ABSTRACT

Title of dissertation: Data and Distribution Privacy Under Function Recoverability

Ajaykrishnan Nageswaran, Doctor of Philosophy, 2023

Dissertation directed by: Professor Prakash Narayan
Department of Electrical and Computer Engineering
Institute for Systems Research

Many data-driven applications entail function computation based on user data, with accompanying requirements of data privacy. In such an application, a user holding data must publicly furnish accurate attributes of the data (function recoverability or utility) while simultaneously protecting the data or the data-generating mechanism (privacy). Two broad formulations of function computation with privacy are considered: "data privacy" which requires that data or a sensitive attribute of it be protected; and "distribution privacy" in which the workings of an underlying data-generating algorithm must remain under wraps.

The concept of differential privacy rules the data privacy landscape. Our new approach can be viewed as a complement. It enables exact characterizations of optimal utility versus privacy performance tradeoffs, and specifies explicit randomized privacy mechanisms for attaining them.

We consider the following set of problems in the data privacy category. A user's data is represented by a finite-valued random variable. Given a function of the data, a querier is required to recover, with at least a prescribed probability, the value of the function on the basis of a query

response provided by the user. The user devises the query response, subject to the recoverability condition, so as to maximize privacy of the data from the querier. Privacy is measured by the probability of error incurred by the querier in estimating the data from the query response. We analyze single and multiple independent query responses, with each response satisfying the recoverability requirement, which provide maximum privacy to the user. In the former setting, we also consider privacy for a predicate of the user's data. Achievability schemes that constitute explicit randomization mechanisms for query responses are given, and their privacy compared with converse upper bounds.

Under the same recoverability constraint, we introduce a more demanding measure of privacy: list privacy, measured by the probability that the user data is not contained in a list formed by the querier based on the query response. We obtain a general converse upper bound for the maximum list privacy which is shown to be tight for the special case of a binary-valued function.

In another line of work, we consider analog user data represented by a Gaussian random variable. Given a linear function of the data, a querier is required to recover, with at least a specified accuracy level, the function value from a query response obtained from the user. The user devises the query response, subject to the recoverability requirement, so as to maximize privacy of the data from the querier. Both recoverability and privacy are measured by ℓ_2-distance criteria. An exact characterization of maximum user data privacy under the recoverability condition is derived. An explicit optimal privacy mechanism for the user is given whose privacy is shown to match a converse upper bound.

Finally, turning to distribution privacy, a user generates n independent and identically distributed data random variables with a probability mass function (a stand-in for a data-generating

probabilistic algorithm) that must be guarded from a querier. The querier must recover, with a prescribed accuracy, a given function of the data from each of the n 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. A basic achievable lower bound for distribution privacy is provided that does not depend on n and corresponds to worst-case privacy. Next, upper and lower 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 bring out explicit strategies for the user and the querier.

A special feature of all our optimal privacy mechanisms throughout this dissertation is that they are of the "add-noise" variety and afford ready implementability. Specifically, the user designs a query response by adding to the function value an appropriate value-dependent noise.

Data and Distribution Privacy Under Function Recoverability

by

Ajaykrishnan Nageswaran

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2023

Advisory Committee:
Professor Prakash Narayan, Chair/Advisor
Professor Alexander Barg
Professor Sennur Ulukus
Professor Nuno Miguel L. C. Martins
Professor Aravind Srinivasan

Acknowledgments

I would like to express my deepest and most sincere gratitude to my advisor Prof. Prakash Narayan for his continuous support and unrelenting patience throughout my Ph. D. I have learned from him not only the skills necessary to do research but also critical thinking and professional attitude necessary to succeed in life. I gratefully thank him for his guidance, care and advice.

This dissertation could not have been completed without the generous support of U. S. National Science Foundation under the grant CCF 1527354.

I am indebted to Himanshu Tyagi and Shun Watanabe for educating me and Prof. Prakash Narayan in private function computation, helping formulate the models in this dissertation, and for numerous beneficial discussions that informed our approach. I am also grateful to Prof. Adam Smith for raising the question of predicate privacy in this work. I would like to thank my labmates Praneeth Boda, Yi-Peng Wei, Ahmed Arafa, Karim Banawan, Baturalp Buyukates, Melih Bastopcu and Sagnik Bhattacharya for the many fun and thought-provoking discussions.

My time at the University of Maryland would not have been so much memorable without Karthik, Hari, Shravan, Yogesh, Navaneeth, Chinmay and other innumerable friends who made Maryland my home away from home. I am eternally grateful to my sister, Sweatha, and brother-in-law, Ashwin, for their encouragement over the years. Last and the most, I thank my parents for their unconditional love and support throughout.

Table of Contents

Chapter 1: Introduction

1.1. Motivation

Various applications in social media and healthcare involve releasing information regarding a database that hosts users' data, such as user demographics or success rates in clinical drug trial records. An important goal is to preserve and enhance user *data privacy* while ensuring high accuracy of the information released to a consumer.

A different consideration arises when data is governed by an underlying probability distribution or generating mechanism, and aggregate information regarding the data has to be released. An important objective is to protect the data-generating distribution or mechanism, i.e., maximize *distribution privacy*, while guaranteeing recoverability of the released information with high accuracy. Potential futuristic applications include: an AI-driven financial trader who reveals trading preferences through daily actions (recoverability) 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).

We develop a new analytical approach involving a general framework for cooperative function recovery while maximizing individual data or distribution privacy. In our basic model, a querier, typically a consumer of information, seeks a desired function of a statistical database

with the cooperation of the database user who simultaneously endeavors to maximize data or distribution privacy. In this dissertation, for the two categories of problems above, we investigate fundamental tradeoffs that arise between accuracy of function computation and privacy. We study the following broad questions.

- What are appropriate metrics for data or distribution privacy and accuracy of function recovery?
- For various measures of privacy and accuracy of recovery, what are the exact tradeoffs between them?
- What are appropriate release mechanisms, i.e., responses to the querier, that maximize data or distribution privacy while meeting the accuracy requirement?

1.2. Prior Work

In data privacy, an important movement that has commanded dominant attention over the years is differential privacy, introduced in [26], [27] and explored further in [49], [9], [6], [45], [50] among others. Consider a data vector that represents multiple users' data. The notion of differential privacy requires that altering a data vector slightly leads only to a near-imperceptible change in the corresponding probability distribution of the output of the data release mechanism, which is a randomized function of the data vector. Upon imposing a differential privacy constraint, there exists a large body of work that seeks to maximize function recoverability by minimizing a discrepancy cost between function value and randomized query response, a representative sample is [35], [68], [7], [34], [33]. In contrast, our work will involve maximizing privacy under a constraint on recoverability, and can be viewed as a companion approach.

The following observations are in order regarding the differential privacy framework [71]. The first involves the close relationship between the sensitivity of a function and differential privacy. The sensitivity of a function is the maximum difference in the values that the function takes on a pair of adjacent databases, with an appropriate metric measuring distance between databases. For instance, for a given query function, a differentially private data release mechanism involves adding to the true function value a Laplace noise whose variance is proportional to the sensitivity of the query function [27]. However, in practice, either the sensitivity of the query function is too large or cannot be determined. This can affect implementability of differential privacy mechanisms. Next, from a legal standpoint, it is unclear what differential privacy addresses. Concretely, for example, General Data Protection Regulation (GDPR), which is a regulation in European Union law on data protection and privacy, requires that when information about a database is released, the Personal Identifiable Information (PII) of any user should not be inferred from the output. Another requirement for the data release mechanism is that it should prevent "singling out," i.e., details about an individual in the database should defy isolation or identification in a unique manner. It is not clear how a differentially private mechanism adheres to the two requirements above. Our approach attempts to address these considerations.

Directions other than differential privacy have also been pursued. As mentioned in [73], these include studies based on clustering (e.g., [69]), t-closeness (e.g., [47]), data pertubation (e.g., [30]), etc; see [73] for a comprehensive list. Other methods include (ρ_1, ρ_2)-privacy (e.g., [31]), confidence intervals (e.g., [2]), and cryptographic approaches (e.g., [8]).

Our approach is in the spirit of prior works [64], [12], [66], [48], [38], [74] that deal with information leakage of a user's private data with associated nonprivate correlated data. A randomized version of the nonprivate data is released publicly under a constraint on the expected

distortion between the nonprivate and public data. The public data is designed such that it minimizes information leakage, which is measured by the mutual information between public and private data, under said distortion constraint. These works are based on principles of rate distortion theory.

In a related data privacy model in [5], [23], maximum a posteriori (MAP) estimates of private and nonprivate data, that are digital, are formed on the basis of randomized public versions of the latter. The private, nonprivate and public data are assumed to form a Markov chain. Under a constraint on the probability of estimating correctly the private data, mechanisms are sought for said randomization so as to maximize correct MAP estimation of the nonprivate data. In the same vein, but involving analog data, in [3], [4], [13], [22], private and nonprivate correlated data with a given joint distribution is considered. In [3], a Gaussian noise, independent of the private and nonprivate data, is added to the latter and released publicly. The parameters of the Gaussian noise are obtained as a result of minimizing the minimum mean-square error (MMSE) in estimating the nonprivate data from the public data. This minimization is done under a constraint on the MMSE in estimating the private data from the public data. In [4], first a Gaussian noise independent of the private and nonprivate data is added to the latter, and the sum is quantized and released publicly. In this case, the parameters of the Gaussian noise are obtained as a result of maximizing the mutual information between the public and nonprivate data under a constraint on the mutual information between the public and private data. These works involve maximizing recoverability under a privacy constraint. In this dissertation, by contrast, we tackle the complementary problem, where privacy is maximized under a recoverability constraint.

Turning to problem settings of relevance to distribution privacy, an extensive body of prior work exists on distribution estimation in the context of data privacy (cf. e.g., [25], [32], [14], [37],

and references therein). Privacy constraints, when explicitly present, are prominently in the sense of differential privacy. In a series of works [24], [40], [76], [62], [1], [15], 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 another line of work [17], [46], [10], [11], [61], *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 [43] for a similar minmax study under other loss measures. These works on distribution estimation, with or without privacy, do not require computation of a function of the underlying data.

1.3. Our Approach and Main Contributions

We introduce a general approach for two categories of problems: data and distribution privacy under function recoverability requirements. In a setting where a querier wishes to obtain a given function of user data, we seek to design user query responses that not only enable the querier

to recover the function value with a desired utility level but also to maximize privacy of the user data or the probability distribution that governs the data. Our objective is to characterize optimal tradeoffs between the extent of data or distribution privacy afforded to the user and the accuracy level of the function recoverability by the querier, and specify suitable randomization mechanisms for query responses that attain maximal privacy.

The main contributions of this dissertation are summarized below. Our work on data and distribution privacy under function recoverability are presented in Chapters 2-4 and Chapter 5, respectively. Chapter 6 contains closing remarks.

1.3.1. Data Privacy

In Chapter 2, we consider a (legitimate) user's data that is represented by a finite-valued random variable (rv) with known probability mass function (pmf). A querier seeks to compute a given function of the data from a user-provided query response which is a suitably randomized version of the data. The user forms the query response from which the querier can recover the function value with probability at least $\rho,\ 0 \leq \rho \leq 1$. Under this requirement, the chosen query response must afford maximum data privacy. Specifically, the query response must inflict – on the querier's best estimate from it of the data value – a maximum probability of error. Beginning with a single query response, we give an explicit characterization of a randomization mechanism, i.e., achievability scheme that enables ρ-recoverability of the function value and yields the corresponding maximum privacy, termed *ρ-privacy*. In particular, our query-response scheme is tantamount to an "add-noise" mechanism with the user computing first the function value and then adding to it a suitable *value-dependent* noise. Our optimal single query response depends

on the pmf of the data rv only in a limited way through associated minentropies. Furthermore, when privacy is sought for a predicate or attribute of the user data, we obtain a characterization of *predicate ρ-privacy* and an explicit randomization mechanism that attains it. Next, when the querier elicits $n \geq 1$ ρ-recoverable and independent query responses, privacy of user data can degrade while accuracy of function estimation by the querier improves. We provide a converse upper bound for maximum privacy with respect to such responses, i.e., ρ-privacy for every n. When $0.5 < \rho \leq 1$, this upper bound decays exponentially in n to a limit which is the querier's data-estimation error on the basis of a knowledge of the exact function value (i.e., corresponding to $\rho = 1$). The rate of this decay is shown to be the (Kullback-Leibler) divergence $D\left(\text{Ber}(0.5)||\text{Ber}(\rho)\right)$. We provide an explicit add-noise achievability scheme with privacy that converges to the mentioned limit at the same exponential rate. When $0 \leq \rho \leq 0.5$, we again provide an explicit add-noise achievability scheme. While it remains unknown whether the corresponding privacy is optimal, this scheme is shown to prevent the querier from estimating exactly the function value for any n. Neither achievability scheme depends on a knowledge of the pmf of the data rv. Finally, these two achievability schemes are shown to be asymptotically superior in privacy to a scheme made up of (conditionally) independent and identically distributed (i.i.d.) repetitions of our optimal single query response; this is done by means of suitable asymptotic approximations of privacy in terms of Chernoff radii. The superiority of the former schemes is enabled by rendering an estimation by the querier of the exact function value to be more error-prone than by the latter scheme, while conforming to the ρ-recoverability requirement.

Next in Chapter 3, under the same function ρ-recoverability constraint mentioned above, we consider a more demanding measure of privacy: "list privacy," measured[1] by the probability

[1]List privacy has been considered earlier in a cryptographic context in [67].

that the user data is not contained in a list of prescribed size formed by the querier based on the query response. This is relevant, for example, in a movie streaming application where a user requests a particular movie, and the identity of that movie is protected, say, by end-to-end encryption. But the application might still be interested in the genre of movies that are being streamed, which a user wishes to be kept private. Here, the movie requested can be thought of as the user data and the genre as a list, of which the particular movie requested, is a part. In this case, the function is the identity function.

We develop a general converse upper bound for maximum list privacy. For the special case of a binary-valued function, the upper bound is shown to be optimal through an achievability scheme based on an explicit query response.

Next, we turn to a model where user data is analog. For example, when analog biometric data, such as fingerprint or voice patterns, are collected and certain attributes are released, an objective is to safeguard the privacy of individual user data while ensuring high utility of the released information. In Chapter 4, we consider analog user data that is represented by a Gaussian rv and a querier who wishes to compute a given linear function of the data from a query response elicited from the user. The query response is a suitably randomized version of the data which the user forms so as to enable the querier to recover the function value with a prescribed accuracy. The user's objective is to maximize the privacy of the data from the querier while adhering to the recoverability requirement, where both recoverability and privacy are measured by ℓ_2-distance criteria.

In this formulation, the user-provided query response should be such that its expected ℓ_2-distance from the function value is no greater than ρ, $\rho \geq 0$. Under this recoverability constraint, we consider a notion of privacy measured by the expected ℓ_2-distance between the

user data and the querier's best estimate of it based on the query response, i.e., the corresponding minimum mean-square estimation error. We provide an exact characterization of maximum privacy under the ρ-recoverablity requirement as a function of ρ, and specify an explicit query response that attains it. This maximum privacy is shown to be a nondecreasing piecewise affine function of ρ, and depends on the linear mapping only through its rank and singular values. The user implements the optimal query response by attenuating the function value and adding to it a suitable independent Gaussian noise. This query response constitutes a multidimensional extension of a scheme in [75] in the separate context of maximizing the MMSE in estimating a one-dimensional Gaussian rv on the basis of a one-dimensional randomized version of it under a constraint on the expected ℓ_2-distance between the input and the randomized output, where the maximization is over all possible randomization mechanisms satisfying the constraint.

1.3.2. Distribution Privacy

In Chapter 5, we consider a (legitimate) user's data to be represented by i.i.d. repetitions of a finite-valued rv with an underlying pmf that the user chooses and seeks to keep private from a querier. The querier's objective is to compute a given function of the data from user-provided i.i.d. query responses that are randomized versions of the data. The user designs the query responses in such a way that the querier can 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.[2] 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

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

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 chosen 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 a probability not less than ρ; the queriers then cooperate to estimate P_X from their pooled n i.i.d. query responses.

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" 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 strategy restricted to a locally uniform estimator, the user can make do with a sparse pmf and add-noise 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.

Chapter 2: Data Privacy Under Function Recoverability

2.1. Synopsis

We consider a user's data to be represented by a finite-valued rv with a known pmf. A querier wishes to compute a given function of the data from a query response provided by the user. The user devises the query response, which is a suitably randomized version of the data, so as to enable the querier to recover from it the function value with a given probability ρ, $0 \leq \rho \leq 1$, while maximizing privacy of the data. Privacy is measured by the probability of error incurred by the querier in estimating the data from the query response. Single and multiple independent query responses, with each response satisfying the recoverability requirement, which provide maximum privacy to the user are analyzed. In the former setting, we also consider privacy for a predicate of the user's data, i.e., a specified attribute of it and described in terms of a given mapping.

Our model for ρ-recoverable function computation with associated privacy is described in Section 2.2. The ρ-privacy for a single query response is characterized in Section 2.3, and ρ-privacy is extended to multiple independent query responses in Section 2.4. Predicate privacy is presented in Section 2.5. Converse and achievability proofs of results stated in Section 2.4 are provided in Section 2.6. The inadequacy of (conditionally) i.i.d. repetitions of the optimum ρ-privacy scheme of Section 2.3 in the context of Section 2.4 is brought out in Section 2.7. A closing

discussion is contained in Section 2.8 along with open problems including one that touches on local differential privacy. The results of this chapter were reported in [54], [55], [56].

2.2. Preliminaries

A (legitimate) user's data is represented by a rv X taking values in a finite set $\mathcal{X}$ with $|\mathcal{X}|= r$, say, and of known pmf P_X with $P_X(x) > 0$, $x \in \mathcal{X}$. Throughout this chapter, we shall 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 inverse image of f, with $f^{-1}(i) \triangleq \{x \in \mathcal{X} : f(x) = i\}$, $i \in \mathcal{Z}$. For a realization $X = x$ in $\mathcal{X}$, a querier – who does not know x – wishes to compute $f(x)$ from a *query response* (QR) $F(x)$ provided by the user, where $F(x)$ is a rv with values in $\mathcal{Z}$. The QR $F(X)$ must satisfy the following recoverability condition.

Definition 2.1. Given $0 \leq \rho \leq 1$, a QR $F(X)$ is *ρ-recoverable* if

$$P(F(X) = f(x) \,|X = x) \geq \rho, \quad x \in \mathcal{X}. \tag{2.1}$$

Condition (2.1) can be written equivalently in terms of a stochastic matrix $W : \mathcal{X} \to \mathcal{Z}$ with the requirement

$$W(f(x)\,|x) \geq \rho, \quad x \in \mathcal{X}; \tag{2.2}$$

which, too, will constitute a *ρ-recoverable* QR. Such a ρ-recoverable $F(X)$ or W will be termed ρ-QR. Note that ρ-recoverability in (2.1), (2.2) does not depend on P_X.

Definition 2.2. A ρ-QR $F(X)$ will be called an *add-noise* ρ-QR if it can be expressed as

$$F(X) = f(X) + N \bmod k \tag{2.3}$$

where N is a $\mathcal{Z}$-valued rv that satisfies

$$N \multimap f(X) \multimap X \tag{2.4}$$

and with conditional pmf given by

$$\begin{aligned} P\left(N = i | X = x\right) &= P\left(N = i | f(X) = f(x), X = x\right) \\ &= P\left(N = i | f(X) = f(x)\right) \qquad (2.5) \\ &= V\left(i + f(x) \bmod k \,|f(x)\right) \qquad (2.6) \end{aligned}$$

for some stochastic matrix $V : \mathcal{Z} \to \mathcal{Z}$ with $V(i|i) \geq \rho,\ i \in \mathcal{Z}$; we shall refer to it also as add-noise ρ-QR V. Thus, an add-noise ρ-QR is obtained by adding to the function value $f(x)$ a noise N whose (conditional) pmf can depend on $f(x)$.

By (2.3)-(2.6), an add-noise ρ-QR $F(X)$ with $V : \mathcal{Z} \to \mathcal{Z}$ has the following property:

$$P\left(F\left(X\right) = i | f(X) = f(x), X = x\right) = V\left(i | f(x)\right), \quad i \in \mathcal{Z},\ \ x \in \mathcal{X}. \tag{2.7}$$

Definition 2.3. Denoting by Z the rv $F\left(X\right)$ with values in $\mathcal{Z}$, the *privacy* of a ρ-QR $F\left(X\right)$ (or

equivalently ρ-QR W) satisfying (2.1) (respectively (2.2)) is

$$\pi_\rho(F) = \pi_\rho(W) = \min_g \; P(g(Z) \neq X) \tag{2.8}$$

where the minimum is over all estimators $g : \mathcal{Z} \to \mathcal{X}$ of X on the basis of $F(X)$. Clearly, the minimum in (2.8) is attained by the MAP estimator $g_{MAP} = g_{MAP(W)} : \mathcal{Z} \to \mathcal{X}$ given by

$$g_{MAP(W)}(i) = \arg \max_{x \in \mathcal{X}} \; P_X(x) W(i|x), \quad i \in \mathcal{Z} \tag{2.9}$$

so that (2.8) equals $P(g_{MAP(W)}(Z) \neq X)$. When $F(X)$ is an add-noise ρ-QR V as in Definition 2.2, we shall denote $\pi_\rho(F)$ in (2.8) by $\pi_\rho(V)$. The corresponding minimum in (2.8) will be denoted by $P(g_{MAP(V)}(Z) \neq X)$ where

$$g_{MAP(V)}(i) = \arg \max_{x \in \mathcal{X}} \; P_X(x) V(i|f(x)), \quad i \in \mathcal{Z}. \tag{2.10}$$

Ties in (2.9) and (2.10) are broken arbitrarily.

Remarks:

(i) Our notion of privacy assumes conservatively that the querier is aware of the user's choice of privacy mechanism W and pmf P_X for computing the MAP estimate in (2.9).

(ii) Concerning ρ-recoverability, we add that there is no loss of generality in (2.1), (2.2) by not considering an *estimate* of $f(X)$ on the basis of $F(X)$; this is so, because the user can emulate any such estimation strategy of the querier to produce yet another ρ-QR.

Definition 2.4. For each $0 \leq \rho \leq 1$, the maximum privacy that can be attained by a ρ-QR is termed *ρ-privacy* and denoted by $\pi(\rho)$, i.e.,

$$\pi(\rho) = \max_{\substack{W: W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \pi_\rho(W). \tag{2.11}$$

Remark: That the maximum in (2.11) exists will be seen below.

The following simple lemma shows when a ρ-QR W is also an add-noise ρ-QR, and will be helpful in our achievability proofs.

