left|f'^{-1}(0)\right|}(1-\theta_n)^{\frac{1-\theta_n}{\theta_n}}\theta_n\right). \quad (139)$$

From[8] (139) and the fact that $(1-\theta_n)^{\frac{1-\theta_n}{\theta_n}} \geq 1/e$, we get the desired lower bound for (98) which along with (91) and (136) gives (87), (99), (100).

Proof of (66), (67)*:*

To show (66), (67) for the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$, we have from (119), (120) that

$$\begin{aligned}
&\min_{t=1,\ldots,k'-l'} \underline{\alpha}_t(0) \\
&= l\rho - \left(\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\ l\rho\right\} - l\left(\frac{1-l\rho}{k-l'-l}\right)\right) \\
&\geq l\rho - \left(\frac{\left\lfloor nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rfloor}{n} - l\left(\frac{1-l\rho}{k-l'-l}\right)\right) \\
&\geq l\rho - \frac{1}{n} \geq \frac{1}{2} - \frac{1}{n} \quad \text{since from (56), } l\rho \geq \frac{l}{l+1} \geq \frac{1}{2},
\end{aligned}$$

so that the last inequality in (66) holds if

$$\frac{1}{2} - \frac{1}{n} - \frac{k'-1}{n} = \frac{1}{2} - \frac{k'}{n} \geq 0 \quad \text{i.e.,} \quad n \geq N_0(k') = 2k'. \tag{140}$$

Next, for the case $l > \left\lfloor \frac{k}{2} \right\rfloor$, from (135),

$$\begin{aligned}
\min_{t=1,2} \underline{\alpha}_t(0) &= 1 - \frac{\lceil n(1-l\rho)\rceil}{n} \\
&\geq 1 - \frac{n(1-l\rho)+1}{n} = l\rho - \frac{1}{n} \geq \frac{1}{2} - \frac{1}{n}
\end{aligned}$$

and, in this case too, (140) holds. ■

Appendix D
Proof of (101)

First, choosing $g : \Delta_k \to \Delta_r$ given by

$$g\left(P_X\left(f^{-1}\right)\right)(x) = \frac{P_X\left(f^{-1}(j)\right)}{\left|f^{-1}(j)\right|}, \quad x \in f^{-1}(j), \quad j \in \mathcal{Z},$$

the left-side of (101) is maximized by P_X being a point-mass on any $x \in f^{-1}(0)$. Then, (101) holds with "$\leq$."

Next, the reverse inequality "$\geq$" in (101) obtains from mimicking the steps in (22) with $l = 1$. ■

Acknowledgment

The authors are grateful to: Peter Kairouz, Himanshu Tyagi, and Shun Watanabe for their helpful critique of our problem formulation; Lorenzo Finesso for his informative pointers that led to Remark (ii) after Definition 6; and the anonymous referees and associate editor for their thoughtful comments which led to material improvements in presentation.

[8]When $\theta_n = 0$, the expression in (139) reduces to $\log\left|f^{-1}(0)\right|$.

References

[1] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Information extraction under privacy constraints," *Information*, vol. 7, no. 1, p. 15, 2016.

[2] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Estimation efficiency under privacy constraints," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1512–1534, Mar. 2019.

[3] R. Bassily and A. Smith, "Local, private, efficient protocols for succinct histograms," in *Proc. 47th Annu. ACM Symp. Theory Comput.*, Jun. 2015, pp. 127–135.

[4] D. Braess, J. Forster, T. Sauer, and H. U. Simon, "How to achieve minimax expected Kullback–Leibler distance from an unknown finite distribution," in *Proc. Int. Conf. Algorithmic Learn. Theory*, Nov. 2002, pp. 380–394.

[5] D. Braess and T. Sauer, "Bernstein polynomials and learning theory," *J. Approximation Theory*, vol. 128, no. 2, pp. 187–206, Jun. 2004.

[6] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1401–1408.

[7] T. H. Chan, M. Li, E. Shi, and W. Xu, "Differentially private continual monitoring of heavy hitters from distributed streams," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, Jul. 2012, pp. 140–159.

[8] T. M. Cover, "Admissibility properties or Gilbert's encoding for unknown source probabilities (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 216–217, Jan. 1972.

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.

[10] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[11] I. Csiszár and P. C. Shields, "Information theory and statistics: A tutorial," *Found. Trends Commun. Inf. Theory*, vol. 1, no. 4, pp. 417–528, 2004.

[12] L. Devroye, "The equivalence of weak, strong and complete convergence in L_1 for kernel density estimates," *Ann. Statist.*, vol. 11, no. 3, pp. 896–904, Dec. 1984.