Lemma 2.1. *Given $0 \leq \rho \leq 1$, for a ρ-QR $W : \mathcal{X} \to \mathcal{Z}$ with identical rows for all $x \in f^{-1}(i),\ i \in \mathcal{Z}$, there exists an add-noise ρ-QR $V = V(W) : \mathcal{Z} \to \mathcal{Z}$ with the same privacy, i.e., with $\pi_\rho(V) = \pi_\rho(W)$. Conversely, for an add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$, there exists a ρ-QR $W = W(V) : \mathcal{X} \to \mathcal{Z}$ with identical rows as above, and with $\pi_\rho(W) = \pi_\rho(V)$.*

Proof: For a stochastic matrix $W : \mathcal{X} \to \mathcal{Z}$ which satisfies (2.2) and has rows $\{(W(i'|x),\ i' \in \mathcal{Z}), x \in \mathcal{X}\}$ that are identical for all $x \in f^{-1}(i),\ i \in \mathcal{Z}$, consider a stochastic matrix $V = V(W) : \mathcal{Z} \to \mathcal{Z}$ given by

$$V(i|j) = W(i|x) \text{ for every } x \in f^{-1}(j),\ i, j \in \mathcal{Z} \tag{2.12}$$

and an associated add-noise QR $F'(X)$ defined as in (2.3)-(2.6) with V as above. Since $V(i|i) \geq \rho,\ i \in \mathcal{Z}$, in (2.12), $F'(X)$ is an add-noise ρ-QR. To see that $\pi_\rho(V) = \pi_\rho(W)$, we have

$$P\Big(g_{MAP(V)}(F'(X)) = X\Big) = \sum_{i \in \mathcal{Z}} \max_{x \in \mathcal{X}} P(X = x, F'(X) = i) \tag{2.13}$$

where in the right-side,

$$\begin{aligned} P(X=x, F'(X)=i) &= \sum_{j\in\mathcal{Z}} P(X=x, f(X)=j, F'(X)=i) \\ &= P(X=x, f(X)=f(x))P_{F'(X)|f(X)}\left(i|f(x)\right), \quad \text{by (2.7)} \\ &= P_X(x)V(i|f\left(x\right)) \\ &= P_X(x)W(i|x), \quad \text{by (2.12)}. \end{aligned}$$

Hence, by (2.13),

$$\begin{aligned} 1-\pi_\rho(V) &= P\Big(g_{MAP(V)}(F'\left(X\right)) = X\Big) \\ &= \sum_{i\in\mathcal{Z}} \max_{x\in\mathcal{X}} P_X(x)W(i|x) \\ &= 1-\pi_\rho(W). \end{aligned}$$

Conversely, given an add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$, consider a stochastic matrix $W = W(V) : \mathcal{X} \to \mathcal{Z}$ with identical rows for all $x \in f^{-1}(i),\ i \in \mathcal{Z}$, defined by (2.12). By the same steps as above, this W is a ρ-QR and, furthermore, $\pi_\rho(W) = \pi_\rho(V)$. ■

2.3. ρ-Privacy for a Single Query Response

A characterization of ρ-privacy is provided by obtaining first an upper bound for $\pi(\rho)$ and then identifying explicitly an add-noise ρ-QR whose privacy meets the bound.

Let

$$x^* = \arg \max_{x \in \mathcal{X}} \; P_X(x), \quad x_* = \arg \min_{x \in \mathcal{X}} \; P_X(x), \quad x_i^* = \arg \max_{x \in f^{-1}(i)} \; P_X\left(x\right), \quad i \in \mathcal{Z} \tag{2.14}$$

and suppose that $x^* \in f^{-1}\left(i^*\right)$ for some $i^* \in \mathcal{Z}$, where x^*, x_*, i^* and x_i^*, $i \in \mathcal{Z}$, need not be unique. Further, set

$$\rho_c = \frac{P_X\left(x^*\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(x_i^*\right)} \tag{2.15}$$

and observe that $1/k \leq \rho_c < 1$, where the left inequality is by

$$\frac{P_X\left(x^*\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(x_i^*\right)} \geq \frac{P_X\left(x^*\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(x^*\right)} = \frac{1}{k}.$$

The following choice of ρ-QR $W = W_o : \mathcal{X} \to \mathcal{Z}$ will play a material role in the achievability proof of ρ-privacy in Theorem 2.2 below:

$$W_o\left(i|x\right) = \begin{cases} \max\{\rho_c, \rho\}, & i = f(x) \\ \left(1 - \max\{\rho_c, \rho\}\right) \frac{P_X\left(x_i^*\right)}{\sum\limits_{l \neq f(x)} P_X\left(x_l^*\right)}, & i \neq f(x), \;\; x \in \mathcal{X}, \; i \in \mathcal{Z}. \end{cases} \tag{2.16}$$

We note that W_o has the property that for each $i \in \mathcal{Z}$, all rows of W_o corresponding to $x \in f^{-1}\left(i\right)$ are identical. By dint of Lemma 2.1, the associated stochastic matrix $V_o : \mathcal{Z} \to \mathcal{Z}$ given by

$$V_o\left(i|j\right) = W_o\left(i|x\right) \;\; \text{for every } x \in f^{-1}\left(j\right)$$

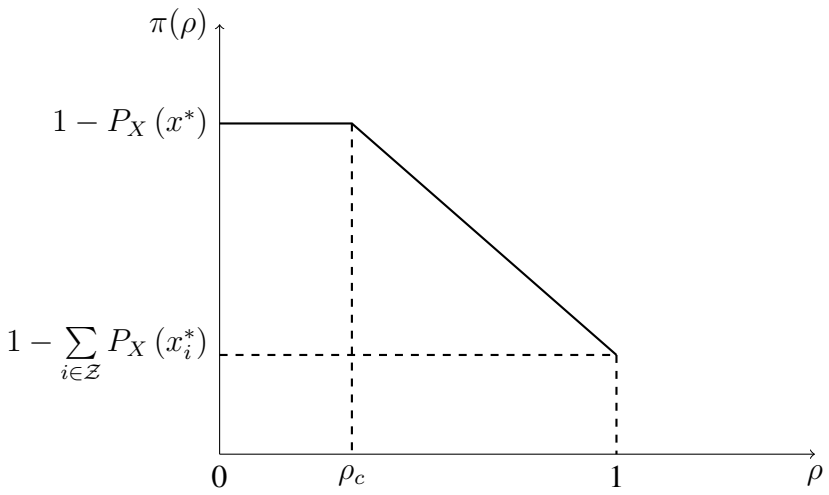


Figure 2.1: $\pi(\rho)$ vs. ρ.

$$= \begin{cases} \max\{\rho_c, \rho\}, & i = j \\ \left(1 - \max\{\rho_c, \rho\}\right) \frac{P_X\left(x_i^*\right)}{\sum_{l \neq j} P_X\left(x_l^*\right)}, & i \neq j, \;\; i, j \in \mathcal{Z} \end{cases} \tag{2.17}$$

will be also of consequence in achieving ρ-privacy.

An exact characterization of ρ-privacy is provided by

Theorem 2.2. *ρ-privacy equals*

$$\pi(\rho) = 1 - \max\left\{P_X(x^*), \rho \sum_{i \in \mathcal{Z}} P_X(x_i^*)\right\} = 1 - \max\{\rho_c, \rho\} \sum_{i \in \mathcal{Z}} P_X(x_i^*), \quad 0 \leq \rho \leq 1. \tag{2.18}$$

Furthermore, ρ-privacy is achieved by the ρ-QR W_o in (2.16) and, additionally, by the add-noise ρ-QR V_o in (2.17).

Remarks:

(i) By Theorem 2.2,

$$\pi(\rho) = \begin{cases} 1 - P_X(x^*), & 0 \le \rho \le \rho_c \\ 1 - \rho \sum_{i \in \mathcal{Z}} P_X(x_i^*), & \rho_c \le \rho \le 1 \end{cases}$$

and is plotted in Fig. 2.1. In particular, for $0 \le \rho \le \rho_c$, $\pi(\rho) = 1 - P_X(x^*)$ and is the error of a MAP estimator of X without any observation. For $\rho = 1$, $\pi(1) = 1 - \sum_{i \in \mathcal{Z}} P_X(x_i^*)$ is the error of a MAP estimator of X on the basis of $f(X)$.

(ii) In (2.18), since $\sum_{i \in \mathcal{Z}} P_X(x_i^*) \le 1$, we get

$$\pi(\rho) \ge 1 - \max\{P_X(x^*), \rho\}. \tag{2.19}$$

Also, since

$$\sum_{i \in \mathcal{Z}} P_X(x_i^*) \ge P_X(x^*) + P_X(x_*),$$

we get

$$\pi(\rho) \le 1 - \max\{P_X(x^*), \rho(P_X(x^*) + P_X(x_*))\}. \tag{2.20}$$

Combining (2.19) and (2.20),

$$1 - \max\{P_X(x^*), \rho\} \le \pi(\rho) \le 1 - \max\{P_X(x^*), \rho(P_X(x^*) + P_X(x_*))\}, \quad 0 \le \rho \le 1. \tag{2.21}$$

From (2.21), for a given user data pmf P_X, we can obtain worst-case and best-case mappings $f : \mathcal{X} \to \mathcal{Z}$ for $\pi(\rho)$, $0 \le \rho \le 1$. It can be seen readily that the lower bound on $\pi(\rho)$ in (2.21) is attained by any invertible mapping $f : \mathcal{X} \to \mathcal{X}$ and the upper bound on $\pi(\rho)$

in (2.21) is attained by the binary-mapping $f : \mathcal{X} \to \{0, 1\}$ given by

$$f(x) = \begin{cases} 0, & x = x_* \\ 1, & x \neq x_*. \end{cases}$$

Thus, as is to be expected, ρ-privacy increases with decreasing "atomicity" of the mapping $f : \mathcal{X} \to \mathcal{Z}$. Specifically, fewer and larger the atoms induced in $\mathcal{X}$ by f^{-1}, the better is the ability of the user to hide the realization of $X = x,\ x \in \mathcal{X}$, from the querier which results in higher ρ-privacy.

(iii) The choice of W_o and V_o in (2.16) and (2.17), and the value of ρ-privacy in (2.18), depend on P_X only through $P_X\left(x_i^*\right), i \in \mathcal{Z}$, i.e., $P_X\left(f^{-1}(i)\right) 2^{-H_{min}(P_i)}$, $i \in \mathcal{Z}$, where $H_{min}(P_i)$ is the minentropy of the pmf $P_i = \left(P_X(x)/P_X\left(f^{-1}(i)\right),\ x \in f^{-1}(i)\right)$.

Proof: That the two characterizations of $\pi(\rho)$ in (2.18) are identical follows by straightforward manipulation. We first show that ρ-privacy cannot exceed the right-side(s) of (2.18), and then identify a ρ-QR that attains it.

Converse: Clearly

$$P(g_{MAP(W)}(Z) = X) \geq P_X(x^*)$$

and for every $W : \mathcal{X} \to \mathcal{Z}$ satisfying (2.2),

$$P(g_{MAP(W)}(Z) = X) = \sum_{i \in \mathcal{Z}} \max_{x \in \mathcal{X}} P_X(x) W(i|x)$$

$$\geq \sum_{i \in \mathcal{Z}} \max_{x \in f^{-1}(i)} P_X(x) W(i|x) \geq \rho \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)$$

leading to

$$P(g_{MAP(W)}(Z) = X) \geq \max\left\{P_X(x^*), \rho \sum_{i\in\mathcal{Z}} P_X(x_i^*)\right\}. \tag{2.22}$$

Hence

$$\pi_\rho(W) = P(g_{MAP(W)}(Z) \neq X) \leq 1 - \max\left\{P_X(x^*), \rho \sum_{i\in\mathcal{Z}} P_X(x_i^*)\right\}, \quad 0 \leq \rho \leq 1 \tag{2.23}$$

so that the same upper bound, valid for all $W : \mathcal{X} \to \mathcal{Z}$ subject to (2.2), applies to $\pi(\rho)$, too.

Achievability: We show that the choice of the ρ-QR $W_o : \mathcal{X} \to \mathcal{Z}$ in (2.16) has privacy $\pi_\rho(W_o)$ equal to the right-side(s) of (2.18). To this end,

$$\begin{aligned}
1 - \pi_\rho(W_o) &= P(g_{MAP(W_o)}(Z) = X) \\
&= \sum_{i\in\mathcal{Z}} \max_{x\in\mathcal{X}} P_X(x) W_o(i|x) \\
&= \sum_{i\in\mathcal{Z}} \max\left\{\max_{x\in f^{-1}(i)} P_X(x) W_o(i|x), \max_{x\notin f^{-1}(i)} P_X(x) W_o(i|x)\right\} \\
&= \sum_{i\in\mathcal{Z}} \max\left\{P_X(x_i^*)\max\{\rho_c, \rho\}, \max_{x\notin f^{-1}(i)} P_X(x) W_o(i|x)\right\}, \quad \text{by (2.16)}.
\end{aligned} \tag{2.24}$$

We claim that

$$P_X(x_i^*)\max\{\rho_c, \rho\} \geq \max_{x\notin f^{-1}(i)} P_X(x) W_o(i|x), \quad i \in \mathcal{Z} \tag{2.25}$$

whereupon (2.24) becomes

$$1 - \pi_\rho(W_o) = \max\{\rho_c, \rho\} \sum_{i\in\mathcal{Z}} P_X(x_i^*)$$

so that the privacy $\pi_\rho(W_o)$ equals the right-side(s) of (2.18). It remains to establish (2.25).

Considering first the case $0 \leq \rho \leq \rho_c$, we must show for each $x \notin f^{-1}(i)$ that

$$P_X\left(x_i^*\right)\rho_c \geq P_X\left(x\right)W_o\left(i|x\right) = P_X(x)\left(1-\rho_c\right)\frac{P_X\left(x_i^*\right)}{\sum\limits_{j\neq f(x)} P_X(x_j^*)}, \quad \text{by (2.16)}$$

i.e.,

$$\frac{\rho_c}{1-\rho_c} \geq \frac{P_X\left(x\right)}{\sum\limits_{j\neq f(x)} P_X(x_j^*)} \tag{2.26}$$

which, in turn, would follow if

$$\frac{\rho_c}{1-\rho_c} \geq \frac{P_X\left(x^*\right)}{\sum\limits_{j\neq f(x)} P_X(x_j^*)},$$

which is tantamount to showing that

$$\frac{\sum\limits_{j\neq i^*} P_X(x_j^*)}{\sum\limits_{j\neq f(x)} P_X(x_j^*)} \leq 1. \tag{2.27}$$

Clearly, (2.27) holds for each $x \notin f^{-1}(i)$, as the denominator is either larger than or equal to the numerator for all $i \in \mathcal{Z}$. For the case $\rho_c \leq \rho < 1$, we must show (2.26) with ρ_c replaced by ρ; this follows readily since

$$\frac{\rho}{1-\rho} \geq \frac{\rho_c}{1-\rho_c}, \quad \rho_c \leq \rho < 1.$$

For $\rho = 1$, we have by (2.16) that $W_o\left(i|x\right) = \mathbb{1}(i = f\left(x\right))$, $x \in \mathcal{X}, i \in \mathcal{Z}$, whereby (2.25) holds trivially.

Finally, that the add-noise ρ-QR V_o achieves ρ-privacy follows by Lemma 1. ■

Remark: The ρ-privacy achieving ρ-QR W_o and the corresponding add-noise ρ-QR V_o in Theorem 2.2 are not unique. For instance, see Remark (i) following Theorem 2.4, Remark (i)

following Theorem 2.5 and Remark (ii) after Theorem 2.8.

2.4. Multiple Independent Query Responses

Consider a general setting where, for a realization $X = x$ in $\mathcal{X}$, a querier wishes to compute $f(x)$, $x \in \mathcal{X}$, from ρ-QRs $\{(F_t(x),\ x \in \mathcal{X})\}_{t=1}^{n}$, $n \geq 1$. The rvs $\{F_t(X)\}_{t=1}^{n}$ are taken to be conditionally mutually independent, conditioned on X, but not necessarily identically distributed, with *each* $F_t(X)$ satisfying the ρ-recoverability condition (2.1). Correspondingly, consider stochastic matrices $\{W_t : \mathcal{X} \to \mathcal{Z}\}_{t=1}^{n}$ such that

$$\begin{aligned} P(F_1(X) = i_1, \ldots, F_n(X) = i_n | X = x) &= \prod_{t=1}^{n} P(F_t(X) = i_t | X = x) \\ &= \prod_{t=1}^{n} W_t(i_t|x), \quad x \in \mathcal{X},\ i_1, \ldots, i_n \in \mathcal{Z} \end{aligned} \tag{2.28}$$

say, with *each* W_t satisfying (2.2). Similarly, for add-noise ρ-QRs $F_t(X)$ as in Definition 2.2 with $\{V_t : \mathcal{Z} \to \mathcal{Z}$ where $V_t(i|i) \geq \rho,\ i \in \mathcal{Z}\}_{t=1}^{n}$,

$$P(F_1(X) = i_1, \ldots, F_n(X) = i_n | X = x) = \prod_{t=1}^{n} V_t(i_t | f(x)), \quad x \in \mathcal{X},\ i_1, \ldots, i_n \in \mathcal{Z}. \tag{2.29}$$

In all contexts, denote $Z_t = F_t(X)$, $t = 1, \ldots, n$.

This formulation is pertinent when the main objective of the querier is to improve its estimation accuracy (beyond ρ) of a *given* $f(X)$ by soliciting multiple ρ-QRs whereas the user designs said ρ-QRs so as to maximize the privacy of its data X. Precisely, for a MAP estimator h_{MAP} of $f(X)$ on the basis of $\{F_t(X)\}_{t=1}^{n}$ in (2.28), we have

$$P(h_{\text{MAP}}(F_1(X),\ldots,F_n(X)) = f(X))$$
$$\geq \max\left\{\rho, \max_{i\in\mathcal{Z}} P(f(X)=i), P\left(\text{Bin}(n,\rho) \geq \left\lfloor \frac{n}{2}\right\rfloor + 1\right)\right\} \quad (2.30)$$

where $\text{Bin}(n,\rho)$ is a binomial rv with parameters $n \geq 1$ and $0 \leq \rho \leq 1$. In particular, for $0.5 < \rho \leq 1$, the right-side of (2.30) tends to 1 as $n \to \infty$. See Appendix A.2 and Lemma 2.6. In addition to possibly improving the estimation accuracy of $f(X)$, privacy can erode, the details of which are given below. We first define ρ-privacy for the setting mentioned above.

Definition 2.5. For each $0 \leq \rho \leq 1$ and $n \geq 1$, the ρ-privacy that can be attained by ρ-QRs $\{F_t(X)\}_{t=1}^n$ as in (2.28) with each $F_t(X)$ satisfying (2.1) (or equivalently each W_t satisfying (2.2)) is

$$\pi_n(\rho) = \max_{\substack{W_1,\ldots,W_n: \\ W_t(f(x)|x)\geq\rho,\ x\in\mathcal{X}}} \pi_\rho(W_1,\ldots,W_n), \quad (2.31)$$

where

$$\pi_\rho(W_1,\ldots,W_n) = \min_{g_n} P(g_n(Z_1,\ldots,Z_n) \neq X),$$

with the minimum being taken over all estimators $g_n : \mathcal{Z}^n \to \mathcal{X}$ on the basis of $\{F_t(X)\}_{t=1}^n$. Thus,

$$\pi_\rho(W_1,\ldots,W_n) = P(g_{\text{MAP}(W_1,\ldots,W_n)}(Z_1,\ldots,Z_n) \neq X) \quad (2.32)$$

where

$$g_{MAP(W_1,\ldots,W_n)}(i_1,\ldots,i_n) = \arg\max_{x\in\mathcal{X}} P_X(x)\prod_{t=1}^n W_t(i_t|x), \quad i_1,\ldots,i_n \in \mathcal{Z}.$$

Similarly, for add-noise ρ-QRs $\{F_t(X)\}_{t=1}^n$ as in (2.29), we define

$$\pi_\rho\left(V_1,\ldots,V_n\right) = P(g_{\text{MAP}\,(V_1,\ldots,V_n)}\left(Z_1,\ldots,Z_n\right) \neq X) \tag{2.33}$$

with

$$g_{MAP(V_1,\ldots,V_n)}\left(i_1,\ldots,i_n\right) = \arg\,\max_{x\in\mathcal{X}}\; P_X\left(x\right)\prod_{t=1}^{n} V_t(i_t|f(x)), \quad i_1,\ldots,i_n \in \mathcal{Z}.$$

Of particular interest will be the cases $W_t = W$ or $V_t = V$, $t = 1,\ldots,n$, when we write (2.32) and (2.33) as

$$\pi_\rho\left(W^n\right) = P(g_{\text{MAP}\,(W^n)}\left(Z_1,\ldots,Z_n\right) \neq X)$$

and

$$\pi_\rho\left(V^n\right) = P(g_{\text{MAP}\,(V^n)}\left(Z_1,\ldots,Z_n\right) \neq X).$$

We provide first in Section 2.4.1 an upper bound for ρ-privacy $\pi_n(\rho)$ which is valid for each $0 \leq \rho \leq 1$ and every $n \geq 1$. Next, in Section 2.4.2, considering the realms $0.5 < \rho \leq 1$ and $0 \leq \rho \leq 0.5$ separately, we show corresponding explicit achievability schemes. However, unlike in Section 2.3 for the case $n = 1$, the lower bound for $\pi_n(\rho)$ from the achievability schemes below, that use add-noise ρ-QRs, need not coincide with the upper bound in Section 2.4.1 for any finite $n \geq 1$. These upper and lower bounds for $\pi_n(\rho)$ are rendered into more convenient, albeit blunter forms in Section 2.4.3. Proofs of the theorems in Sections 2.4.1 and 2.4.2 are contained in Section 2.6.

2.4.1. Converse

We now present, as a converse result, an upper bound for $\pi_n(\rho)$, $n \geq 1$. For $0 \leq \rho \leq 1$, set

$$\Gamma_n(\rho) = \min\left\{1-\rho_c, \min\left\{1-\rho, P\left(\text{Bin}(n,\rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right)\right\}\right\} \sum_{i\in\mathcal{Z}} P_X(x_i^*), \quad n \geq 1 \tag{2.34}$$

and note that $0 \leq \Gamma_n(\rho) \leq 1$.

Theorem 2.3. *For each* $0 \leq \rho \leq 1$ *and for every* $n \geq 1$,

$$\pi_n(\rho) \leq 1 - \sum_{i\in\mathcal{Z}} P_X(x_i^*) + \Gamma_n(\rho).$$

Remarks:

(i) For $0 \leq \rho \leq 1$ and $n = 1$, since

$$\Gamma_1(\rho) = (1 - \max\{\rho_c, \rho\}) \sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right),$$

we have that the upper bound for $\pi_n(\rho)$ above reduces to that for $\pi(\rho)$ in the right-side of (2.23).

(ii) When $\mathcal{Z} = \mathcal{X}$ and $f : \mathcal{X} \to \mathcal{X}$ is a one-to-one mapping, the upper bound for $\pi_n(\rho)$ becomes

$$\pi_n(\rho) \leq \Gamma_n(\rho), \quad 0 \leq \rho \leq 1,$$

since $\sum_{i\in\mathcal{X}} P_X(x_i^*) = \sum_{x\in\mathcal{X}} P_X(x) = 1$.

2.4.2. Achievability

Throughout our achievability proofs, for the sake of convenience and without loss of essential generality, we assume that

$$P_X(x_i^*) \geq P_X(x_{i+1}^*), \quad i = 0, 1, \ldots, k-2. \tag{2.35}$$

2.4.2.1. Realm $0.5 < \rho \leq 1$

Our achievability scheme uses the following stochastic matrix $V_1 : \mathcal{Z} \to \mathcal{Z}$, not depending on P_X, given by

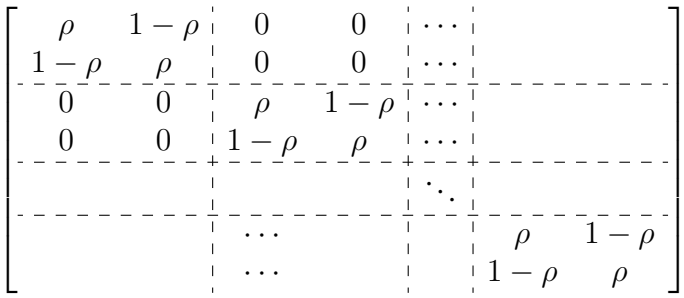
$$V_1(i|j) = \begin{cases} \rho, & i = j \\ 1-\rho, & j \text{ even and } i = j+1 \bmod k \text{ or } j \text{ odd and } i = j-1 \\ 0, & \text{otherwise,} \end{cases} \tag{2.36}$$

for $i, j \in \mathcal{Z}$. Thus, for k even, the $k \times k$-matrix V_1 is block-diagonal with exactly $k/2$ blocks of 2×2-matrices

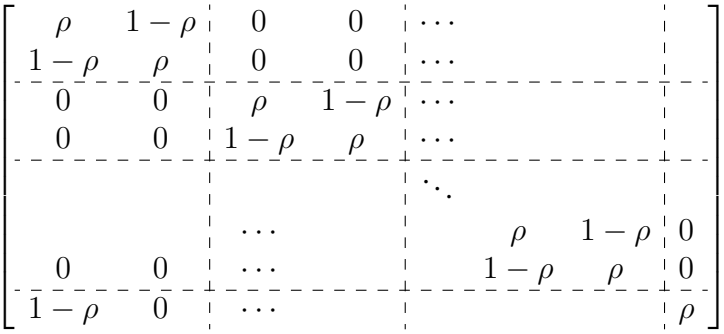
$$\begin{bmatrix} \rho & 1-\rho \\ 1-\rho & \rho \end{bmatrix}.$$

For k odd, the upper-left $(k-1) \times (k-1)$-submatrix of V_1 is similarly structured with $(k-1)/2$ such blocks, and with the kth row being $V_1(0|k-1) = 1-\rho$ and $V_1(k-1|k-1) = \rho$.

See Fig. 2.2. Corresponding to $V_1 : \mathcal{Z} \to \mathcal{Z}$ in (2.36), consider the conditionally i.i.d. ρ-QRs



(a) k even



(b) k odd

Figure 2.2: Add-noise ρ-QR V_1.

$\{Z_t = F_t(X)\}_{t=1}^n$ given by (2.29) as

$$P(F_1(X) = i_1, \ldots, F_n(X) = i_n | X = x) = \prod_{t=1}^{n} V_1(i_t | f(x)). \tag{2.37}$$

For $0 \leq \rho \leq 1$, set

$$\Lambda_n(\rho) = P\left(\text{Bin}(n, \rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right) \left(\sum_{i \in \mathcal{Z}:\, i \text{ odd}} P_X(x_i^*) \right), \quad n \geq 1 \tag{2.38}$$

and note that $0 \leq \Lambda_n(\rho) \leq 1$.

Theorem 2.4. *Let* $0.5 < \rho \leq 1$. *For every* $n \geq 1$, *the add-noise* ρ*-QRs* $\{Z_t = F_t(X)\}_{t=1}^n$

in (2.37) *with* $V_1 : \mathcal{Z} \to \mathcal{Z}$ *in* (2.36) *yield privacy*

$$\pi_\rho\left(V_1^n\right) \geq 1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) + \Lambda_n(\rho). \tag{2.39}$$

Remarks:

(i) Observe that when P_X is the uniform pmf on $\mathcal{X}$, for $n = 1$, $\pi_\rho\left(V_1\right) = 1 - k\rho/r = \pi(\rho)$, the latter by (2.18). On the other hand, $\pi_\rho\left(V_1\right)$ can be strictly smaller than $\pi(\rho)$; for instance for $\mathcal{X} = \mathcal{Z} = \{0, 1, 2\}$, $P_X = (0.5, 0.3, 0.2)$, $f(x) = x$, and $\rho = 0.6$, it is straightforward to show that $\pi(\rho) = 0.4$ whereas $\pi_\rho\left(V_1\right) = 0.38$.

(ii) When $f : \mathcal{X} \to \mathcal{X}$ is a one-to-one mapping, we get from (2.39) that

$$\pi_\rho\left(V_1^n\right) \geq \Lambda_n(\rho), \quad 0.5 < \rho \leq 1.$$

(iii) Observe that using the achievability scheme V_1, specified by (2.36), for every realization of the ρ-QR $F_t(X) = i,\ i \in \mathcal{Z}$, $t = 1, \ldots, n$, we can infer that the user's data X will be from a list of size $|f^{-1}(i) \cap f^{-1}\left(i + 1 \bmod k\right)|$ if i is even or $|f^{-1}(i) \cap f^{-1}(i-1)|$ if i is odd. Therefore, even though there is privacy for the exact value of the user data, privacy is lost if the querier seeks only a list containing X [70]. This motivates the concept of list privacy in Chapter 3.

2.4.2.2. Realm $0 \leq \rho \leq 0.5$

Our achievability scheme uses ρ-QRs as in (2.37) with V_1 replaced by $V_2 : \mathcal{Z} \to \mathcal{Z}$, not depending on P_X, which is:

for $0 \le \rho \le 1/k$,

$$V_2(i|j) = \frac{1}{k}, \quad i, j \in \mathcal{Z} \tag{2.40}$$

and for $1/k < \rho \le 0.5$,

$$V_2(i|j) = \begin{cases} \frac{1}{\left\lfloor \frac{1}{\rho} \right\rfloor}, & j = 0, \ldots, \left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor - 1, \;\; i = \left\lfloor \frac{j}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, \left(\left\lfloor \frac{j}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor + 1 \right) \left\lfloor \frac{1}{\rho} \right\rfloor - 1 \\ \frac{1}{k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor}, & j = \left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, k-1, \;\; i = \left\lfloor \frac{j}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, k-1 \\ 0, & \text{otherwise.} \end{cases} \tag{2.41}$$

In particular, for $1/k < \rho \le 0.5$, the $k \times k$-matrix V_2 consists of $\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor$ diagonal blocks of $\left\lfloor \frac{1}{\rho} \right\rfloor \times \left\lfloor \frac{1}{\rho} \right\rfloor$-matrices, each with identical elements equal to $1/\left\lfloor \frac{1}{\rho} \right\rfloor$; and a single "filler" block of size $k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor \times k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor$ with identical elements equal to $1/\left(k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor\right)$. The latter is vacuous if $\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor = k$, i.e., $k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor = 0$. See Fig. 2.3.

$$\left[\begin{array}{ccc:ccc:cc} 1/3 & 1/3 & 1/3 & 0 & 0 & 0 & 0 & 0 \\ 1/3 & 1/3 & 1/3 & 0 & 0 & 0 & 0 & 0 \\ 1/3 & 1/3 & 1/3 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 \end{array}\right]$$

Figure 2.3: Add-noise ρ-QR V_2 for $\rho = 1/3$ and $k = 8$.

Theorem 2.5. *Let* $0 \le \rho \le 0.5$. *For every* $n \ge 1$, *the add-noise* ρ*-QRs* $\{Z_t = F_t(X)\}_{t=1}^n$ *in* (2.37)

with V_1 replaced by $V_2 : \mathcal{Z} \to \mathcal{Z}$ in (2.40), (2.41) yield privacy

$$\pi_\rho\left(V_2^n\right) = \begin{cases} 1 - P_X\left(x^*\right), & 0 \le \rho \le \frac{1}{k} \\ 1 - \sum_{i=0}^{\left\lfloor \frac{k}{\lfloor \frac{1}{\rho} \rfloor} \right\rfloor} P_X\left(x^*_{i\lfloor \frac{1}{\rho} \rfloor}\right), & k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor \neq 0, \quad \frac{1}{k} < \rho \le 0.5 \\ 1 - \sum_{i=0}^{\left\lfloor \frac{k}{\lfloor \frac{1}{\rho} \rfloor} \right\rfloor - 1} P_X\left(x^*_{i\lfloor \frac{1}{\rho} \rfloor}\right), & k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor = 0, \quad \frac{1}{k} < \rho \le 0.5. \end{cases} \tag{2.42}$$

Remarks:

(i) For $0 \le \rho \le 0.5$, the privacy $\pi_\rho\left(V_2^n\right)$ above lacks dependence on n. However, for $0 \le \rho \le 1/k$,

$$\pi_\rho\left(V_2^n\right) = \pi_\rho\left(V_2\right) = 1 - P_X\left(x^*\right) = \pi(\rho)$$

where the last identity is by (2.18). Thus, for $n = 1$, the add-noise ρ-QR with V_2 too achieves ρ-privacy, as did V_o in Theorem 2.2.

(ii) On the other hand, for $1/k < \rho \le 0.5$, V_2 can be strictly inferior to V_o for $n = 1$; for instance, with P_X being the uniform pmf on $\mathcal{X}$, by Theorem 2.5 with $k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor \neq 0$,

$$\pi_\rho\left(V_2\right) = 1 - \left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor + 1 \right) \frac{1}{r} < 1 - \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \frac{1}{r} \le 1 - \frac{\rho k}{r} = \pi(\rho) = \pi(V_o)$$

where the last two identities are by Theorem 2.2.

2.4.3. Asymptotic Implications

Theorems 2.3 and 2.4 yield effective upper and lower bounds for $\pi_n(\rho)$. Upon rewriting these bounds with a slight weakening, useful information can be extracted including the limiting behaviour of $\pi_n(\rho)$ as $n \to \infty$. Specifically by Theorem 2.3, for each $0 \leq \rho \leq 1$ and for every $n \geq 1$,

$$\pi_n(\rho) \leq 1 - \sum_{i \in \mathcal{Z}} P_X(x_i^*) + \Gamma_n(\rho) \tag{2.43}$$

and by Theorem 2.4, for $0.5 < \rho \leq 1$ and for every $n \geq 1$,

$$\pi_n(\rho) \geq \pi_\rho\left(V_1^n\right) \geq 1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) + \Lambda_n(\rho). \tag{2.44}$$

For $0.5 < \rho \leq 1$, (2.43) and (2.44) are interpreted as follows. Note that $\pi(1) = 1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)$ is the privacy afforded to the user when the querier has the exact value of $f(X)$. The additional privacy gained by the user due to the ρ-recoverability for $\rho < 1$ is between $\Gamma_n(\rho)$ and $\Lambda_n(\rho)$.

Estimates of $P\left(\text{Bin}(n, \rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right)$ appearing in $\Gamma_n(\rho)$ and $\Lambda_n(\rho)$ (cf. (2.34) and (2.38)) lead to bounds for $\pi_n(\rho)$ in (2.43) and (2.44). Let Ber(α) denote a Bernoulli rv with the probability of "1" being α, $0 \leq \alpha \leq 1$. Hereafter, throughout the dissertation, all logarithms and exponentials are with respect to the base 2.

Lemma 2.6. *(i) For each* $0.5 \leq \rho \leq 1$ *and every* $n \geq 1$,

$$\frac{1}{n+1} \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle\| \text{Ber}\left(\rho\right)\right)\right] \leq P\left(\text{Bin}(n, \rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right)$$

$$\leq \left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}(\rho)\right)\right].$$

(ii) For each $0 \leq \rho \leq 0.5$ *and for every* $n \geq 1$,

$$P\left(\text{Bin}(n,\rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right) \geq 1 - \rho.$$

Proof: See Appendix A.1. ■

Lemma 2.6(i) leads to the following useful bounds for $\pi_n(\rho)$.

Proposition 2.7. *For each* $0.5 < \rho \leq 1$,

(i)

$$\pi_n(\rho) \leq 1 - \sum_{i \in \mathcal{Z}} P_X(x_i^*) + \left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}(\rho)\right)\right] \sum_{i \in \mathcal{Z}} P_X(x_i^*)$$

for all n *such that*

$$\left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}(\rho)\right)\right] \leq 1 - \min\{\rho, \rho_c\}.$$

(ii) for every $n \geq 1$,

$$\begin{aligned}
&\pi_n(\rho) \geq \pi_\rho(V_1^n) \\
&\geq 1 - \sum_{i \in \mathcal{Z}} P_X(x_i^*) + \frac{1}{n+1} \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}(\rho)\right)\right] \left(\sum_{i \in \mathcal{Z}:\, i \text{ odd}} P_X(x_i^*)\right).
\end{aligned}$$

Proof: The assertions follow directly by applying the upper and lower bounds in Lemma 2.6(i) to the right-sides of (2.43) and (2.44), respectively, and recalling (2.34) and (2.38). ■

We close this section with the asymptotic implications of Theorems 2.3, 2.4, 2.5 and Proposition 2.7. Considering first the (more interesting) realm $0.5 < \rho \leq 1$, the upper bounds for $\pi_n(\rho)$ in Theorem 2.3 and Proposition 2.7(i), as also the lower bounds in Theorem 2.4 and Proposition 2.7(ii), converge according to

$$\lim_n \pi_n(\rho) = 1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) = \pi(1), \quad 0.5 < \rho \leq 1 \tag{2.45}$$

(see Remark (i) after Theorem 2.2), i.e., the error probability of a MAP estimator of X on the basis of a knowledge of $f(X)$. Furthermore, both the sets of bounds converge at the same exponential rate in n with the (n-dependent) exponent itself tending to $D(\text{Ber}(0.5)||\text{Ber}(\rho)) > 0$. Thus, in the realm $0.5 < \rho \leq 1$, the asymptotic privacy in (2.45) is that which is provided to the user when the querier forms an accurate MAP estimate of $f(X)$ w.p. 1 from ρ-QRs $\{F_t(X)\}_{t=1}^n$, followed by a MAP estimate of X that is compatible with the estimated $f(X)$.

In the realm $0 \leq \rho \leq 0.5$, the upper bound for $\pi_n(\rho)$ in Theorem 2.3, by Lemma 2.6(ii), equals

$$1 - \max\{\rho_c, \rho\} \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) \tag{2.46}$$

for *all* $n \geq 1$, which is the ρ-privacy for $n = 1$ in Theorem 2.2. As remarked after Theorem 2.5, this upper bound is unattainable, in general, by add-noise ρ-QRs $\{F_t(X)\}_{t=1}^n$ with $V_2 : \mathcal{Z} \to \mathcal{Z}$ in (2.40), (2.41). Hence, an interpretation as above in the complementary realm is lacking as is

the answer to the putative tightness (or not) of the mentioned bound. However, since

$$\pi_n(\rho) \geq \pi_\rho\left(V_2^n\right) > 1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) = \pi(1),$$

where the strict inequality is evident from Theorem 2.5 (by comparing the expressions in (2.42) with $1 - \sum\limits_{i \in \mathcal{Z}} P_X\left(x_i^*\right)$), we can conclude that no accurate estimate of $f(X)$ w.p. 1 is possible from ρ-QRs $\{F_t(X)\}_{t=1}^n$ for any n, unlike for $0.5 < \rho \leq 1$.

2.5. Predicate Privacy

We consider a model where privacy is sought for a predicate of the user's data which is a specified attribute of it described in terms of a given mapping. The user designs the ρ-QR that maximizes the "predicate privacy" of the data, i.e., minimizes the likelihood of the querier learning the predicate of the user's data from the ρ-QR. Since such predicate learning by the querier is less difficult than learning the data itself, predicate privacy is more stringent than data privacy.

Our aim is to derive ρ-privacy for a predicate $Y = h(X)$ of X, where $h : \mathcal{X} \to \mathcal{Y} = \{0, 1, \ldots, m-1\},\ 2 \leq m \leq r$, is a given mapping.

Definition 2.6. Given a (predicate) mapping $h : \mathcal{X} \to \mathcal{Y} = \{0, 1, \ldots, m-1\}$, $2 \leq m \leq r$, the *predicate privacy* of a ρ-QR $F\left(X\right)$ (or equivalently ρ-QR W) satisfying (2.1) (respectively (2.2)) is

$$\pi'_\rho(F) = \pi'_\rho(W) \triangleq \min_{g'}\ P(g'\left(Z\right) \neq Y) \tag{2.47}$$

where the minimum is over all estimators $g' : \mathcal{Z} \to \mathcal{Y}$ of $Y = h(X)$ on the basis of Z. Since the minimum in (2.47) is attained by a MAP estimator

$g'_{MAP} = g'_{MAP(W)} : \mathcal{Z} \to \mathcal{Y}$ given by

$$g'_{MAP(W)}(i) = \arg \max_{y \in \mathcal{Y}} \; P\left(Y = y, Z = i\right)$$

$$= \arg \max_{y \in \mathcal{Y}} \sum_{x \in h^{-1}(y)} P_X\left(x\right) W\left(i|x\right), \quad i \in \mathcal{Z}, \quad (2.48)$$

we have that (2.47) equals $P(g'_{MAP(W)}(Z) \neq Y)$. For $0 \leq \rho \leq 1$, the maximum predicate privacy that can be attained by a ρ-QR is termed *predicate ρ-privacy* and denoted by $\pi'(\rho)$, i.e.,

$$\pi'\left(\rho\right) = \max_{\substack{W: W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \pi'_{\rho}(W). \quad (2.49)$$

When $h : \mathcal{X} \to \mathcal{Y} = \mathcal{X}$ is the identity mapping, predicate ρ-privacy in (2.49) specializes to ρ-privacy in (2.11). With h being the identity mapping, since we get from (2.48) that $P\left(g'_{MAP(W)}(Z) \neq Y\right) \leq P\left(g_{MAP(W)}(Z) \neq X\right)$, it holds that $\pi'(\rho) \leq \pi(\rho),\ 0 \leq \rho \leq 1$.

Theorem 2.8 below provides an exact characterization of $\pi'(\rho)$. Its proof builds on that for $\pi(\rho)$ in Theorem 2.2 and is relegated to Appendix A.3. Define

$$j^* = \arg \max_{j \in \mathcal{Y}} \; P_X\left(h^{-1}(j)\right),$$

$$P_X(i,j) = P_X\left(f^{-1}(i) \cap h^{-1}(j)\right), \quad i \in \mathcal{Z}, \quad j \in \mathcal{Y}, \quad (2.50)$$

$$j_i^* = \arg \max_{j \in \mathcal{Y}} \; P_X(i,j), \quad i \in \mathcal{Z} \quad (2.51)$$

and

$$\rho'_c = \frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right)}, \quad (2.52)$$

where the maxima above need not be attained uniquely. Observe that $\max\left\{\frac{1}{m}, \frac{1}{k}\right\} \leq \rho_c' \leq 1$. The right inequality is by

$$\rho_c' = \frac{\sum\limits_{i \in \mathcal{Z}} P_X\left(i, j^*\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right)} \leq 1$$

while the left inequality follows from

$$\frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right)} \geq \frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(f^{-1}(i)\right)} = P_X\left(h^{-1}(j^*)\right) \geq \frac{1}{m}$$

and

$$\frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right)} \geq \frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(h^{-1}(j_i^*)\right)} \geq \frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{i \in \mathcal{Z}} P_X\left(h^{-1}(j^*)\right)} = \frac{1}{k}.$$

The following ρ-QR $W_o' : \mathcal{X} \to \mathcal{Z}$ specified for $x \in \mathcal{X}$, $i \in \mathcal{Z}$, $j \in \mathcal{Y}$, is relevant to the achievablity proof of predicate ρ-privacy below.

For $\rho_c' = 1$

$$W_o'(i|x) = \mathbb{1}\left(f(x) = i\right) \tag{2.53}$$

and for $\rho_c' < 1$,

$$W_o'(i|x) = \begin{cases} \max\{\rho_c', \rho\} + \left(1 - \max\{\rho_c', \rho\}\right) \frac{P_X\left(i, j_i^*\right) - P_X(i,j)}{\sum\limits_{l \in \mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)}, & i = f(x), \;\; j = h(x) \\ \left(1 - \max\{\rho_c', \rho\}\right) \frac{P_X\left(i, j_i^*\right) - P_X(i,j)}{\sum\limits_{l \in \mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)}, & i \neq f(x), \;\; j = h(x). \end{cases} \tag{2.54}$$

Theorem 2.8. *Predicate ρ-privacy equals*

$$\pi'(\rho) = 1 - \max\left\{P_X\left(h^{-1}(j^*)\right), \rho \sum_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right)\right\} \tag{2.55}$$

$$= 1 - \max\{\rho_c', \rho\} \sum_{i \in \mathcal{Z}} P_X(i, j_i^*), \quad 0 \le \rho \le 1. \tag{2.56}$$

Furthermore, predicate ρ-privacy is achieved by the ρ-QR W_o' in (2.53) *and* (2.54).

Remarks:

(i) Note that W_o' has the property that for each i in $\mathcal{Z}$, j in $\mathcal{Y}$, all rows corresponding to x in $f^{-1}(i) \cap h^{-1}(j)$ are identical. Pursuant to Lemma 2.1, W_o' can be interpreted as an add-noise ρ-QR obtained by adding to $f(X)$ a noise N that satisfies the Markov condition $N \multimap f(X), h(X) \multimap X$.

(ii) When h is the identity mapping, W_o' in (2.54) *does not* coincide with W_o in (2.16); in fact, W_o' reduces to

$$W_o''(i|x) = \begin{cases} \max\{\rho_c, \rho\} + (1 - \max\{\rho_c, \rho\}) \frac{P_X(x_i^*) - P_X(x)}{\sum_{l \in \mathcal{Z}} P_X(x_l^*) - P_X(x)}, & i = f(x), \\ (1 - \max\{\rho_c, \rho\}) \frac{P_X(x_i^*) - P_X(x)}{\sum_{l \in \mathcal{Z}} P_X(x_l^*) - P_X(x)}, & i \ne f(x). \end{cases}$$

By Theorem 2.8 and Theorem 2.2, $\pi_\rho'(W_o'') = \pi(\rho) = \pi_\rho(W_o)$. On the other hand, and unlike W_o, the ρ-QR W_o'' is not of the add-noise type in the sense of Definition 2.2 and also depends on the entirety of P_X.