[13] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Minimax optimal procedures for locally private estimation," *J. Amer. Stat. Assoc.*, vol. 113, no. 521, pp. 182–201, May 2018.

[14] G. T. Duncan and D. Lambert, "Disclosure-limited data dissemination," *J. Amer. Stat. Assoc.*, vol. 81, no. 393, pp. 25–27, Mar. 1986.

[15] C. Dwork, "Differential privacy," in *Proc. Int. Colloq. Automata, Lang. Program.*, Jul. 2006, pp. 1–12.

[16] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.*, Mar. 2006, pp. 265–284.

[17] S. E. Fienberg, U. E. Makov, and R. J. Steele, "Disclosure limitation using perturbation and related methods for categorical data," *J. Off. Statist.*, vol. 14, no. 4, pp. 485–502, Dec. 1998.

[18] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 925–951, Feb. 2016.

[19] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proc. 42nd ACM Symp. Theory Comput.*, Jun. 2010, pp. 705–714.

[20] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Context-aware generative adversarial privacy," *Entropy*, vol. 19, no. 12, p. 656, Dec. 2017.

[21] J. Hsu, S. Khanna, and A. Roth, "Distributed private heavy hitters," in *Automata, Languages, and Programming*. Jul. 2012, pp. 461–472.

[22] P. Kairouz, K. Bonawitz, and D. Ramage, "Discrete distribution estimation under local privacy," in *Proc. Int. Conf. Mach. Learn.*, Jun. 2016, pp. 2436–2444.

[23] S. Kamath, A. Orlitsky, V. Pichapati, and T. A. Suresh, "On learning distributions from their samples," in *Proc. Conf. Learn. Theory*, Jul. 2015, pp. 1066–1100.

[24] R. Krichevsky and V. Trofimov, "The performance of universal encoding," *IEEE Trans. Inf. Theory*, vol. 27, no. 2, pp. 199–207, Mar. 1981.

[25] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "Privacy under hard distortion constraints," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.

[26] A. Makhdoumi and N. Fawaz, "Privacy-utility tradeoff under statistical uncertainty," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 1627–1634.

[27] B. Michele and A. Karpow, "Watch and be watched: Compromising all smart TV generations," in *Proc. IEEE 11th Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2014, pp. 351–356.

[28] N. Morača, "Bounds for norms of the matrix inverse and the smallest singular value," *Linear Algebra Appl.*, vol. 429, no. 10, pp. 2589–2601, Nov. 2008.

[29] A. Nageswaran and P. Narayan, "Data privacy for a ρ-recoverable function," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3470–3488, Jun. 2019.

[30] A. Nageswaran and P. Narayan, "Distribution privacy under function recoverability," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 890–895.

[31] A. Nageswaran and P. Narayan, "Distribution privacy under function ρ-recoverability," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 3332–3337.

[32] L. Paninski, "Variational minimax estimation of discrete distributions under KL loss," in *Proc. Adv. Neural Inf. Process. Syst.*, Dec. 2004, pp. 1033–1040.

[33] A. Pastore and M. Gastpar, "Locally differentially-private randomized response for discrete distribution learning," *J. Mach. Learn. Res.*, vol. 22, pp. 1–56, Jul. 2021.

[34] A. R. Rao and P. Bhimasankaram, *Linear Algebra*, 2nd ed. New Delhi, India: Hindustan Book Agency, 2000.

[35] D. Rebollo-Monedero, J. Forne, and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 11, pp. 1623–1636, Nov. 2010.

[36] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[37] A. Smith, "Privacy-preserving statistical estimation with optimal convergence rates," in *Proc. 43rd Annu. ACM Symp. Theory Comput. (STOC)*, 2011, pp. 813–822.

[38] J. M. Varah, "A lower bound for the smallest singular value of a matrix," *Linear Algebra Appl.*, vol. 11, no. 1, pp. 3–5, 1975.

[39] M. Ye and A. Barg, "Optimal schemes for discrete distribution estimation under locally differential privacy," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5662–5676, Aug. 2018.

Ajaykrishnan Nageswaran received the B.Tech. degree in electronics and communication engineering from the National Institute of Technology Karnataka, India, in 2015. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Maryland, College Park.

Prakash Narayan (Life Fellow, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology Madras in 1976, and the M.S. degree in systems science and mathematics and the D.Sc. degree in electrical engineering from Washington University in St. Louis, MO, USA, in 1978 and 1981, respectively.

He is currently a Professor of electrical and computer engineering at the University of Maryland, College Park, with a joint appointment at the Institute for Systems Research. His research interests are in multiuser information theory, communication theory, communication networks, cryptography, and applied probability and statistics.