(iii) From (2.50), (2.51) and recalling (2.14), in the right-side of (2.55),

$$P_X\left(h^{-1}(j^*)\right) \le 1 - P_X(x_*) \quad \text{and} \quad \sum_{i \in \mathcal{Z}} P_X(i, j_i^*) \le \sum_{i \in \mathcal{Z}} P_X\left(f^{-1}(i)\right) = 1,$$

so that

$$\pi'(\rho) \geq 1 - \max\{1 - P_X(x_*), \rho\}, \quad 0 \leq \rho \leq 1. \tag{2.57}$$

From (2.57), for a given mapping $f : \mathcal{X} \to \mathcal{Z}$ and user data pmf P_X, we can characterize the worst-case predicate mapping $h : \mathcal{X} \to \mathcal{Y} = \{0, 1, \ldots, m-1\},\ 2 \leq m \leq r$, for $\pi'(\rho),\ 0 \leq \rho \leq 1$. When $1 - P_X(x_*) \leq \rho \leq 1$, it can be verified that the lower bound in (2.57) is attained by the predicate mapping h given by

$$Y = h(X) = \delta(f(X)), \text{ where } \delta : \mathcal{Z} \to \mathcal{Y} = \{0, 1, \ldots, m-1\},\ 2 \leq m \leq k, \tag{2.58}$$

is any mapping. Next, when $0 \leq \rho \leq 1 - P_X(x_*)$, the lower bound in (2.57) is attained by the binary-valued mapping $h : \mathcal{X} \to \{0, 1\}$ given by

$$h(x) = \begin{cases} 0, & x = x_* \\ 1, & x \neq x_*. \end{cases} \tag{2.59}$$

The worst-case predicate mappings for $\pi'(\rho),\ 0 \leq \rho \leq 1$, described above, afford the following interpretation. When $\rho \cong 1$, the querier has full knowledge of $f(X)$ and so can compute any function of $f(X)$. Therefore, for $1 - P_X(x_*) \leq \rho \leq 1$, the worst-case predicate mapping for $\pi'(\rho)$ takes the form of (2.58). For $\rho \cong 0$, the ρ-QR for computing $f(X)$ is less reliable to the querier. Therefore, for $0 \leq \rho \leq 1 - P_X(x_*)$, the worst-case predicate mapping for the user is the one that has the lowest atomicity, i.e., a binary-valued mapping, specifically (2.59).

(iv) Theorem 2.8 covers the setting when privacy is sought for a randomized function Y of the

data X with the (finite-valued) rvs X, Y having a given joint pmf. Specifically ρ-privacy for Y corresponds to predicate ρ-privacy in Theorem 2.8 with $\bar{X}$, $h(\bar{X})$, $f(\bar{X})$ and $F(\bar{X})$, where

$$\bar{X} = (X, Y), \;\; h(\bar{X}) = Y, \;\; f(\bar{X}) = f(X), \;\; F(\bar{X}) = Z,$$

(with an abuse of notation in f).

(v) In a similar vein, Theorem 2.8 also covers the setting with "private data X, correlated nonprivate data Y and publicly released data Z" alluded to in Chapter 1. Formally, ρ-privacy for the mentioned setting equals predicate ρ-privacy in Theorem 2.8 applied to $\tilde{X}$, $h(\tilde{X})$, $f(\tilde{X})$ and $F(\tilde{X})$, where

$$\tilde{X} = (X, Y), \;\; h(\tilde{X}) = X, \;\; f(\tilde{X}) = Y, \;\; F(\tilde{X}) = Z.$$

2.6. Converse and Achievability Theorems

2.6.1. Converse Proof

Proof of Theorem 2.3: For $W_1, \ldots, W_n$ satisfying (2.2),

$$\begin{aligned} P(g_{\text{MAP}\,(W_1,\ldots,W_n)}(Z_1,\ldots,Z_n) = X) &\geq P(g_{\text{MAP}\,(W_1)}(Z_1) = X) \\ &\geq \max\left\{ P_X(x^*), \rho \sum_{i \in \mathcal{Z}} P_X(x_i^*) \right\} \end{aligned} \tag{2.60}$$

by (2.22). Also,

$$P(g_{\text{MAP}\,(W_1,\ldots,W_n)}\,(Z_1,\ldots,Z_n)=X)=\sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n}\max_{x\in\mathcal{X}}\;P_X\,(x)\prod_{t=1}^{n}W_t\,(i_t|x)\,. \tag{2.61}$$

For each $i\in\mathcal{Z}$ and for $l=\left\lfloor\frac{n}{2}\right\rfloor+1,\ldots,n$, set

$$\mathcal{A}_l(i)=\{(i_1,\ldots,i_n)\in\mathcal{Z}^n : i \text{ occurs } l \text{ times in } (i_1,\ldots,i_n)\}\,. \tag{2.62}$$

Then, in (2.61),

$$\begin{aligned}P(g_{\text{MAP}\,(W_1,\ldots,W_n)}\,(Z_1,\ldots,Z_n)=X)&\geq\sum_{i\in\mathcal{Z}}\sum_{l=\left\lfloor\frac{n}{2}\right\rfloor+1}^{n}\sum_{(i_1,\ldots,i_n)\in\mathcal{A}_l(i)}\max_{x\in\mathcal{X}}\;P_X\,(x)\prod_{t=1}^{n}W_t\,(i_t|x)\\&\geq\sum_{i\in\mathcal{Z}}P_X\,(x_i^*)\sum_{l=\left\lfloor\frac{n}{2}\right\rfloor+1}^{n}\sum_{(i_1,\ldots,i_n)\in\mathcal{A}_l(i)}\prod_{t=1}^{n}W_t\,(i_t|x_i^*)\\&=\sum_{i\in\mathcal{Z}}P_X\,(x_i^*)\,s_i(n)\end{aligned} \tag{2.63}$$

where

$$s_i(n)=\sum_{l=\left\lfloor\frac{n}{2}\right\rfloor+1}^{n}s_i^l(n) \tag{2.64}$$

with

$$s_i^l(n)=\sum_{(i_1,\ldots,i_n)\in\mathcal{A}_l(i)}\prod_{t=1}^{n}W_t\,(i_t|x_i^*)\,,\quad i\in\mathcal{Z}. \tag{2.65}$$

To understand the functional dependence of $s_i^l(n)$ on $(W_1\,(i|x_i^*)\,,\ldots,W_n\,(i|x_i^*)\,)$, consider as an instance all $(i_1,\ldots,i_n)\in\mathcal{A}_l(i)$ with $i_1=\ldots=i_l=i$ and $i_t\neq i$, $t=l+1,\ldots,n$. The

corresponding sum for such $(i_1, \ldots, i_n) \in \mathcal{A}_l(i)$ in (2.65) equals

$$\left(\prod_{t=1}^{l} W_t\left(i|x_i^*\right)\right) \sum_{\substack{(i_{l+1},\ldots,i_n)\in\mathcal{Z}^{n-l} \\ i_t\neq i,\ t=l+1,\ldots,n}} \prod_{t=l+1}^{n} W_t\left(i_t|x_i^*\right) = \left(\prod_{t=1}^{l} W_t\left(i|x_i^*\right)\right) \prod_{t=l+1}^{n} \left(1 - W_t\left(i|x_i^*\right)\right).$$

In this manner, we observe that $s_i^l(n)$ reduces to a sum of $\binom{n}{l}$ terms (corresponding to the locations of l is), each of which is a product of $W_t\left(i|x_i^*\right)$-terms for l locations of t in $\{1, \ldots, n\}$ corresponding to occurrences of i, and $\left(1 - W_t\left(i|x_i^*\right)\right)$-terms in the remaining $(n - l)$ locations. Thus, $s_i^l(n)$ is a function of $\left(W_1\left(i|x_i^*\right), \ldots, W_n\left(i|x_i^*\right)\right)$.

We seek a suitable lower bound for $s_i(n)$ in terms of ρ and n, to which end we make the

Claim: For $i \in \mathcal{Z}$, $s_i(n)$ is a nondecreasing function of each $W_t\left(i|x_i^*\right)$, $t = 1, \ldots, n$.

By (2.64), the claim and the observation following (2.65), $s_i(n)$ is bounded below in an identical manner for $i = 0, 1, \ldots, k-1$, upon replacing each $W_1\left(i|x_i^*\right), \ldots, W_n\left(i|x_i^*\right)$ by ρ, in accordance with (2.2). By said observation, we have from (2.64) for $i = 0, 1, \ldots, k-1$ that

$$\begin{aligned} s_i(n) &\geq \sum_{l=\left\lfloor \frac{n}{2} \right\rfloor + 1}^{n} \binom{n}{l} \rho^l (1-\rho)^{n-l} \\ &= P\left(\text{Bin}(n, \rho) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1\right). \end{aligned} \tag{2.66}$$

Then from (2.63),

$$P(g_{\text{MAP}\,(W_1,\ldots,W_n)}(Z_1, \ldots, Z_n) = X) \geq \left(\sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right)\right) P\left(\text{Bin}(n, \rho) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1\right). \tag{2.67}$$

Combining (2.60) and (2.67), we get

$$
\begin{aligned}
&P(g_{\text{MAP}\,(W_1,\ldots,W_n)}\,(Z_1,\ldots,Z_n)=X)\\
&\geq \max\left\{P_X\,(x^*)\,,\left(\sum_{i\in\mathcal{Z}}P_X\,(x_i^*)\right)\max\left\{\rho,P\left(\text{Bin}(n,\rho)\geq\left\lfloor\frac{n}{2}\right\rfloor+1\right)\right\}\right\}\\
&=\max\left\{\rho_c,\max\left\{\rho,P\left(\text{Bin}(n,\rho)\geq\left\lfloor\frac{n}{2}\right\rfloor+1\right)\right\}\right\}\sum_{i\in\mathcal{Z}}P_X\,(x_i^*)\\
&=\sum_{i\in\mathcal{Z}}P_X\,(x_i^*)-\Gamma_n(\rho)
\end{aligned}
$$

from which the assertion of the theorem follows since $W_1,\ldots,W_n$ were arbitrary subject to (2.2).

It remains to establish the claim, and it suffices to do so with $i=0,\,t=1$, i.e., we show that $s_0(n)$ is nondecreasing in $W_1\,(0|x_0^*)$. From the observation following (2.65), $s_0^l(n)$ is a sum of $\binom{n}{l}$ terms, each of which is a product of $W_t\,(0|x_0^*)$-terms for l locations of t in $\{1,\ldots,n\}$ where $0s$ occur and $(1-W_t\,(0|x_0^*)\,)$-terms for the remaining $(n-l)$ locations. Thus, each of these $\binom{n}{l}$ terms will have either $W_1\,(0|x_0^*)$ or $1-W_1\,(0|x_0^*)$ in it (depending on whether or not $i_1=0$). The latter possibility yields a term with $-W_1\,(0|x_0^*)$ which is seen to be canceled by a suitable term from $s_0^{l+1}(n)$. Also, $s_0^n(n)=W_1\,(0|x_0^*)\prod_{t=2}^{n}W_t\,(0|x_0^*)$. Thus, $s_0(n)$ consists of terms with $+W_1\,(0|x_0^*)$ or with no $W_1\,(0|x_0^*)$, and thereby is linear and nondecreasing in $W_1\,(0|x_0^*)$. This proves the claim. ■

2.6.2. Achievability Proofs

The choice of $V_1:\mathcal{Z}\to\mathcal{Z}$ (2.36) for the proof of Theorem 2.4 takes its cue from the proof of Theorem 2.3. The first lower bound in (2.63) results upon discarding those $(i_1,\ldots,i_n)$ in $\mathcal{Z}^n,\ n\geq 1$, in which the most frequent symbol from $\mathcal{Z}$ occurs no more than $\lfloor\frac{n}{2}\rfloor$ times. The

specific choice of V_1 in (2.36) ensures that the number of such occurrences is at least $\lfloor \frac{n}{2} \rfloor + 1$.

Proof of Theorem 2.4: We have

$$P(g_{\text{MAP}(V_1^n)}(Z_1, \ldots, Z_n) = X) = \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{x\in\mathcal{X}} P_X(x) \prod_{t=1}^{n} V_1(i_t|f(x)). \tag{2.68}$$

When $\rho = 1$, $V_1 : \mathcal{Z} \to \mathcal{Z}$ in (2.36) has 1s along its diagonal and 0s elsewhere. Hence, the right-side of (2.68) equals $\sum_{i\in\mathcal{Z}} P_X(x_i^*)$. Since $\Lambda_n(1) = 0$, (2.39) holds (with equality).

Hereafter we take $0.5 < \rho < 1$. By the form of V_1 in (2.36), for each $x \in \mathcal{X}$ only those $(i_1, \ldots, i_n) \in \mathcal{Z}^n$ yield nonzero contributions in (2.68) when consisting of $i_t = f(x)$; and $i_t = f(x)+1 \bmod k$ for $f(x)$ even or $i_t = f(x)-1$ for $f(x)$ odd. Accordingly, we distinguish between the cases when k is even or it is odd.

(i) k *even*: For $i = 0, 2, \ldots, k-2$, set

$$\mathcal{B}_n(i) = \{(i_1, \ldots, i_n) \in \mathcal{Z}^n : i_t = i \text{ or } i_t = i+1\}. \tag{2.69}$$

Then in (2.68),

$$P(g_{\text{MAP}(V_1^n)}(Z_1, \ldots, Z_n) = X) = \sum_{i=0,2,\ldots,k-2} \sum_{(i_1,\ldots,i_n)\in\mathcal{B}_n(i)} \max_{x\in f^{-1}(i)\cup f^{-1}(i+1)} P_X(x) \prod_{t=1}^{n} V_1(i_t|f(x)) \tag{2.70}$$

where for each $i = 0, 2, \ldots, k-2$ and for each $(i_1, \ldots, i_n) \in \mathcal{B}_n(i)$,

$$\max_{x\in f^{-1}(i)\cup f^{-1}(i+1)} P_X(x) \prod_{t=1}^{n} V_1(i_t|f(x)) =$$

$$\max\left\{P_X(x_i^*)\rho^{l_i(i_1,\ldots,i_n)}\left(1-\rho\right)^{n-l_i(i_1,\ldots,i_n)}, P_X(x_{i+1}^*)\left(1-\rho\right)^{l_i(i_1,\ldots,i_n)}\rho^{n-l_i(i_1,\ldots,i_n)}\right\} \quad (2.71)$$

with $l_i\left(i_1,\ldots,i_n\right)$ being the number of is in $(i_1,\ldots,i_n)$. The first term in $\{\cdot,\cdot\}$ above is no larger than the second if

$$l_i\left(i_1,\ldots,i_n\right) \leq \tau_n(i,\rho) \triangleq \left\lfloor \frac{1}{2}\left(n - \frac{\log\frac{P\left(x_i^*\right)}{P\left(x_{i+1}^*\right)}}{\log\frac{\rho}{1-\rho}}\right)\right\rfloor.$$

Since $0.5 < \rho < 1$, we observe by the assumption in (2.35) that $\tau_n(i,\rho) \leq \lfloor\frac{n}{2}\rfloor$; and $\tau_n(i,\rho) \leq \frac{n}{2}-1$ for even [1] n.

Then for $i = 0, 2, \ldots, k-2$ and when $\tau_n(i,\rho) \geq 0$, by (2.71) we get in (2.70) that

$$\begin{aligned}
&\sum_{(i_1,\ldots,i_n)\in\mathcal{B}_n(i)} \max_{x\in f^{-1}(i)\cup f^{-1}(i+1)} P_X(x)\prod_{t=1}^{n} V_1(i_t|f(x)) \\
&= P_X(x_{i+1}^*)\sum_{l=0}^{\tau_n(i,\rho)}\binom{n}{l}\left(1-\rho\right)^l\rho^{n-l} + P_X(x_i^*)\sum_{l=\tau_n(i,\rho)+1}^{n}\binom{n}{l}\rho^l\left(1-\rho\right)^{n-l} \\
&= P_X(x_{i+1}^*)\sum_{l=n-\tau_n(i,\rho)}^{n}\binom{n}{l}\rho^l\left(1-\rho\right)^{n-l} + P_X(x_i^*)\sum_{l=\tau_n(i,\rho)+1}^{n}\binom{n}{l}\rho^l\left(1-\rho\right)^{n-l} \\
&\leq P_X(x_{i+1}^*)\sum_{l=\lfloor\frac{n}{2}\rfloor+1}^{n}\binom{n}{l}\rho^l\left(1-\rho\right)^{n-l} + P_X(x_i^*)\sum_{l=0}^{n}\binom{n}{l}\rho^l\left(1-\rho\right)^{n-l} \qquad (2.72)
\end{aligned}$$

where the first term in the previous inequality readily follows from the observation above, since

$$n-\tau_n(i,\rho) \geq \begin{cases} n-\lfloor\frac{n}{2}\rfloor \geq \lfloor\frac{n}{2}\rfloor+1 \text{ for odd } n \\ \\ \frac{n}{2}+1 \text{ for even } n. \end{cases}$$

[1] When $P\left(x_i^*\right) = P\left(x_{i+1}^*\right)$, we get $\tau_n(i,\rho) = n/2$ for even n. In this case, replacing $\tau_n(i,\rho) = n/2$ by $\tau_n(i,\rho) = n/2-1$ does not alter subsequent calculations.

Note that when $\tau_n(i,\rho) < 0$, this upper bound in (2.72) remains valid. By (2.70) and (2.72),

$$
\begin{aligned}
&P(g_{\text{MAP}(V_1^n)}(Z_1,\ldots,Z_n) = X) \\
&\le \sum_{i=0,2,\ldots,k-2} \Bigg[P_X\left(x^*_{i+1}\right) P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) + P_X\left(x^*_i\right) P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) \\
&\quad + P_X\left(x^*_i\right) P\left(\text{Bin}(n,\rho) \le \left\lfloor \frac{n}{2} \right\rfloor\right) \Bigg] \\
&= \left(\sum_{i\in\mathcal{Z}} P_X\left(x^*_i\right) \right) P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) + \left(\sum_{i=0,2,\ldots,k-2} P_X\left(x^*_i\right) \right) P\left(\text{Bin}(n,\rho) \le \left\lfloor \frac{n}{2} \right\rfloor\right)
\end{aligned}
\tag{2.73}
$$

$$
= \sum_{i\in\mathcal{Z}} P_X\left(x^*_i\right) - \Lambda_n(\rho). \tag{2.74}
$$

(ii) k *odd*: For $i = 0, 2, \ldots, k-3$, set $\mathcal{B}_n(i)$ as in (2.69), and

$$
\mathcal{B}_n(k-1) = \{ (i_1,\ldots,i_n) \in \mathcal{Z}^n : i_t = 0 \text{ or } i_t = k-1 \}.
$$

Then

$$
\begin{aligned}
&P(g_{\text{MAP}(V_1^n)}(Z_1,\ldots,Z_n) = X) \\
&\le \sum_{i=0,2,\ldots,k-3} \sum_{(i_1,\ldots,i_n)\in\mathcal{B}_n(i)} \max_{x\in f^{-1}(i)\cup f^{-1}(i+1)} P_X(x) \prod_{t=1}^n V_1(i_t|f(x)) \qquad (2.75) \\
&\quad + \sum_{(i_1,\ldots,i_n)\in\mathcal{B}_n(k-1)} \max_{x\in f^{-1}(k-1)} P_X(x) \prod_{t=1}^n V_1(i_t|f(x)) \\
&\le \left(\sum_{i=0}^{k-2} P_X\left(x^*_i\right) \right) P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) + \sum_{i=0,2,\ldots,k-3} P_X\left(x^*_i\right) P\left(\text{Bin}(n,\rho) \le \left\lfloor \frac{n}{2} \right\rfloor\right) \\
&\quad + P_X\left(x^*_{k-1}\right) \left(P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) + P\left(\text{Bin}(n,\rho) \le \left\lfloor \frac{n}{2} \right\rfloor\right) \right)
\end{aligned}
$$

$$= \left(\sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) \right) P\left(\text{Bin}(n,\rho) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1 \right) + \left(\sum_{i=0,2,\ldots,k-1} P_X\left(x_i^*\right) \right) P\left(\text{Bin}(n,\rho) \leq \left\lfloor \frac{n}{2} \right\rfloor \right)$$

$$= \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right) - \Lambda_n(\rho) \tag{2.76}$$

where in the inequality above, the first two terms on the right-side obtain *a la* (2.73). When $(i_1, \ldots, i_n) = (0, \ldots, 0)$ (the all-zero sequence), the maximum in (2.75) is over x in $f^{-1}(0) \cup f^{-1}(1) \cup f^{-1}(k-1)$. The preceding calculations are, in effect over x in $f^{-1}(0)$, and are justified since $P_X\left(x_0^*\right) \rho^n \geq P_X\left(x_1^*\right)(1-\rho)^n \geq P_X\left(x_{k-1}^*\right)(1-\rho)^n$ for $0.5 \leq \rho \leq 1$.

The assertion of the theorem holds by (2.74) and (2.76). ■

Proof of Theorem 2.5: We have

$$P(g_{\text{MAP}(V_2^n)}(Z_1, \ldots, Z_n) = X) = \sum_{(i_1,\ldots,i_n) \in \mathcal{Z}^n} \max_{x \in \mathcal{X}} P_X(x) \prod_{t=1}^{n} V_2(i_t | f(x)). \tag{2.77}$$

When $0 \leq \rho \leq 1/k$, we get from (2.40) that

$$P(g_{\text{MAP}(V_2^n)}(Z_1, \ldots, Z_n) = X) = P_X\left(x^*\right)$$

so that $\pi_\rho\left(V_2^n\right) = 1 - P_X\left(x^*\right)$. Considering next $1/k < \rho \leq 0.5$, by the form of V_2 in (2.41), for each

$$x \in \mathcal{X} \setminus \left\{ f^{-1}\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor \right) \cup \ldots \cup f^{-1}(k-1) \right\}$$

only those $(i_1, \ldots, i_n) \in \mathcal{Z}^n$ yield nonzero contributions in (2.77) when

$$i_t \in \left\{ \left\lfloor \frac{f(x)}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, \left(\left\lfloor \frac{f(x)}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor + 1 \right) \left\lfloor \frac{1}{\rho} \right\rfloor - 1 \right\}, \quad t = 1, \ldots, n,$$

and for each

$$x \in \left\{ f^{-1}\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor \right) \cup \ldots \cup f^{-1}(k-1) \right\}$$

only those $(i_1, \ldots, i_n) \in \mathcal{Z}^n$ yield nonzero contributions in (2.77) when

$$i_t \in \left\{ \left\lfloor \frac{f(x)}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, k-1 \right\}, \quad t = 1, \ldots, n.$$

For $i = 0, \ldots, \left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1 \right)$, set

$$\mathcal{C}_n(i) = \left\{ (i_1, \ldots, i_n) \in \mathcal{Z}^n : i_t \in \left\{ i \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, (i+1) \left\lfloor \frac{1}{\rho} \right\rfloor - 1 \right\} \right\}$$

and, when the filler block above exists,

$$\mathcal{C}_n \left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \right) = \left\{ (i_1, \ldots, i_n) \in \mathcal{Z}^n : i_t \in \left\{ \left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor, \ldots, k-1 \right\} \right\}.$$

Then in (2.77), with the filler block existing

$$\begin{aligned}
& P\left(g_{\text{MAP}(V_2^n)}\left(Z_1, \ldots, Z_n\right) = X \right) \\
& = \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1} \sum_{(i_1,\ldots,i_n) \in \mathcal{C}_n(i)} \max_{x \in f^{-1}\left(i \left\lfloor \frac{1}{\rho} \right\rfloor\right) \cup \ldots \cup f^{-1}\left((i+1)\left\lfloor \frac{1}{\rho} \right\rfloor - 1\right)} P_X(x) \prod_{t=1}^{n} V_2(i_t | f(x)) \\
& \quad + \sum_{(i_1,\ldots,i_n) \in \mathcal{C}_n\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \right)} \max_{x \in f^{-1}\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor \right) \cup \ldots \cup f^{-1}(k-1)} P_X(x) \prod_{t=1}^{n} V_2(i_t | f(x))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1} \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n(i)} \max_{x\in f^{-1}\left(i\left\lfloor \frac{1}{\rho} \right\rfloor\right)\cup\ldots\cup f^{-1}\left((i+1)\left\lfloor \frac{1}{\rho} \right\rfloor - 1\right)} P_X(x) \left(\frac{1}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \\
&\quad + \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor\right)} \max_{x\in f^{-1}\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor\right)\cup\ldots\cup f^{-1}(k-1)} P_X(x) \left(\frac{1}{k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \\
&= \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1} \left(\frac{1}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n(i)} \max_{x\in f^{-1}\left(i\left\lfloor \frac{1}{\rho} \right\rfloor\right)\cup\ldots\cup f^{-1}\left((i+1)\left\lfloor \frac{1}{\rho} \right\rfloor - 1\right)} P_X(x) \\
&\quad + \left(\frac{1}{k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor\right)} \max_{x\in f^{-1}\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor\right)\cup\ldots\cup f^{-1}(k-1)} P_X(x) \\
&= \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1} \left(\frac{1}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n(i)} P_X\left(x^*_{i\left\lfloor \frac{1}{\rho} \right\rfloor} \right) \\
&\quad + \left(\frac{1}{k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor} \right)^n \sum_{(i_1,\ldots,i_n)\in\mathcal{C}_n\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor\right)} P_X\left(x^*_{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor \left\lfloor \frac{1}{\rho} \right\rfloor} \right) \qquad (2.78) \\
&= \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor} P_X\left(x^*_{i\left\lfloor \frac{1}{\rho} \right\rfloor} \right),
\end{aligned}
$$

where (2.78) uses (2.35) and $|\mathcal{C}_n(i)| = \left(\left\lfloor \frac{1}{\rho} \right\rfloor\right)^n$, $\left|\mathcal{C}_n\left(\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor\right)\right| = \left(k \bmod \left\lfloor \frac{1}{\rho} \right\rfloor\right)^n$. In the absence of the filler block, clearly

$$
P\left(g_{\text{MAP}(V_2^n)}(Z_1,\ldots,Z_n) = X\right) = \sum_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho} \right\rfloor} \right\rfloor - 1} P_X\left(x^*_{i\left\lfloor \frac{1}{\rho} \right\rfloor} \right).
$$

The assertion of the theorem follows. ■

2.7. Inadequacy of Repetitions of Optimum Single Query Response for Multiple Query Responses

Theorem 2.2 establishes the optimality of the add-noise ρ-QR $W_o : \mathcal{X} \to \mathcal{Z}$, or equivalently $V_o : \mathcal{Z} \to \mathcal{Z}$, in achieving ρ-privacy $\pi(\rho)$, $0 \leq \rho \leq 1$, for $n = 1$. Upon choosing $W_t = W_o$ or $V_t = V_o$, $t = 1, \ldots, n$, $n \geq 2$, in (2.28) or (2.29), respectively, how does the corresponding privacy $\pi_\rho\left(W_o^n\right)$ or $\pi_\rho\left(V_o^n\right)$ compare with the achievable privacy in Theorems 2.4 and 2.5? In the regime of all suitably large n, we show below that the former does not exceed the latter and, in fact, can be strictly smaller.

To this end, the concept of Chernoff information [16] plays a material role. Given a stochastic matrix $V : \mathcal{Z} \to \mathcal{Z}$, define its *Chernoff radius*, denoted $C(V)$, as the minimum of pairwise Chernoff information quantities:

$$\begin{aligned} C(V) &= \min_{\substack{j \neq j' \\ j, j' \in \mathcal{Z}}} C(j, j') \\ &= \min_{\substack{j \neq j' \\ j, j' \in \mathcal{Z}}} \left[- \min_{0 \leq \lambda \leq 1} \log \left(\sum_{i \in \mathcal{Z}} V(i|j)^\lambda V\left(i|j'\right)^{1-\lambda} \right) \right], \end{aligned} \tag{2.79}$$

noting that $C(V) \geq 0$ with $C(V) > 0$ iff all the rows of V are distinct.

Also useful will be the next two technical lemmas. Let $\tilde{f}(X)$ be a $\mathcal{Z}$-valued rv with pmf

$$P\left(\tilde{f}(X) = i\right) = \frac{P_X(x_i^*)}{\sum\limits_{l \in \mathcal{Z}} P_X\left(x_l^*\right)}, \quad i \in \mathcal{Z}$$

with x_i^*, $i \in \mathcal{Z}$, as in (2.14). Let $\tilde{Z}_t$, $t = 1, \ldots, n$, be conditionally mutually independent

$\mathcal{Z}$-valued rvs conditioned on $\tilde{f}(X)$, with

$$P_{\tilde{Z}_t|\tilde{f}(X)} = V, \quad t = 1, \ldots, n.$$

We use the notation $A \doteq \exp(-nB)$ to mean $\lim_n -\frac{1}{n} \log A = B$ (cf. e.g., [44]).

Lemma 2.9. *For $0 \leq \rho \leq 1$, consider add-noise ρ-QRs $\{F_t(X)\}_{t=1}^{\infty}$ with (2.28) holding for every $n \geq 1$, where $W_t = W$, $t \geq 1$, and $W : \mathcal{X} \to \mathcal{Z}$ has identical rows for all $x \in f^{-1}(i)$, $i \in \mathcal{Z}$, and has associated $V : \mathcal{Z} \to \mathcal{Z}$ in (2.12).*

(i) The corresponding privacy for every $n \geq 1$ is

$$\pi_\rho\left(W^n\right) = \pi_\rho\left(V^n\right) = 1 - \left(\sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)\right) P\left(g_{\text{MAP}\left(V^n\right)}\left(\tilde{Z}_1, \ldots, \tilde{Z}_n\right) = \tilde{f}(X)\right). \quad (2.80)$$

(ii) Furthermore,

$$\pi_\rho\left(V^n\right) - \left(1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)\right) \doteq \exp\left[-nC(V)\right]. \quad (2.81)$$

Proof:

(i)

$$\begin{aligned}
&P\left(g_{\text{MAP}(W^n)}\left(Z_1, \ldots, Z_n\right) = X\right) \\
&= \sum_{(i_1,\ldots,i_n) \in \mathcal{Z}^n} \max_{x \in \mathcal{X}} P_X(x) \prod_{t=1}^{n} W\left(i_t|x\right) \\
&= \sum_{(i_1,\ldots,i_n) \in \mathcal{Z}^n} \max_{\substack{x \in \cup f^{-1}(j) \\ j \in \mathcal{Z}}} P_X(x) \prod_{t=1}^{n} W\left(i_t|x\right)
\end{aligned}$$

$$= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} P_X\left(x_j^*\right) \prod_{t=1}^{n} W\left(i_t|x_j^*\right)$$

$$= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} P_X\left(x_j^*\right) \prod_{t=1}^{n} V\left(i_t|f\left(x_j^*\right)\right), \quad \text{by (2.12)}$$

$$= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} P_X(x_j^*) \prod_{t=1}^{n} V\left(i_t|j\right) \tag{2.82}$$

$$= \left(\sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right)\right) \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} \frac{P_X(x_j^*)}{\sum\limits_{i\in\mathcal{Z}} P_X\left(x_i^*\right)} \prod_{t=1}^{n} V\left(i_t|j\right)$$

$$= \left(\sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right)\right) P\left(g_{\text{MAP}(V^n)}\left(\tilde{Z}_1,\ldots,\tilde{Z}_n\right) = \tilde{f}(X)\right) \tag{2.83}$$

where the third equality above is by the assumed form of W.

The first assertion in (2.80) follows from (2.82) and the second from (2.83).

(ii) By [44, Theorem 2],

$$P\left(g_{\text{MAP}(V^n)}\left(\tilde{Z}_1,\ldots,\tilde{Z}_n\right) \neq \tilde{f}(X)\right) \doteq \exp\left[-nC(V)\right],$$

which, applied to (2.80), yields (2.81).

■

Remark: Observe that a direct application of [44, Theorem 2] to

$$\pi_\rho\left(W^n\right) = P\left(g_{\text{MAP}(W^n)}\left(Z_1,\ldots,Z_n\right) \neq X\right)$$

is not useful as it yields

$$\pi_\rho\left(W^n\right) \doteq \exp\left[-nC(W)\right]$$

where the Chernoff radius of $W : \mathcal{X} \to \mathcal{Z}$ is $C(W) = 0$ owing to the presence of identical rows when $k \leq r - 1$.

Lemma 2.10. *For V_o in (2.17) and V_1 in (2.36), we have*

$$C\left(V_1\right) = D(\text{Ber}(0.5)||\text{Ber}(\rho)) = -\log 2\sqrt{\rho(1-\rho)}, \quad 0 \leq \rho \leq 1 \tag{2.84}$$

and for $0.5 < \rho < 1$

$$C\left(V_o\right) = -\log 2\sqrt{\max\{\rho_c, \rho\}\left(1 - \max\{\rho_c, \rho\}\right)}, \quad k = 2 \tag{2.85}$$

$$C\left(V_o\right) > -\log 2\sqrt{\max\{\rho_c, \rho\}\left(1 - \max\{\rho_c, \rho\}\right)}, \quad k \geq 3. \tag{2.86}$$

Proof: First observe that for $0 < \rho < 1$,

$$\begin{aligned} C\left(V_1\right) &= \sup_{0<\lambda<1} \log \frac{1}{\rho^{\lambda}\left(1-\rho\right)^{1-\lambda} + \rho^{1-\lambda}\left(1-\rho\right)^{\lambda}} \\ &= \log \frac{1}{\inf\limits_{0<\lambda<1} \rho^{\lambda}\left(1-\rho\right)^{1-\lambda} + \rho^{1-\lambda}\left(1-\rho\right)^{\lambda}} \\ &= \log \frac{1}{2\sqrt{\rho(1-\rho)}} \\ &= D(\text{Ber}(0.5)||\text{Ber}(\rho)) \end{aligned} \tag{2.87}$$

where the infimum is attained as a minimum at $\lambda = 0.5$; and $C(V_1) = \infty$ for $\rho = 0$ and $\rho = 1$. The last equality above is by a simple calculation.

Turning to (2.85), for $k = 2$,

$$C\left(V_o\right) = \sup_{0<\lambda<1} \log \frac{1}{\left(\max\{\rho_c, \rho\}\right)^{\lambda} \left(1 - \max\{\rho_c, \rho\}\right)^{1-\lambda} + \left(\max\{\rho_c, \rho\}\right)^{1-\lambda} \left(1 - \max\{\rho_c, \rho\}\right)^{\lambda}}$$
$$= \log \frac{1}{2\sqrt{\max\{\rho_c, \rho\}\left(1 - \max\{\rho_c, \rho\}\right)}},$$

in the manner of (2.87).

To show (2.86), for $j \neq j'$ in $\mathcal{Z}$,

$$C\left(j, j'\right) = \sup_{0<\lambda<1} \log \frac{1}{\sum\limits_{i \in \mathcal{Z}} V_o(i|j)^{\lambda} V_o(i|j')^{1-\lambda}} = \sup_{0<\lambda<1} \left(1 - \lambda\right) D_{\lambda}(V_o(.|j)||V_o(.|j')) \tag{2.88}$$

where D_{λ} is the Rényi divergence of order λ [65]. For each $\lambda \in (0, 1)$, since D_{λ} satisfies the data processing theorem [29, Theorem 1], we get

$$D_{\lambda}(V_o(.|j)||V_o(.|j')) \geq D_{\lambda}\left(\text{Ber}\left(V_o(j'|j)\right)||\text{Ber}\left(V_o(j'|j')\right)\right)$$
$$= D_{\lambda}\left(\text{Ber}\left(\frac{P_X(x^*_{j'})}{\sum\limits_{l \neq j} P_X\left(x^*_l\right)}(1 - \max\{\rho_c, \rho\})\right)\Big|\Big|\text{Ber}(\max\{\rho_c, \rho\})\right). \tag{2.89}$$

Claim: For $k \geq 3$ and $0.5 < \rho < 1$, the right-side of (2.89) is strictly larger than

$$D_{\lambda}\left(\text{Ber}\left(1 - \max\{\rho_c, \rho\}\right)||\text{Ber}(\max\{\rho_c, \rho\})\right).$$

Then applying the claim to (2.88), for all $j \neq j'$ in $\mathcal{Z}$,

$$\begin{aligned} C(j,j') &> \sup_{0<\lambda<1} (1-\lambda) D_\lambda \left(\text{Ber}\left(1-\max\{\rho_c,\rho\}\right) || \text{Ber}(\max\{\rho_c,\rho\})\right) \\ &\geq 0.5 D_{0.5} \left(\text{Ber}\left(1-\max\{\rho_c,\rho\}\right) || \text{Ber}(\max\{\rho_c,\rho\})\right) \\ &= -\log 2\sqrt{\max\{\rho_c,\rho\}(1-\max\{\rho_c,\rho\})} \end{aligned}$$

which yields (2.86).

It remains to prove the claim. Note that for $k \geq 3$, $P_X(x^*_{j'}) \Big/ \sum_{l\neq j} P_X\left(x^*_l\right) < 1$ and so

$$\frac{P_X(x^*_{j'})}{\sum_{l\neq j} P_X\left(x^*_l\right)}(1-\max\{\rho_c,\rho\}) < 1-\max\{\rho_c,\rho\} < \max\{\rho_c,\rho\}$$

since $\max\{\rho_c,\rho\} > 0.5$. Then, it suffices to show that $D_\lambda(\text{Ber}(\alpha)||\text{Ber}(\beta))$ is (strictly) decreasing in α for $0 \leq \alpha < \beta$. We have

$$\frac{d}{d\alpha} D_\lambda(\text{Ber}(\alpha)||\text{Ber}(\beta)) = \frac{1}{\lambda-1} \frac{\lambda\alpha^{\lambda-1}\beta^{1-\lambda} - \lambda\left(1-\alpha\right)^{\lambda-1}\left(1-\beta\right)^{1-\lambda}}{\alpha^\lambda\beta^{1-\lambda} + \left(1-\alpha\right)^\lambda\left(1-\beta\right)^{1-\lambda}}. \tag{2.90}$$

Since $\lambda \in (0,1)$, the right-side of (2.90) is negative iff

$$\alpha^{\lambda-1}\beta^{1-\lambda} > \left(1-\alpha\right)^{\lambda-1}\left(1-\beta\right)^{1-\lambda}, \text{ i.e., } \left(\frac{1-\alpha}{\alpha}\right)^{1-\lambda} > \left(\frac{1-\beta}{\beta}\right)^{1-\lambda}$$

which holds since $\alpha < \beta$. ■

Finally, we show that the privacy of add-noise ρ-QRs $\{F_t(X)\}_{t=1}^\infty$ under (2.29) for every $n \geq 1$ with $V_t = V_o$, $t \geq 1$, is no better than with $V_t = V_1$ or V_2 accordingly as $0.5 < \rho \leq 1$ or

$0 \leq \rho \leq 0.5$; and, in fact, the former can be strictly smaller than the latter.

Proposition 2.11. *For all n suitably large (depending on case below):*

(i) $0 \leq \rho \leq 0.5$:

$$\pi_\rho\left(V_2^n\right) \geq \pi_\rho\left(V_o^n\right); \tag{2.91}$$

(ii) $0.5 < \rho < 1$:

$k = 2$ –

$$\pi_\rho\left(V_1^n\right) > \pi_\rho\left(V_o^n\right), \quad \rho < \rho_c \tag{2.92}$$

$$\pi_\rho\left(V_1^n\right) = \pi_\rho\left(V_o^n\right), \quad \rho \geq \rho_c; \tag{2.93}$$

$k \geq 3$ –

$$\pi_\rho\left(V_1^n\right) > \pi_\rho\left(V_o^n\right). \tag{2.94}$$

Proof:

(i) See Appendix A.4.

(ii) For $0 \leq \rho < 1$, we have by Lemma 2.9(ii),

$$\pi_\rho\left(V_o^n\right) - \left(1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)\right) \doteq \exp\left[-nC\left(V_o\right)\right], \tag{2.95}$$

and by Theorem 2.4 for $0.5 < \rho \leq 1$,

$$\pi_\rho\left(V_1^n\right) - \left(1 - \sum_{i \in \mathcal{Z}} P_X\left(x_i^*\right)\right)$$

$$
\begin{aligned}
&\geq \Lambda_n(\rho), \quad n \geq 1 \\
&\doteq \exp\left[-nD(\text{Ber}(0.5)||\text{Ber}(\rho))\right], \text{ by (2.38) and Lemma 2.6(i)} \\
&= \exp\left[-nC(V_1)\right], \text{ by (2.84).}
\end{aligned} \tag{2.96}
$$

For $k = 2$ and $0.5 < \rho < \rho_c$, by (2.84) and (2.85),

$$
C(V_1) = -\log 2\sqrt{\rho(1-\rho)} < -\log 2\sqrt{\rho_c(1-\rho_c)} = C(V_o)
$$

so that (2.92) holds by (2.95) and (2.96). For $k = 2$ and $\rho \geq \rho_c$, observe in (2.36) and (2.17) that $V_1 = V_o$ whereby (2.93) holds. For $k \geq 3$ and $0.5 < \rho < 1$, by (2.84) and (2.86),

$$
C\left(V_1\right) = -\log 2\sqrt{\rho(1-\rho)} \leq -\log 2\sqrt{\max\{\rho_c, \rho\}\left(1-\max\{\rho_c, \rho\}\right)} < C(V_o)
$$

and so (2.94) holds by (2.95) and (2.96).

■

2.8. Discussion and Open Problems

The choice of probability of error as a measure of recoverability as well as privacy is driven by considerations of tractability and obtaining exact answers. In particular, it enables us to identify optimal or asymptotically optimal ρ-QRs in our achievability proofs. However, observe that (2.1) or (2.2) is a pointwise (in $X = x,\ x \in \mathcal{X}$) measure of recoverability while (2.8) or (2.11) is an average (in $Z = i,\ i \in \mathcal{Z}$) measure of privacy. In symmetry with the pointwise measure of

recoverability, it would be preferable to consider a redolent measure of privacy in (2.8), (2.11) that is pointwise in $Z = i$, viz.

$$\pi(\rho) = \max_{\substack{W: W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \min_{i \in \mathcal{Z}} P(g_{MAP(W)}(Z) \neq X \mid Z = i), \quad 0 \leq \rho \leq 1. \tag{2.97}$$

What would be the characterization of $\pi(\rho)$ given by (2.97)?

As mentioned above, we have used the probability of error criterion to measure privacy. In a different formulation, privacy can be defined in terms of more discerning measures such as L_1- or L_2-distances between user data and the querier's estimate of it which penalizes deviation of the querier's estimate from its true value. Will the resulting insights be qualitatively different?

The choice of $W_o : \mathcal{X} \to \mathcal{Z}$ or $V_o : \mathcal{Z} \to \mathcal{Z}$ in (2.16), (2.17), depending on P_X through $P_X(x_i^*)$, $i \in \mathcal{Z}$, yields maximal privacy for a single ρ-QR for all $0 \leq \rho \leq 1$. However, for the case of multiple conditionally independent ρ-QRs, our achievability schemes in Section 2.4, that do not depend on P_X, perform variously according to the value of ρ. In particular, for $0.5 < \rho \leq 1$, conditionally i.i.d. add-noise ρ-QRs $\{F_t(X)\}_{t=1}^{\infty}$ with $V_1 : \mathcal{Z} \to \mathcal{Z}$ in (2.36) are asymptotically optimal with privacy $\pi_\rho(V_1^n)$ converging to the limit of the upper bounds for ρ-privacy $\pi_n(\rho)$, $n \geq 1$, in Theorem 2.3. However, when $0 \leq \rho \leq 0.5$, our add-noise ρ-QRs with $V_2 : \mathcal{Z} \to \mathcal{Z}$ in (2.40), (2.41) yield privacy $\pi_\rho(V_2^n)$ not depending on n, which, in general, does not meet the corresponding upper bound in (2.46). Thus, it remains open whether conditionally independent ρ-QRs $\{W_t\}_{t=1}^{\infty}$ that are P_X-dependent or are not necessarily of the add-noise variety, can outperform $\pi_\rho(V_1^n)$ or $\pi_\rho(V_2^n)$. Indeed, the goodness of our upper bound for $\pi_n(\rho)$ in (2.46), $0 \leq \rho \leq 0.5$ (that does not depend on n), is unresolved. These observations are analogous – in our setting – to the "composition" results for differential privacy (cf. e.g., [42]).

In Section 2.4, the objective of the querier is to compute $f(X)$, for a prespecified f, from multiple ρ-QRs provided by the user. In an alternative formulation where an "adversarial querier" elicits multiple ρ-QRs for various choices of functions in order to isolate the value of X and compromise data privacy.

2.8.1. Local Differential Privacy

We close with a suggested framework for examining the work in this chapter in the context of differential privacy that was described in Section 1.2 and is now restated. 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 data privacy. However, unlike in a differential privacy setting, our model lacks a notion of closeness between data vectors. Instead, we consider local differential privacy (ϵ-LDP) [24], [40], [76], [62], which is a more general and conservative measure of privacy compared with differential privacy (see [24]). Specifically, ϵ-LDP, $\epsilon > 0$, requires a QR $W : \mathcal{X} \to \mathcal{Z}$ to satisfy

$$\frac{W(j|x')}{W(j|x)} \leq e^{\epsilon}, \quad x, x' \in \mathcal{X}, \;\; j \in \mathcal{Z}. \tag{2.98}$$

The objective of the user is to select the randomization mechanism that enables function recoverability and maximizes data privacy while simultaneously being locally differentially private.

For each $j \in \mathcal{Z}$, ρ-recoverability in (2.2) and (2.98) with $x' \in f^{-1}(j)$ imply that

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

Furthermore, we must have

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

whence

$$\rho \leq \frac{1}{1 + (k-1)e^{-\epsilon}} < 1. \tag{2.99}$$

Thus, an ϵ-LDP QR $W : \mathcal{X} \to \mathcal{Z}$ will be a ρ-QR for ρ as in (2.99), implying that f cannot be ρ-recoverable for ρ violating (2.99).

For $\epsilon > 0$ and ρ satisfying (2.99), what is a characterization of ρ-privacy in (2.31) under the additional requirement that the ρ-QRs are locally differentially private? To this end, for establishing a converse bound, how would we incorporate the ϵ-LDP constraint (2.98) in the proof of Theorem 2.3? With regard to achievability, it is significant that the ϵ-LDP requirement (2.98) would preclude the ρ-QRs used in the proofs of Theorems 2.4 and 2.5 (with zeros in the associated stochastic matrices). For that reason, to begin with, we can compare the performance of well-established ϵ-LDP mechanisms RAPPOR [28] and Randomized Response [41] with the converse bound. However, in general, a closed-form expression for ρ-privacy under an ϵ-LDP constraint is not apparent. Therefore, as a first step, can a particularization to the special case of a binary-valued mapping $f : \mathcal{X} \to \{0, 1\}$ make the characterization of ρ-privacy tractable? These

problems are open.

Chapter 3: List Privacy Under Function Recoverability

3.1. Synopsis

We consider a user's data to be depicted by a finite-valued rv with known pmf and a querier who wishes to compute a given function of the data from a user-provided QR. The user fashions the QR so as to enable the querier to recover from it the function value with a prescribed probability $\rho,\ 0 \leq \rho \leq 1$, while maximizing list privacy of the data. List privacy is measured by the likelihood of the querier guessing a list of prescribed size, based on the QR, to which the data value belongs. We derive a general converse upper bound for maximum list privacy; and for the special case of a binary-valued function, the mentioned upper bound is shown to be tight through an achievability scheme, consisting of a suitable QR.

List ρ-privacy is described in Section 3.2 and the main results are given in Section 3.3. The concluding discussion Section 3.4 also contains relevant open problems. The results of this chapter were reported in [56], [60].

3.2. Preliminaries

Consider the model as in Chapter 2 and outlined in Section 2.2 before Definition 2.1. A QR $F(X)$ or $W : \mathcal{X} \to \mathcal{Z}$ that satisfies the ρ-recoverability condition described in Definition 2.1 is

termed a ρ-QR.

Definition 3.1. Let $\mathcal{L}_l$ be the set of all l-sized subsets of $\mathcal{X}$, $1 \leq l < r$. For a given l, $1 \leq l < r$, the (l-)*list privacy* of a ρ-QR $F(X)$ or W satisfying (2.1) or (2.2) is

$$\pi_{\rho}^{(l)}(F) = \pi_{\rho}^{(l)}(W) \triangleq \min_{g} \; P\left(X \notin g\left(F(X)\right)\right), \tag{3.1}$$

where the minimum is over all estimators $g : \mathcal{Z} \to \mathcal{L}_l$. The minimum in (3.1) is attained by a maximum a MAP estimator

$$g_{MAP(W)}^{(l)}(i) = \arg \max_{L \in \mathcal{L}_l} \; P\left(X \in L, Z = i\right) = \arg \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X\left(x\right) W\left(i|x\right), \quad i \in \mathcal{Z}. \tag{3.2}$$

Ties in (3.2) are broken arbitrarily. For $0 \leq \rho \leq 1$, the maximum list privacy that can be attained by a ρ-QR is termed *list ρ-privacy* and denoted by $\pi^{(l)}(\rho)$, i.e.,

$$\pi^{(l)}\left(\rho\right) \triangleq \max_{\substack{W : W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \pi_{\rho}^{(l)}\left(W\right).$$

In this chapter, too, we shall assume conservatively that the querier knows the pmf P_X and the ρ-QR F or W.

Remarks:

(i) Our work in Chapter 2 was concerned primarily with privacy for the data X. The associated concept of *ρ-privacy* $\pi(\rho)$ for X is a special case of list ρ-privacy $\pi^{(l)}(\rho)$ for list size $l = 1$. Clearly, list privacy is a more stringent notion than (data) privacy since $\pi^{(l)}(\rho) \leq \pi(\rho)$. Also, for $1 \leq l' < l < r$, $\pi^{(l)}(\rho) \leq \pi^{(l')}(\rho)$.

(ii) The list privacy framework addresses the drawback mentioned in Remark (iii) after Theorem 2.4 in Chapter 2 by choosing a suitable list size l.

Our objective is to characterize list ρ-privacy, and identify *explicitly* ρ-QRs that achieve them, $0 \leq \rho \leq 1$. This objective is met below in part for $\pi^{(l)}(\rho)$.

3.3. List ρ-Privacy

Our characterization of list ρ-privacy $\pi^{(l)}(\rho)$, $0 \leq \rho \leq 1$, is partial. We provide an upper bound for $\pi^{(l)}(\rho)$, and an achievability proof for the special case of a binary-valued mapping $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$. A general achievability proof is not yet in hand.

For any $A \subseteq \mathcal{X}$, we denote by $[A]_t$ the set of t largest P_X-probability elements in A, $0 \leq t \leq |A| \leq r$; in particular, $[A]_0 = \emptyset$ and $L_t^* \triangleq [\mathcal{X}]_t$ is the set of t largest P_X-probability elements in $\mathcal{X}$. Define

$$\Lambda_\rho \triangleq \arg \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[P_X(\Lambda) + \rho \sum_{i \in \mathcal{Z}} P_X \left(\left[f^{-1}(i) \setminus \Lambda \right]_{\min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\}} \right) \right], \quad 0 \leq \rho \leq 1. \quad (3.3)$$

Theorem 3.1. *(i) List ρ-privacy is bounded above according to*

$$\begin{aligned} \pi^{(l)}(\rho) &\leq \pi_u^{(l)}(\rho) \\ &= 1 - \left[P_X(\Lambda_\rho) + \rho \sum_{i \in \mathcal{Z}} P_X \left(\left[f^{-1}(i) \setminus \Lambda_\rho \right]_{\min\{l - |\Lambda_\rho|, |f^{-1}(i) \setminus \Lambda_\rho|\}} \right) \right], \quad 0 \leq \rho \leq 1. \quad (3.4) \end{aligned}$$

(ii) For $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$, it holds that

$$\pi^{(l)}(\rho) = \pi_u^{(l)}(\rho) = 1 - \left[P_X(\Lambda_\rho) + \rho \sum_{i \in \{0,1\}} P_X\left(\left[f^{-1}(i) \setminus \Lambda_\rho \right]_{l - |\Lambda_\rho|} \right) \right], \quad 0 \le \rho \le 1. \tag{3.5}$$

Remarks:

(i) The maximizing $\Lambda = \Lambda_\rho$ in (3.3) need not be unique.

(ii) In the right-side of (3.4), $\pi_u^{(l)}(\rho)$ is piecewise affine in $\rho \in [0, 1]$. See, for example, Fig. 3.1.

(iii) The form of $\pi_u^{(l)}(\rho)$ in (3.4), (3.3) affords the following interpretation for the querier's best list estimate. For $\rho \cong 0$, i.e., a "useless" ρ-QR $F(X) = Z$, the querier's best (MAP) estimate of a list is L_l^*. For $\rho = 1$, i.e., a full knowledge of $f(X)$, say $f(X) = i$ in $\mathcal{Z}$, the querier's best list estimate will contain $[f^{-1}(i)]_{\min\{l, |f^{-1}(i)|\}}$. For any intermediate value of ρ, the expression in (3.4) captures a tradeoff between these extremes.

(iv) For $l = 1$,

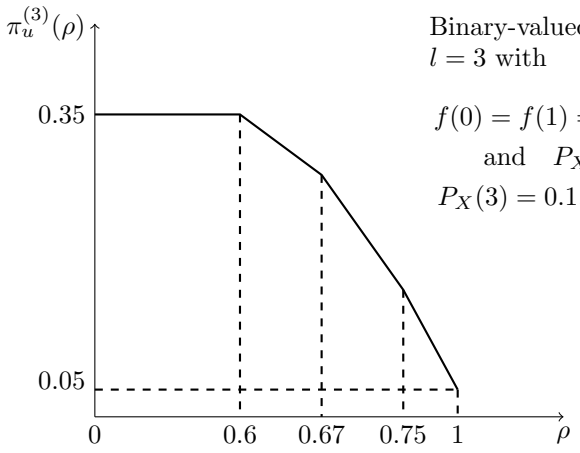
$$\pi_u^{(l)}(\rho) = 1 - \max\left\{ \max_{x \in \mathcal{X}} P_X(x), \rho \sum_{i \in \mathcal{Z}} \max_{x \in f^{-1}(i)} P_X(x) \right\}$$

which, by Theorem 2.2 equals ρ-privacy $\pi(\rho)$. Thus, Theorem 3.1 is tight for $l = 1$.

(v) The special case $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$ enables an achievability proof through a suitable choice of ρ-QR below.

The following technical lemma, whose proof is relegated to Appendix B, states properties of Λ_ρ and $\pi_u^{(l)}(\rho)$ in (3.3), (3.4) of pertinence to the achievability proof of Theorem 3.1(ii).

Lemma 3.2. (*Properties of Λ_ρ and $\pi_u^{(l)}(\rho)$ in* (3.3), (3.4), (3.5))



Binary-valued mapping $f : \{0, 1, \ldots, 6\} \to \{0, 1\}$ and $l = 3$ with

$$f(0) = f(1) = f(2) = 0, \quad f(3) = f(4) = f(5) = f(6) = 1$$
$$\text{and} \quad P_X(0) = 0.3,\ P_X(1) = 0.2,\ P_X(2) = 0.15,$$
$$P_X(3) = 0.1,\ P_X(4) = 0.1,\ P_X(5) = 0.1,\ P_X(6) = 0.05.$$

Figure 3.1: $\pi_u^{(3)}(\rho)$ vs. ρ

(i) $\Lambda_\rho = \bigcup_{i\in\mathcal{Z}} (\Lambda_\rho \cap f^{-1}(i)) = \bigcup_{i\in\mathcal{Z}} [f^{-1}(i)]_{|\Lambda_\rho \cap f^{-1}(i)|}$, *i.e.,* $\Lambda_\rho \cap f^{-1}(i)$ *consists of* $|\Lambda_\rho \cap f^{-1}(i)|$*-largest* P_X*-probability elements in* $f^{-1}(i),\ i \in \mathcal{Z}$.

(ii) For $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$, Λ_ρ *satisfies*

$$l - |\Lambda_\rho| \leq |f^{-1}(i) \setminus \Lambda_\rho|, \quad i \in \{0, 1\}. \tag{3.6}$$

(iii) $\pi_u^{(l)}(\rho)$ *in* (3.3), (3.4) *is piecewise affine, continuous and nonincreasing in* $\rho \in [0, 1]$, *with*

$$\pi_u^{(l)}(0) = 1 - P_X\left(L_l^*\right), \quad \pi_u^{(l)}(1) = 1 - \sum_{i\in\mathcal{Z}} P_X\left(\left[f^{-1}(i)\right]_{\min\{l,|f^{-1}(i)|\}}\right). \tag{3.7}$$

(iv) $|\Lambda_\rho|$ *is nonincreasing in* $\rho,\ 0 \leq \rho \leq 1$, *with* $|\Lambda_0| = l$ *and* $0 \leq |\Lambda_1| \leq \max\{0, l - \min_{i\in\mathcal{Z}} |f^{-1}(i)|\}$.

(v) $|\Lambda_\rho|$ *is piecewise constant in* $0 \leq \rho \leq 1$ *with* $|\Lambda_\rho| = l - j$ *for* $\rho \in [\rho_j, \rho_{j+1}]$, $0 \leq j \leq l$, *where* $\rho_0 = 0 < \rho_1 \leq \ldots \leq \rho_l \leq \rho_{l+1} = 1$; *and* ρ_j, $j = 1, \ldots, l$, *is the solution to*

$$\max_{\substack{\Lambda\subset\mathcal{X}:\\ |\Lambda|=l-j+1}} \left[P_X(\Lambda) + \rho \sum_{i\in\mathcal{Z}} P_X\left(\left[f^{-1}(i) \setminus \Lambda\right]_{\min\{j-1,|f^{-1}(i)\setminus\Lambda|\}}\right)\right]$$

$$= \max_{\substack{\Lambda' \subset \mathcal{X}: \\ |\Lambda'| = l-j}} \left[P_X(\Lambda') + \rho \sum_{i \in \mathcal{Z}} P_X \left(\left[f^{-1}(i) \setminus \Lambda' \right]_{\min\{j, |f^{-1}(i) \setminus \Lambda'|\}} \right) \right].$$

Proof of Theorem 3.1:

(i) For every ρ-QR $W : \mathcal{X} \to \mathcal{Z}$ in (2.2),

$$\begin{aligned}
1 - \pi_\rho^{(l)}(W) &= P\left(X \in g_{MAP(W)}^{(l)}(Z) \right) \\
&= \sum_{i \in \mathcal{Z}} P\left(X \in g_{MAP(W)}^{(l)}(Z), Z = i \right) \\
&= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} P\left(X \in L, Z = i \right) \\
&= \sum_{i \in \mathcal{Z}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W(i|x) \qquad (3.8) \\
&\geq \sum_{i \in \mathcal{Z}} \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \sum_{x \in \Lambda \cup \left[f^{-1}(i) \setminus \Lambda \right]_{\min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \\
&= \sum_{i \in \mathcal{Z}} \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[\sum_{x \in \Lambda} P_X(x) W(i|x) + \sum_{x \in [f^{-1}(i) \setminus \Lambda]_{\min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \right] \\
&\geq \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \sum_{i \in \mathcal{Z}} \left[\sum_{x \in \Lambda} P_X(x) W(i|x) + \sum_{x \in [f^{-1}(i) \setminus \Lambda]_{\min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\}}} P_X(x) W(i|x) \right] \\
&\geq \max_{\substack{\Lambda \subset \mathcal{X}: \\ 0 \leq |\Lambda| \leq l}} \left[P_X(\Lambda) + \rho \sum_{i \in \mathcal{Z}} P_X \left(\left[f^{-1}(i) \setminus \Lambda \right]_{\min\{l - |\Lambda|, |f^{-1}(i) \setminus \Lambda|\}} \right) \right] \qquad (3.9)
\end{aligned}$$

which yields (3.4).

(ii) For $f : \mathcal{X} \to \{0, 1\}$, we note by Lemma 3.2(ii) that $\pi_u^{(l)}(\rho)$ in (3.4) simplifies to $\pi_u^{(l)}(\rho)$ in (3.5).

We present a ρ-QR that achieves (3.4). By Lemma 3.2(iii), we know that $\pi_u^{(l)}(\rho)$ is piecewise affine, continuous and nonincreasing in $\rho \in [0, 1]$, with $\pi_u^{(l)}(0) = 1 - P_X\left(L_l^*\right)$. Let ρ_1 be such

that

$$\pi_u^{(l)}(\rho) = 1 - P_X\left(L_l^*\right), \quad 0 \le \rho \le \rho_1,$$

i.e., ρ_1 is the largest value for ρ for which $\pi_u^{(l)}(\rho) = 1 - P_X\left(L_l^*\right)$. Note that for $0 \le \rho \le \rho_1$, $\Lambda_\rho = L_l^*$. For the choice of ρ-QR $W_o : \mathcal{X} \to \{0,1\}$ given by

$$W_o(i|x) = \begin{cases} \max\{\rho, \rho_1\}, & i = f(x) \\ 1 - \max\{\rho, \rho_1\}, & i \neq f(x), \ \ x \in \mathcal{X}, \ \ i \in \{0,1\}, \end{cases} \tag{3.10}$$

we get

$$\begin{aligned} 1 - \pi_\rho^{(l)}\left(W_o\right) &= P\left(X \in g_{MAP(W_o)}^{(l)}(Z)\right) \\ &= \sum_{i \in \{0,1\}} \max_{L \in \mathcal{L}_l} \sum_{x \in L} P_X(x) W_o(i|x). \end{aligned} \tag{3.11}$$

With Λ_ρ as in (3.3), and noting by Lemma 3.2(ii) that $l - |\Lambda_\rho| \le |f^{-1}(i) \setminus \Lambda_\rho|, \ i \in \{0,1\}$, we claim that the maxima in (3.11) are attained by $L^i, \ i = 0, 1$, in $\mathcal{L}_l$ given by

$$L^i = \Lambda_\rho \cup \left[f^{-1}(i) \setminus \Lambda_\rho\right]_{l - |\Lambda_\rho|}, \ \ i = 0, 1. \tag{3.12}$$

For any $A \subseteq \mathcal{X}$, let $[A]^i$ denote the (not necessarily unique) ith-largest P_X-probability element in A, $i = 1, \ldots, |A|$. Let $|\Lambda_\rho \cap f^{-1}(i)| = a_i, \ i \in \{0,1\}$. Using Lemma 3.2(i) in (3.12), said claim means that

$$L^1 = \left[f^{-1}(1)\right]_{a_1 + l - |\Lambda_\rho|} \cup \left[f^{-1}(0)\right]_{a_0}$$

$$L^0 = \left[f^{-1}(1)\right]_{a_1} \cup \left[f^{-1}(0)\right]_{a_0+l-|\Lambda_\rho|} \tag{3.13}$$

attain the maxima in (3.11). We first consider the case $\rho > \rho_1$. With the choice of W_o in (3.10), for the maximum in (3.11) for $i = 1$ to be attained by L^1, it suffices if

$$\rho P_X\left([f^{-1}(1)]^{a_1+l-|\Lambda_\rho|}\right) \geq (1-\rho) P_X\left([f^{-1}(0)]^{a_0+1}\right) \tag{3.14}$$

and

$$(1-\rho) P_X\left([f^{-1}(0)]^{a_0}\right) \geq \rho P_X\left([f^{-1}(1)]^{a_1+l-|\Lambda_\rho|+1}\right). \tag{3.15}$$

If $a_0 = 0$ or $a_1 + l - |\Lambda_\rho| = |f^{-1}(1)|$, then it is enough to show (3.14), as (3.15) is vacuous. If $a_0 = |f^{-1}(0)|$ or $a_1 + l - |\Lambda_\rho| = 0$, then again it is adequate to show (3.15), as (3.14) is vacuous. Since Λ_ρ attains the maximum for the expression within $[\cdot]$ in (3.3),

$$\begin{aligned} &P_X(\Lambda_\rho) + \rho \sum_{i\in\{0,1\}} P_X\left(\left[f^{-1}(i) \setminus \Lambda_\rho\right]_{l-|\Lambda_\rho|}\right) \\ &\quad \geq P_X(\Lambda) + \rho \sum_{i\in\{0,1\}} P_X\left(\left[f^{-1}(i) \setminus \Lambda\right]_{\min\{l-|\Lambda|, |f^{-1}(i)\setminus\Lambda|\}}\right), \quad \Lambda \subset \mathcal{X},\ 0 \leq |\Lambda| \leq l. \end{aligned} \tag{3.16}$$

By choosing $\Lambda = \Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}$ in[1] (3.16), we get

$$\begin{aligned} &P_X\left(\Lambda_\rho\right) + \rho \sum_{i\in\{0,1\}} P_X\left(\left[f^{-1}(i) \setminus \Lambda_\rho\right]_{l-|\Lambda_\rho|}\right) \\ &\quad \geq P_X\left(\Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}\right) + \rho \sum_{i\in\{0,1\}} P_X\left(\left[f^{-1}(i) \setminus \left(\Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}\right)\right]_{l-|\Lambda_\rho|-1}\right), \end{aligned}$$

[1] We know that since $\rho > \rho_1$, $|\Lambda_\rho| \leq l-1$, and therefore, $\Lambda = \Lambda_\rho \cup [f^{-1}(0)]^{a_0+1}$ is a valid choice for Λ in (3.16). Also, by a straightforward calculation, $l - |\Lambda| \leq |f^{-1}(i) \setminus \Lambda|,\ i = 0, 1$.

which reduces to (3.14). Similarly, by choosing $\Lambda = \Lambda_\rho \setminus [f^{-1}(0)]^{a_0}$ in[2] (3.16), we get (3.15).

For establishing that the maximum in (3.11) for $i = 0$ is attained by L^0, similarly it is sufficient to show that

$$\rho P_X\left([f^{-1}(0)]^{a_0+l-|\Lambda_\rho|}\right) \geq (1-\rho) P_X\left([f^{-1}(1)]^{a_1+1}\right) \tag{3.17}$$

and

$$(1-\rho) P_X\left([f^{-1}(1)]^{a_1}\right) \geq \rho P_X\left([f^{-1}(0)]^{a_0+l-|\Lambda_\rho|+1}\right). \tag{3.18}$$

This is done by choosing $\Lambda = \Lambda_\rho \cup [f^{-1}(1)]^{a_1+1}$ and $\Lambda = \Lambda_\rho \setminus [f^{-1}(1)]^{a_1}$ which give (3.17) and (3.18), respectively, by similar calculations as for the case $i = 1$.

When $\rho \leq \rho_1$, it is readily seen in (3.13) that $L^1 = L^0 = [f^{-1}(1)]_{a_1} \cup [f^{-1}(0)]_{a_0} = L_l^*$, and attain the maxima in (3.11).

Finally, upon substituting (3.12) in (3.11), the resulting $\pi_\rho^{(l)}(W_o)$ equals the upper bound $\pi_u^{(l)}(\rho)$ in (3.5). This completes the proof of achievability. ■

Remark: Observe in the proof of Theorem 3.1(i) that in obtaining the bound (3.9), a list of size less than l will be chosen for the second summation in the right-side of (3.8) if Λ_ρ is such that, for some i in $\mathcal{Z}$, it holds that $l - |\Lambda_\rho| > |f^{-1}(i) \setminus \Lambda_\rho|$. This would suggest an apparent slackness in the upper bound on $\pi(\rho)$. We provide next an example to show that this is not necessarily the case. Consider the mapping $f : \{0, 1, \ldots, 4\} \to \{0, 1, 2\}$ with

$$f(0) = f(1) = 0, \quad f(2) = f(3) = 1 \quad \text{and} \quad f(4) = 2.$$

[2]As noted, we only need to show (3.15) if $a_0 > 0$ and $a_1 + l - |\Lambda_\rho| < |f^{-1}(1)|$. Then with $\Lambda = \Lambda_\rho \setminus [f^{-1}(0)]^{a_0}$, it can be verified easily that if $a_0 > 0$ and $a_1 + l - |\Lambda_\rho| < |f^{-1}(1)|$, then $l - |\Lambda| \leq |f^{-1}(i) \setminus \Lambda|$, $i = 0, 1$.

The list size $l = 2$, and P_X is the uniform pmf on $\mathcal{X}$. By a straightforward calculation, we obtain

$$\pi_u^{(l)}(\rho) = \begin{cases} 1-\rho, & \frac{1}{2} \leq \rho \leq 1 \\ \frac{4}{5} - \frac{3}{5}\rho, & \frac{1}{3} \leq \rho \leq \frac{1}{2} \\ \frac{3}{5}, & 0 \leq \rho \leq \frac{1}{3}. \end{cases}$$

Observe that for $1/2 \leq \rho \leq 1$, $\Lambda_\rho = \emptyset$, due to which $l - |\Lambda_\rho| = 2 > |f^{-1}(2) \setminus \Lambda_\rho| = 1$. But the ρ-QR $W : \{0, 1, \ldots, 4\} \to \{0, 1, 2\}$ given by

$$W(i|x) = \begin{cases} \rho, & i \in \{0,1,2\}, \quad x \in f^{-1}(i) \\ 1-\rho, & i = 0, \quad x \in \{2,3\} \\ 1-\rho, & i = 1, \quad x \in \{0,1\} \\ \frac{1-\rho}{2}, & i \in \{0,1\}, \ \ x = 4 \\ 0, & \text{otherwise}, \end{cases}$$

has list privacy $1 - \rho$ for $1/2 \leq \rho \leq 1$. Therefore, for $1/2 \leq \rho \leq 1$, $\pi_u^{(l)}(\rho)$ is optimal even though $l - |\Lambda_\rho| = 2 > |f^{-1}(2) \setminus \Lambda_\rho| = 1$.

3.4. Discussion and Open Problems

By Theorem 3.1, we have obtained an upper bound for list ρ-privacy that is tight for binary-valued functions. What is the exact characterization of list ρ-privacy for functions that are not binary-valued? With regard to the converse, from the derivation of $\pi_u^{(l)}(\rho)$, we get that the querier's best

list estimate, based on i in $\mathcal{Z}$, has the structure that it consists of elements from the highest P_X-probability elements in $\mathcal{X}$ and the highest P_X-probability elements in $f^{-1}(i)$. This natural form of the querier list estimate suggests the optimality of $\pi_u^{(l)}(\rho)$. In that case, what is the optimal ρ-QR, i.e., ρ-QR attaining a list privacy of $\pi_u^{(l)}(\rho)$, for functions that are not binary-valued? By Lemma 2.1, observe that W_o (3.10) is an add-noise ρ-QR. Can ρ-QRs, not necessarily of the add-noise type, be considered for achieving list ρ-privacy? These questions are open.

Chapter 4: Gaussian Data Privacy Under Linear Function Recoverability

4.1. Synopsis

A user's data is represented by a Gaussian rv and a querier seeks to compute a given linear function of the data from a QR provided by the user. The QR is a suitably randomized version of the data that the user constructs so as to enable the querier to recover the function value with a prescribed accuracy, parameterized by $\rho \geq 0$. Under this recoverability requirement, the user wishes to maximize privacy of the data from the querier. Both recoverability and privacy are measured by ℓ_2-distance criteria.

Our model for ρ-recoverable linear function computation with associated privacy is described in Section 4.2 and the derivation of ρ-privacy is given in Section 4.3. A closing discussion along with relevant open problems are contained in Section 4.4. The results of this chapter were reported in [52], [53].

4.2. Preliminaries

Let a user's data be represented by a $\mathbb{R}^n$-valued redundant Gaussian rv $X \sim \mathcal{N}(\mathbf{0}, I_n)$ with covariance matrix $I_n,\ n \geq 1$, the identity matrix of size n. A querier wishes to compute a given linear function of the user data AX, where $A \in \mathbb{R}^{m \times n}$ and has rank $1 \leq r \leq \min\{m, n\}$. The

querier obtains from the user a QR Z that is a $\mathbb{R}^m$-valued rv generated by a conditional probability distribution $P_{Z|X}$. The QR Z must satisfy the following recoverability condition.

Definition 4.1. Given $\rho \geq 0$, a QR Z is *ρ-recoverable* if

$$\mathbb{E}\left[\|AX - Z\|^2\right] \leq \rho, \tag{4.1}$$

where the expectation is with respect to the distribution of (X, Z). Such a ρ-recoverable Z will be termed ρ-QR. We note that the distribution of Z will depend, in general, on ρ.

Remark: Note that unlike in Chapters 2 and 3, recoverability decreases with increasing $\rho \geq 0$.

Definition 4.2. Given $\rho \geq 0$, the *privacy* of a ρ-QR Z satisfying (4.1) is

$$\pi_\rho(Z) \triangleq \inf_g \mathbb{E}\left[\|X - g(Z)\|^2\right] = \text{mmse}(X|Z) \tag{4.2}$$

where the infimum is taken over all (Borel) measurable estimators $g : \mathbb{R}^m \to \mathbb{R}^n$ of X on the basis of Z. Clearly, the infimum in (4.2) is attained by an MMSE estimator so that $\pi_\rho(Z)$ is $\text{mmse}(X|Z)$, where $\text{mmse}(X|Z)$ denotes the MMSE in estimating X on the basis of Z.

Definition 4.3. Given $\rho \geq 0$, the maximum privacy that can be attained by a ρ-QR Z is termed *ρ-privacy* and denoted by $\pi(\rho)$, i.e.,

$$\pi(\rho) \triangleq \sup_{P_{Z|X}:\mathbb{E}\left[\|AX-Z\|^2\right]\leq\rho} \pi_\rho(Z). \tag{4.3}$$

Our objective is to characterize ρ-privacy $\pi(\rho),\ \rho \geq 0$, and identify a ρ-QR that achieves

it, and is addressed next.

4.3. Gaussian Data ρ-Privacy

Theorem 4.1 below provides an exact characterization of ρ-privacy in (4.3). This is done by obtaining first an upper bound (converse) for $\pi(\rho),\ \rho \geq 0$, and then identifying a ρ-QR whose privacy meets the bound (achievability).

Throughout the rest of the chapter, we consider a particular singular value decomposition of[1]

$$A = USV^T, \tag{4.4}$$

where U and V are, respectively, $m \times m$- and $n \times n$-orthonormal matrices. In[2] (4.4), the $m \times n$ matrix S containing the singular values of A and represented by

$$S_{ij} = \begin{cases} s_k, & i = j = k,\ \ k = 1, \ldots, r \\ 0, & \text{otherwise,} \qquad\qquad i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}, \end{cases} \tag{4.5}$$

is such that

$$0 < s_1 \leq \cdots \leq s_r, \tag{4.6}$$

where $s_1, \ldots, s_r$ are the nonzero singular values of A. Let $\tilde{S}$ be the $r \times n$-matrix consisting of the first r rows of S; the remaining $m - r$ rows of S are all-zero rows.

Recalling that U and V are orthonormal matrices and using (4.4), (4.5), standard calculations,

[1] Some notation relevant for the rest of the chapter: For a matrix B, we denote its transpose and trace by B^T and tr(B), respectively. For a rv Y, var(Y) will denote the trace of the covariance matrix of Y.

[2] The columns of U and columns of V are the left-singular vectors and right-singular vectors of A, respectively.

repeated in Appendix C.1 for the sake of completeness, show that $\text{var}(AX) = \text{tr}\left(AA^T\right) = \sum_{i=1}^{r} s_i^2$ and

$$\text{mmse}\,(X|AX) = n - r. \tag{4.7}$$

Theorem 4.1. *ρ-privacy equals*

$$\pi(\rho) = n - r + \min\left\{\frac{\rho}{s_1^2}, 1 + \frac{\rho - s_1^2}{s_2^2}, \ldots, r - 1 + \frac{\rho - \sum_{i=1}^{r-1} s_i^2}{s_r^2}, r\right\}, \qquad \rho \geq 0. \tag{4.8}$$

Remarks:

(i) By Theorem 4.1 and (4.6),

$$\pi(\rho) = \begin{cases} n - r + \frac{\rho}{s_1^2}, & 0 \leq \rho \leq s_1^2 \\ n - r + 1 + \frac{\rho - s_1^2}{s_2^2}, & s_1^2 \leq \rho \leq s_1^2 + s_2^2 \\ \vdots & \vdots \\ n - r + r - 1 + \frac{\rho - \sum_{i=1}^{r-1} s_i^2}{s_r^2}, & \sum_{i=1}^{r-1} s_i^2 \leq \rho \leq \sum_{i=1}^{r} s_i^2 \\ n, & \rho \geq \sum_{i=1}^{r} s_i^2, \end{cases} \tag{4.9}$$

is piecewise affine in ρ. For example, a plot of $\pi(\rho)$ vs. ρ is given in Fig. 4.1 for $n = 5$, $m = r = 3,\ s_1 = 2,\ s_2 = 3$ and $s_3 = 4$.

(ii) In particular, for $\rho = 0$, $\pi(\rho) = n - r$ which, from (4.7), is the error of an MMSE estimator of X on the basis of AX. For $\rho \geq \sum_{i=1}^{r} s_i^2 = \text{tr}\left(AA^T\right) = \text{var}(AX)$, $\pi(\rho) = n = \text{var}(X)$ is the error of a MMSE estimator of X without any observation.

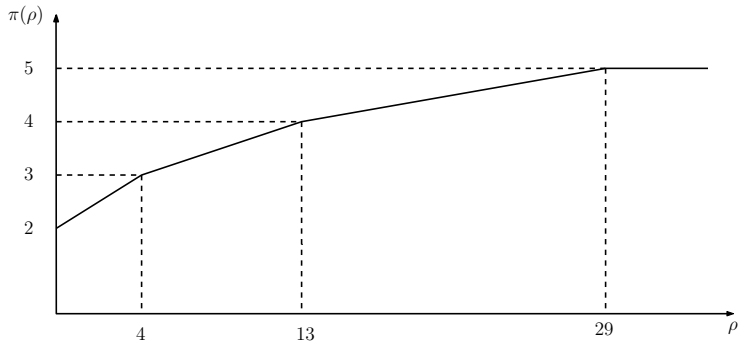


Figure 4.1: $\pi(\rho)$ vs. ρ.

(iii) ρ-privacy $\pi(\rho)$, $\rho \geq 0$, is a nonincreasing function of each individual singular value when the remaining $r-1$ singular values are fixed.

The following Lemmas 4.2 and 4.3 are pertinent to the proof of Theorem 4.1. Their proofs are relegated to Appendix C.2.

Lemma 4.2. *For* $\rho \geq 0$,

$$\sup_{P_{Z|X}:\mathbb{E}\left[\|AX-Z\|^2\right]\leq\rho} \inf_g \mathbb{E}\left[\|X-g(Z)\|^2\right] = \sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\leq\rho} \inf_g \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right] \quad (4.10)$$

where the $\mathbb{R}^m$*-valued rv* $\bar{Z}$ *represents a generic stand-in for a* ρ*-QR under recoverability of* SV^TX.

Remark: Since V is orthonormal and $X \sim \mathcal{N}(\mathbf{0}, I_n)$, $\bar{X} = V^TX$ has the same distribution as X. Hence, the right-side of (4.10) can be interpreted as ρ-privacy under recoverability of $S\bar{X}$, $\bar{X} \sim \mathcal{N}(\mathbf{0}, I_n)$. For reasons of ease of notation, we do not use this observation for the proof of Theorem 4.1.

The significance of Lemma 4.2 is that ρ-privacy under recoverability of AX from Z is equivalent to ρ-privacy under recoverability of SV^TX from $\bar{Z}$. Recalling that $\tilde{S}$ is the $r \times n$-

matrix consisting of the r nonzero rows of S, the covariance matrix of the $\mathbb{R}^r$-valued rv $\tilde{S}V^TX$ is a diagonal matrix $\tilde{S}\tilde{S}^T$, an observation that facilitates establishing the converse for the proof of Theorem 4.1.

The following notation is relevant for the rest of the chapter. For given $\mathbb{R}^m$-valued rvs Φ and ϕ, let the components of $\Phi - \phi$ be denoted by $[(\Phi-\phi)_1, \ldots, (\Phi-\phi)_m]^T$.

Lemma 4.3. *For $\rho \geq 0$,*

$$\sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\leq\rho} \inf_g \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right] = \sup_{\substack{P_{\tilde{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^TX-\tilde{Z}\right\|^2\right]\leq\rho \\ \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right]\leq s_i^2, \\ i=1,\ldots,r}} \inf_g \mathbb{E}\left[\left\|X-g(\tilde{Z})\right\|^2\right]. \tag{4.11}$$

By Lemma 4.3, we can restrict the class of ρ-QRs $\bar{Z}$ for recovering SV^TX in Lemma 4.2 to those specified $\tilde{Z}$ for the recoverability of $\tilde{S}V^TX$, as detailed under the supremum in the right-side of (4.11) without any loss in ρ-privacy.

Proof of Theorem 4.1: Using Lemmas 4.2 and 4.3, we get in (4.3) that

$$\begin{aligned}
\pi(\rho) &= \sup_{P_{Z|X}:\mathbb{E}\left[\|AX-Z\|^2\right]\leq\rho} \inf_g \mathbb{E}\left[\|X-g(Z)\|^2\right] \\
&= \sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\leq\rho} \inf_g \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right] \\
&= \sup_{\substack{P_{\tilde{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^TX-\tilde{Z}\right\|^2\right]\leq\rho \\ \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right]\leq s_i^2, \\ i=1,\ldots,r}} \inf_g \mathbb{E}\left[\left\|X-g(\tilde{Z})\right\|^2\right].
\end{aligned} \tag{4.12}$$

We establish (4.8), with (4.12) serving as the springboard. First, we prove a converse proof showing that $\pi(\rho)$ cannot exceed the right-side of (4.12). Then an achievability proof shows the

reverse inequality by identifying an explicit ρ-QR that attains the right-side of (4.12) as ρ-privacy.

Starting with the converse, we have that for every $\mathbb{R}^r$-valued rv $\tilde{Z}$, generated according to a $P_{\tilde{Z}|X}$ satisfying the constraints in the right-side of (4.12),

$$\mathbb{E}\left[\left\|\tilde{S}V^TX-\tilde{Z}\right\|^2\right]\le\rho,\qquad \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right]\le s_i^2,\quad i=1,\dots,r, \tag{4.13}$$

so that

$$\begin{aligned}
&\inf_g\ \mathbb{E}\left[\left\|X-g(\tilde{Z})\right\|^2\right]\\
&\le\mathbb{E}\left[\left\|X-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{Z}\right\|^2\right] &(4.14)\\
&=\mathbb{E}\left[\left\|X-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^TX+V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^TX-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{Z}\right\|^2\right]\\
&=\mathbb{E}\left[\left\|X-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^TX\right\|^2\right]\\
&+\mathbb{E}\left[\left\|V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^TX-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{Z}\right\|^2\right]\\
&+2\mathbb{E}\left[X^T\left(I_n-V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^T\right)^TV\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\left(\tilde{S}V^TX-\tilde{Z}\right)\right]\\
&=\text{mmse}\left(X|\tilde{S}V^TX\right)+\mathbb{E}\left[\left\|V\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\left(\tilde{S}V^TX-\tilde{Z}\right)\right\|^2\right] &(4.15)\\
&+2\mathbb{E}\left[X^T\left(\tilde{S}V^T-\tilde{S}V^TV\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\tilde{S}V^T\right)^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\left(\tilde{S}V^TX-\tilde{Z}\right)\right]\\
&=\text{mmse}(X|U^TAX)+\mathbb{E}\left[\left\|\tilde{S}^T\left(\tilde{S}\tilde{S}^T\right)^{-1}\left(\tilde{S}V^TX-\tilde{Z}\right)\right\|^2\right] &(4.16)\\
&=\text{mmse}(X|AX)+\sum_{i=1}^r\frac{1}{s_i^2}\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right] &(4.17)\\
&=n-r+\sum_{i=1}^r\frac{1}{s_i^2}\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right], &(4.18)
\end{aligned}$$

where: (4.14) uses the MMSE estimator of X on the basis of $\tilde{S}V^TX$, leading to the first term in (4.15); the first term in (4.16) is obtained since $\tilde{S}$ is the matrix consisting of the nonzero rows of S and (4.4); the second terms in (4.16) and (4.17), and the first term in (4.18), are obtained by the orthonormality of V, (4.5) and (4.7), respectively. Considering the second term in the right-side of (4.18), for $t = 0, 1, \ldots, r$,

$$
\begin{aligned}
&\sum_{i=1}^{r} \frac{1}{s_i^2} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] \\
&= \sum_{i=1}^{t} \frac{1}{s_i^2} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] + \sum_{i=t+1}^{r} \frac{1}{s_i^2} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] \qquad (4.19) \\
&\leq \sum_{i=1}^{t} \frac{1}{s_i^2} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] + \frac{1}{s_{t+1}^2} \sum_{i=t+1}^{r} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right], \quad \text{using (4.6)} \\
&= \sum_{i=1}^{t} \left(\frac{1}{s_i^2} - \frac{1}{s_{t+1}^2}\right) \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] + \frac{1}{s_{t+1}^2} \sum_{i=1}^{r} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] \\
&\leq \sum_{i=1}^{t} \left(\frac{1}{s_i^2} - \frac{1}{s_{t+1}^2}\right) s_i^2 + \frac{\rho}{s_{t+1}^2}, \qquad \text{using (4.13)} \\
&= t + \frac{\rho - \sum_{i=1}^{t} s_i^2}{s_{t+1}^2}, \qquad (4.20)
\end{aligned}
$$

from[3] which we get

$$
\sum_{i=1}^{r} \frac{1}{s_i^2} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - \tilde{Z}\right)_i\right|^2\right] \leq \min\left\{\frac{\rho}{s_1^2}, 1 + \frac{\rho - s_1^2}{s_2^2}, \ldots, r - 1 + \frac{\rho - \sum_{i=1}^{r-1} s_i^2}{s_r^2}, r\right\}. \qquad (4.21)
$$

[3] In the right-side of (4.19), the first and second terms are vacuous for $t = 0$ and $t = r$, respectively. In the right-side of (4.20), the second term and the summation in the second term are vacuous for $t = r$ and $t = 0$, respectively.

Using (4.21) in (4.18), the right-side of (4.12), and therefore $\pi(\rho)$, is bounded above as

$$\pi(\rho) \leq n - r + \min\left\{\frac{\rho}{s_1^2}, 1 + \frac{\rho - s_1^2}{s_2^2}, \ldots, r - 1 + \frac{\rho - \sum_{i=1}^{r-1} s_i^2}{s_r^2}, r\right\}. \tag{4.22}$$

Next, we demonstrate achievability of the privacy in the right-side of (4.12) by describing explicitly a ρ-QR for the purpose. This ρ-QR represents an extension of the scheme in [75, Theorem 13] in the separate context of maximizing (i.e., under worst-case noise) the MMSE of estimating a one-dimensional Gaussian rv on the basis of a one-dimensional noisy version of it under a constraint on the expected ℓ_2-distance between the input and the noisy output. The scheme in [75, Theorem 13] has the structure of attenuation of the input followed by additive independent Gaussian noise which will be the case for our achievability scheme, too, and is therefore an extension. To this end, by Lemmas 4.2, 4.3, it suffices to show a ρ-QR $\tilde{Z} = \tilde{Z}_o$ for the recoverability of $\tilde{S}V^T X$ and satisfies the constraints in (4.13). Our ρ-QR is the $\mathbb{R}^r$-valued rv given by

$$\tilde{Z}_o = D_a \tilde{S} V^T X + D_{no} N \tag{4.23}$$

where

$$\begin{aligned} D_a &= \text{diag}\left(1 - \frac{\rho_1}{s_1^2}, \ldots, 1 - \frac{\rho_r}{s_r^2}\right), \\ D_{no} &= \text{diag}\left(\sqrt{\rho_1 - \frac{\rho_1^2}{s_1^2}}, \ldots, \sqrt{\rho_r - \frac{\rho_r^2}{s_r^2}}\right) \end{aligned} \tag{4.24}$$

where $\text{diag}(d_1, \ldots, d_r)$ denotes a diagonal matrix with (diagonal) elements $(d_1, \ldots, d_r)$, and $N \sim \mathcal{N}(\mathbf{0}, I_r)$ is a $\mathbb{R}^r$-valued zero-mean Gaussian rv independent of X. Thus, $\tilde{Z}_o$ entails

attenuating $\tilde{S}V^T X$ by D_a and contaminating it with an additive independent Gaussian noise $D_{no}N$. The values of $\rho_1, \ldots, \rho_r$ in (4.24) are chosen for various ranges of values of ρ as follows.

- $0 \le \rho \le s_1^2: \quad \rho_1 = \rho,\ \rho_2 = \cdots = \rho_r = 0;$
- $s_1^2 \le \rho \le s_1^2 + s_2^2: \quad \rho_1 = s_1^2,\ \rho_2 = \rho - s_1^2,\ \rho_3 = \cdots = \rho_r = 0;$
- $s_1^2 + s_2^2 \le \rho \le s_1^2 + s_2^2 + s_3^2: \quad \rho_1 = s_1^2,\ \rho_2 = s_2^2,\ \rho_3 = \rho - s_1^2 - s_2^2,\ \rho_4 = \cdots = \rho_r = 0;$

$\vdots$

- $\sum_{i=1}^{r-1} s_i^2 \le \rho \le \sum_{i=1}^{r} s_i^2: \quad \rho_1 = s_1^2, \ldots, \rho_{r-1} = s_{r-1}^2,\ \rho_r = \rho - \sum_{i=1}^{r-1} s_i^2;$
- $\rho \ge \sum_{i=1}^{r} s_i^2: \quad \rho_1 = s_1^2, \ldots, \rho_r = s_r^2.$

(4.25)

We show in Appendix C.3 that $\tilde{Z}_o$ as in (4.23), (4.24), (4.25) satisfies the constraints in (4.13) (with $\tilde{Z} = \tilde{Z}_o$). Observing that X and $\tilde{Z}_o$ are jointly Gaussian, we have that the right-side of (4.12) is bounded below by

$$
\begin{aligned}
&\inf_g \mathbb{E}\left[\left\|X - g(\tilde{Z}_o)\right\|^2\right] \\
&= \text{mmse}\left(X|\tilde{Z}_o\right) \\
&= \mathbb{E}\left[\left\|X - \mathbb{E}\left[X\tilde{Z}_o^T\right]\left(\mathbb{E}\left[\tilde{Z}_o\tilde{Z}_o^T\right]\right)^{-1}\tilde{Z}_o\right\|^2\right] && (4.26) \\
&= \mathbb{E}\left[\left(X - \mathbb{E}\left[X\tilde{Z}_o^T\right]\left(\mathbb{E}\left[\tilde{Z}_o\tilde{Z}_o^T\right]\right)^{-1}\tilde{Z}_o\right)^T X\right] && (4.27) \\
&= \text{tr}\left(\mathbb{E}\left[XX^T\right]\right) - \text{tr}\left(\mathbb{E}\left[X\tilde{Z}_o^T\right]\left(\mathbb{E}\left[\tilde{Z}_o\tilde{Z}_o^T\right]\right)^{-1}\mathbb{E}\left[\tilde{Z}_o X^T\right]\right)
\end{aligned}
$$

$$= \text{tr}\,(I_n) - \text{tr}\left(I_n V \tilde{S}^T D_a^T \left(D_a \tilde{S} V^T I_n V \tilde{S}^T D_a^T + D_{no} I_r D_{no}^T \right)^{-1} D_a \tilde{S} V^T I_n \right)$$

$$= n - \text{tr}\left(\tilde{S}^T D_a^T \left(D_a \tilde{S} \tilde{S}^T D_a^T + D_{no} D_{no}^T \right)^{-1} D_a \tilde{S} \right), \quad \text{since } V \text{ is orthonormal} \tag{4.28}$$

$$= n - r + \sum_{i=1}^{r} \frac{\rho_i}{s_i^2}, \tag{4.29}$$

where the second term in the right-side of (4.28) is calculated using

$$D_a \tilde{S} \tilde{S}^T D_a^T = \text{diag}\left(s_1^2 + \frac{\rho_1^2}{s_1^2} - 2\rho_1, \ldots, s_r^2 + \frac{\rho_r^2}{s_r^2} - 2\rho_r \right),$$
$$D_{no} D_{no}^T = \text{diag}\left(\rho_1 - \frac{\rho_1^2}{s_1^2}, \ldots, \rho_r - \frac{\rho_r^2}{s_r^2} \right),$$

and for $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, m\}$,

$$\left(D_a \tilde{S} \right)_{ij} = \begin{cases} s_k - \frac{\rho_k}{s_k}, & i = j = k,\ k = 1, \ldots, r \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\tilde{S}^T D_a^T \left(D_a \tilde{S} \tilde{S}^T D_a^T + D_{no} D_{no}^T \right)^{-1} D_a \tilde{S} = \text{diag}\left(1 - \frac{\rho_1}{s_1^2}, \ldots, 1 - \frac{\rho_r}{s_r^2} \right).$$

By recalling the equivalence of the right-sides of (4.8) and (4.9) and substituting (4.25) in (4.29), we get that the right-side of (4.12), and therefore $\pi(\rho)$, is bounded below as

$$\pi(\rho) \geq n - r + \min \left\{ \frac{\rho}{s_1^2}, 1 + \frac{\rho - s_1^2}{s_2^2}, \ldots, r - 1 + \frac{\rho - \sum_{i=1}^{r-1} s_i^2}{s_r^2}, r \right\}. \tag{4.30}$$

The theorem follows from (4.22) and (4.30). ■

Remark: Recalling (4.4), let $\tilde{U}$ be the $m \times r$-matrix containing the first r columns of U. The achievability scheme $\tilde{Z}_o = D_a \tilde{S} V^T X + D_{no} N$ (4.23) is for maximizing privacy under recoverability of $\tilde{S} V^T X$. The corresponding achievability scheme or ρ-QR for the recoverability of AX, denoted by Z_o, is $Z_o = \tilde{U} D_a \tilde{U}^T AX + \tilde{U} D_{no} N$ which can be shown readily from the proof of Lemma 4.2, and also has the same features of attenuation and independent additive Gaussian noise.

We conclude this section by extending ρ-privacy to the case when the querier wishes to compute an affine function $AX + b$ of the Gaussian user data $X \sim \mathcal{N}(\mathbf{0}, I_n)$, $n \geq 1$, for a given A as in Section 4.2, and $b \in \mathbb{R}^m$. In Definition 4.3, (4.3) becomes

$$\begin{aligned} \pi(\rho) &= \sup_{P_{Z|X}: \mathbb{E}\left[\|AX+b-Z\|^2\right] \leq \rho} \inf_g \mathbb{E}\left[\|X - g(Z)\|^2\right] \\ &= \sup_{P_{Z|X}: \mathbb{E}\left[\|AX-(Z-b)\|^2\right] \leq \rho} \inf_g \mathbb{E}\left[\|X - g(Z-b)\|^2\right] \\ &= \sup_{P_{\hat{Z}|X}: \mathbb{E}\left[\left\|AX-\hat{Z}\right\|^2\right] \leq \rho} \inf_g \mathbb{E}\left[\left\|X - g\left(\hat{Z}\right)\right\|^2\right] \end{aligned} \tag{4.31}$$

from which we conclude that $\pi(\rho)$ as in (4.31) is equal to the right-side of (4.8). Observe that $\pi(\rho)$ does not depend on b, as is to be expected.

4.4. Discussion and Open Problems

We give a heuristic explanation of the form of $\pi(\rho)$ in (4.8). By Lemma 4.2, note that the recoverability of AX is equivalent to the recoverability of $SV^T X$, and therefore $\tilde{S} V^T X$, which consists of r components. We recall that $\tilde{S}$ is the matrix composed of the r nonzero rows of S, due to which AX consists effectively of r components corresponding to the r singular values of

A. At $\rho = 0$, the querier is provided the exact value of AX. From (4.23), (4.24), (4.25), observe that as ρ increases to s_1^2, the component of AX corresponding to the smallest singular value of A is concealed from the querier. As ρ increases further, more components of AX are hidden from the querier, with each subsequent component corresponding to a larger singular value of A. This explains the piecewise affine form of $\pi(\rho),\ \rho \geq 0$, in (4.8). Therefore, for lower values of ρ, i.e., in the high recoverability regime, only those components that correspond to smaller singular values of A, can be concealed from the querier.

This work is an initial foray into tackling the larger objective of characterizing data privacy under function recoverability, where the data is of the analog type. Therefore, several open questions remain some of which are stated next.

For reasons of mathematical tractability, we have assumed that the covariance matrix of the Gaussian user data X is I_n. The problem of computing ρ-privacy for an arbitrary (positive-definite) covariance is open. We conjecture that the form of $\pi(\rho)$ (piecewise affine in ρ) and the structure of the achievability scheme (attenuation and independent additive Gaussian noise) in Theorem 4.1, will hold.

A natural extension of this work involves the querier obtaining from the user multiple QRs each satisfying the ρ-recoverabilty condition, analogous to the model in Chapter 2.4. Specifically, given user data $X \sim \mathcal{N}(\mathbf{0}, I_n)$, a querier receives multiple ρ-QRs $Z_1, \ldots, Z_t,\ t \geq 1$, each satisfying (4.1) and generated by conditional distributions $P_{Z_1|X}, \ldots, P_{Z_t|X}$. The ρ-QRs are taken to be conditionally mutually independent, conditioned on X, but not necessarily identically

distributed. Correspondingly, for each $\rho \geq 0$ and $t \geq 1$, the ρ-privacy $\pi_t(\rho)$ is defined as

$$\pi_t(\rho) = \sup_{\substack{P_{Z_1|X},\ldots,P_{Z_t|X}: \\ \mathbb{E}\left[\|AX-Z_i\|^2\right] \leq \rho,\ i=1,\ldots,t}} \inf_{g_t} \mathbb{E}\left[\|X - g_t\left(Z_1,\ldots,Z_t\right)\|^2\right]$$

where the infimum is taken over all estimators $g_t : \mathbb{R}^{m\times t} \to \mathbb{R}^n$ of X on the basis of $Z_1,\ldots,Z_t$. The task is to characterize $\pi_t(\rho)$ and obtain the rate of decay of $\pi_t(\rho)$ with t. A candidate for the for ρ-QRs is (4.23) with mutually independent Gaussian noise rvs added to them. Will this be optimal in attaining $\pi_t(\rho)$?

Another broader extension of this work entails recoverability and privacy being measured by ℓ_p-distance and ℓ_q-distance criteria, $p, q \geq 1$, respectively. We seek a characterization of $\pi_{p,q}(\rho)$ given by

$$\pi_{p,q}(\rho) = \sup_{P_{Z|X}:\mathbb{E}[\|AX-Z\|^p] \leq \rho} \inf_{g} \mathbb{E}\left[\|X - g(Z)\|^q\right].$$

Does the structure of the solution in Theorem 4.1 change?

Finally, it is also of interest to examine ρ-privacy under recoverability of an arbitrary but given measurable function $f : \mathbb{R}^n \to \mathbb{R}^m,\ m \geq 1$, not limited to being linear. This problem, of a more demanding nature owing to the (possible) nonlinearity of the mapping f, requires a new approach.

Chapter 5: Distribution Privacy Under Function Recoverability

5.1. Synopsis

We consider a user's data to be represented by i.i.d. finite-valued rvs generated according to a 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 probability $\rho,\ 0 \leq \rho \leq 1$, while maximizing distribution privacy of the data pmf as determined by the divergence between the data pmf and the querier's best estimate of it based on the query responses. We first provide a basic lower bound for distribution privacy that does not depend on the number of query responses and represents worst-case privacy. Then, converse upper and achievability lower bounds for distribution privacy, dependent on the number of query responses, are derived through specific user and querier strategies.

A suggestive interpretation of distribution ρ-privacy entails Nature generating its secrets according to a maximizing (data) pmf as above, say $P_X = P_X^*$, that is hardest for a mortal querier to fathom under the function recoverability requirement above. A mortal user who wishes a high degree of distribution privacy, but is constrained unlike Nature, can emulate it upon choosing a feasible P_X that is proximate to P_X^*.

Our model for distribution ρ-privacy is described in Section 5.2. The worst-case distribution ρ-privacy, demonstrated by an achievability proof, is given in Section 5.3. Section 5.4 defines specialized user and querier strategies, and states the converse and achievability theorems which are proved in Section 5.5. Distribution ρ-privacy for the special case of a binary-valued mapping is characterized in Section 5.6. A closing discussion is provided in the concluding Section 5.7, and mentions unanswered questions. The results of this chapter were reported in [57], [58], [59].

5.2. Preliminaries

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 $f^{-1}(z) \triangleq \{x \in \mathcal{X} : f(x) = z\}$, $z \in \mathcal{Z}$. 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 QRs $Z_1, \ldots, Z_n$, that are $\mathcal{Z}$-valued rvs provided by the user. Each QR Z_t, $t = 1, \ldots, n$, is required to satisfy the ρ-recoverability condition described in Definition 2.1.[1]

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

$$\begin{aligned} P\left(Z^n = z^n | X^n = x^n\right) &\triangleq P\left(Z_1 = z_1, \ldots, Z_n = z_n | X_1 = x_1, \ldots, X_n = x_n\right) \\ &= \prod_{t=1}^{n} P\left(Z_t = z_t | X_t = x_t\right) \\ &= \prod_{t=1}^{n} W\left(z_t | x_t\right), \quad x^n \in \mathcal{X}^n, z^n \in \mathcal{Z}^n, \end{aligned} \tag{5.1}$$

[1] As observed in Remark (ii) after Definition 2.3, there is no loss of generality 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.

whereupon since $X_1, \ldots, X_n$ are i.i.d., so too are $Z_1, \ldots, Z_n$, with pmf

$(P_X W)(z) \triangleq \sum_{x \in \mathcal{X}} P_X(x) W(z|x), \ z \in \mathcal{Z}$. 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

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n\right) \triangleq \mathbb{E}\left[D\left(P_X || \widehat{P}_n\left(Z^n\right)\right)\right], \quad 0 \leq \rho \leq 1 \tag{5.2}$$

where $D(\cdot||\cdot)$ denotes divergence and expectation is with respect to the pmf $P_X W$. The user and querier devise (W, P_X) and $\widehat{P}_n$, respectively, to maximize and minimize $\pi_n\left(\rho, W, P_X, \widehat{P}_n\right)$. As in Chapters 2-4, 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 (5.2) so as to help contain notational growth.

Definition 5.1. For $0 \leq \rho \leq 1$, *distribution ρ-privacy* is

$$\pi_n(\rho) \triangleq \sup_{\substack{W: W(f(x)|x) \geq \rho \\ x \in \mathcal{X}}} \inf_{\widehat{P}_n : \mathcal{Z}^n \to \Delta_r} \sup_{P_X \in \Delta_r} \pi_n\left(\rho, W, P_X, \widehat{P}_n\right), \quad n \geq 1 \tag{5.3}$$

where W is as in (2.1) and $\pi_n\left(\rho, W, P_X, \widehat{P}_n\right)$ is given by (5.2).

Remarks:

(i) The order of maximizations and minimization in (5.3) 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 $\inf\limits_{\widehat{P}_n} \sup\limits_{W} \sup\limits_{P_X}$ in (5.3), 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 (5.3), if defined instead in terms of $\sup\limits_{W} \sup\limits_{P_X} \inf\limits_{\widehat{P}_n}$, would equal zero unrealistically. Also, reversing the roles of P_X and $\widehat{P}_n\left(Z^n\right)$ in $D\left(\cdot||\cdot\right)$ in (5.2), (5.3) leads to an unrealistic $\pi_n(\rho) = \infty$.

(iii) Clearly, it suffices to restrict the querier's estimators $\widehat{P}_n$ in (5.3) to those that satisfy $\widehat{P}_n\left(z^n\right)(x) > 0,\ z^n \in \mathcal{Z}^n,\ x \in \mathcal{X}$. If the querier were to assign $\widehat{P}_n\left(z^n\right)(x) = 0$ to any $x \in \mathcal{X}$, the user can choose $P_X(x) > 0$ for that x (since by (5.3), 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 (5.2). 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 (5.2) brings out this behavior in precise terms and quantifies its dependence on ρ and n. In fact, our main results in Theorems 5.3, 5.4 and 5.5 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

to make for a conservative (i.e., diminished) extent of privacy. The recoverability requirement in (2.1), (2.2) 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 (5.1), 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 5.1, 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 5.1. *For $0 \leq \rho \leq 1$, $\pi_n(\rho)$ is nonincreasing in $n \geq 1$. Furthermore,*

$$\pi_n(\rho) \leq \log r, \quad n \geq 1. \tag{5.4}$$

Proof: To show that $\pi_{n+1}(\rho) \leq \pi_n(\rho),\ n \geq 1$, observe by (5.2), (5.3) that in $\pi_{n+1}(\rho)$, for every fixed W,

$$\inf_{\widehat{P}_{n+1}:\mathcal{Z}^{n+1}\to\Delta_r} \sup_{P_X} \mathbb{E}\left[D\left(P_X||\widehat{P}_{n+1}\left(Z^{n+1}\right)\right)\right] \leq \inf_{\widehat{P}_n:\mathcal{Z}^{n+1}\to\Delta_r} \sup_{P_X} \mathbb{E}\left[D\left(P_X||\widehat{P}_n\left(Z^{n+1}\right)\right)\right] \tag{5.5}$$

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 (5.5) with respect to $z^{n+1} \in \mathcal{Z}^{n+1}$ is effectively over $z^n \in \mathcal{Z}^n$, we get

from (5.5) that

$$\inf_{\widehat{P}_{n+1}} \sup_{P_X} \mathbb{E}\left[D\left(P_X||\widehat{P}_{n+1}\left(Z^{n+1}\right)\right)\right] \leq \inf_{\widehat{P}_n} \sup_{P_X} \mathbb{E}\left[D\left(P_X||\widehat{P}_n\left(Z^n\right)\right)\right]. \tag{5.6}$$

Taking $\sup_W$ on both sides of (5.6) yields $\pi_{n+1}(\rho) \leq \pi_n(\rho)$.

Turning to (5.4), upon choosing $\widehat{P}_n\left(z^n\right)(x) = 1/r,\ z^n \in \mathcal{Z}^n,\ x \in \mathcal{X}$, we get from (5.2), (5.3) that

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

■

Given $z^n \in \mathcal{Z}^n$, let $Q^{(n)} = Q^{(n)}\left(z^n\right)$ be its n-type, i.e., the empirical pmf on $\mathcal{Z}$ associated with z^n (cf. e.g., [20]). 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 $(P_X W)^n\left(\mathcal{T}_{Q^{(n)}}\right) \triangleq \sum_{z^n \in \mathcal{T}_{Q^{(n)}}} (P_X W)^n\left(z^n\right)$. 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 (5.3) is provided by

Lemma 5.2. *For* $0 \leq \rho \leq 1$,

$$\pi_n(\rho) = \sup_W \inf_{\widehat{P}_n} \sup_{P_X} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} (P_X W)^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X||\widehat{P}_n\left(Q^{(n)}\right)\right) \tag{5.7}$$

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 $W, \widehat{P}_n, P_X$,

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n\right) = \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \sum_{z^n \in \mathcal{T}_{Q^{(n)}}} (P_X W)^n (z^n)\, D\left(P_X || \widehat{P}_n (z^n)\right). \tag{5.8}$$

For a fixed $Q^{(n)} \in \mathcal{Q}^{(n)}$, 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 picks as new estimator $\widehat{P}_n$ given by

$$\widehat{P}_n(z^n) = \frac{1}{\left|\mathcal{T}_{Q^{(n)}}\right|} \sum_{\tilde{z}^n \in \mathcal{T}_{Q^{(n)}}} \widehat{P}_n (\tilde{z}^n), \quad z^n \in \mathcal{T}_{Q^{(n)}}$$

(with an abuse of notation), denoted as $\widehat{P}_n\left(Q^{(n)}\right)$; by the convexity of $D(P_X||\cdot)$, this will only serve to decrease the right-side of (5.8), bearing in mind the $\inf$ with respect to $\widehat{P}_n$ in the right-side of (5.3). Then the right-side of (5.8) becomes

$$\sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} (P_X W)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X || \widehat{P}_n \left(Q^{(n)}\right)\right) \tag{5.9}$$

leading to (5.7). ■

5.3. Worst-Case Privacy

In this section, we present 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 5.4 by the converse and achievability results of Theorems 5.4 and 5.5, 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 5.4 and "locally uniform estimator" in Definition 5.2 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

$$P_X^l\left(f^{-1}\right) \triangleq \left(\underbrace{\frac{P_X\left(\bigcup_{l'=0}^{l-1} f^{-1}(l')\right)}{l},\ldots,\frac{P_X\left(\bigcup_{l'=0}^{l-1} f^{-1}(l')\right)}{l}}_{l \text{ repetitions}}, P_X\left(f^{-1}(l)\right),\ldots,P_X\left(f^{-1}(k-1)\right)\right). \quad (5.10)$$

In particular, for $l=1$ we denote

$$P_X^1\left(f^{-1}\right) \triangleq P_X\left(f^{-1}\right) = \left(P_X\left(f^{-1}(0)\right), P_X\left(f^{-1}(1)\right),\ldots,P_X\left(f^{-1}(k-1)\right)\right). \quad (5.11)$$

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

$$\omega(\rho) \triangleq \begin{cases} \log\left|\bigcup_{j\in\mathcal{Z}_k} f^{-1}(j)\right| = \log\left|f^{-1}(\mathcal{Z})\right| = \log|\mathcal{X}| = \log r, & 0\le\rho\le\frac{1}{k} \\ \max_{\mathcal{Z}_l\subset\mathcal{Z}} \log\left|\bigcup_{j\in\mathcal{Z}_l} f^{-1}(j)\right| = \max_{\mathcal{Z}_l\subset\mathcal{Z}} \log\sum_{j\in\mathcal{Z}_l}\left|f^{-1}(j)\right|, & \frac{1}{l+1}<\rho\le\frac{1}{l},\ 1\le l\le k-1, \end{cases} \quad (5.12)$$

which, under the assumption

$$|f^{-1}(0)|\ge|f^{-1}(1)|\ge\ldots\ge|f^{-1}(k-1)| \quad (5.13)$$

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

$$\max_{\mathcal{Z}_l \subset \mathcal{Z}} \log \sum_{j \in \mathcal{Z}_l} \left| f^{-1}(j) \right| = \log \sum_{j=0}^{l-1} \left| f^{-1}(j) \right|, \quad 1 \leq l \leq k-1. \tag{5.14}$$

It is verified readily from (5.12) that $\omega(\rho)$ is nonincreasing in $0 \leq \rho \leq 1$.

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

Theorem 5.3. *For each $n \geq 1$, $\pi_n(\rho)$ is nonincreasing in $0 \leq \rho \leq 1$, and*

$$\pi_n(\rho) \geq \omega(\rho), \quad 0 \leq \rho \leq 1 \tag{5.15}$$

and

$$\pi_n(\rho) = \omega(\rho) = \log r, \quad 0 \leq \rho \leq \frac{1}{k}. \tag{5.16}$$

Remark: By Theorem 5.3, for the "single-shot" case $n = 1$, $\pi_1(\rho) = \log r,\ 0 \leq \rho \leq 1/k$, and $\pi_1(\rho) \geq \omega(\rho),\ 1/k < \rho \leq 1$. However, a full characterization of $\pi_1(\rho)$ for $1/k < \rho \leq 1$ remains open.

Proof: For each $n \geq 1$, it is obvious by (5.3) that $\pi_n(\rho)$ is nonincreasing in $0 \leq \rho \leq 1$.

Turning to (5.15), we shall show that

$$\pi_n(\rho) \geq \max_{\mathcal{Z}_l \subseteq \mathcal{Z}} \log \left| \bigcup_{j \in \mathcal{Z}_l} f^{-1}(j) \right|, \ \ 0 \leq \rho \leq \frac{1}{l}, \ \ 1 \leq l \leq k \tag{5.17}$$

from which (5.15) is deduced readily.

Assume (5.13) without loss of essential generality. Fix $l \in \{1, \ldots, k\}$. For $0 \leq \rho \leq 1/l$,

the user selects

$W_l : \mathcal{X} \to \mathcal{Z}$ as

$$W_l(j|x) = \begin{cases} \frac{1}{l}, & x \in \bigcup_{l'=0}^{l-1} f^{-1}(l'),\ j = 0, 1, \ldots, l-1 \\ 1, & x \in \bigcup_{l'=l}^{k-1} f^{-1}(l'),\ j = f(x). \end{cases} \tag{5.18}$$

Clearly, $P_X W_l = P_X^l\left(f^{-1}\right)$ in Δ_k (see (5.10)). Expressing $\sup_{P_X \in \Delta_r}$ in (5.3) as

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

we obtain from (5.3), noting that the expectation in (5.2) is with respect to

$$P_X W_l = P_X^l\left(f^{-1}\right) = \underline{\alpha}^l \triangleq \left(\underbrace{\frac{\alpha}{l},\ldots,\frac{\alpha}{l}}_{l \text{ repetitions}}, \alpha_l, \ldots, \alpha_{k-1}\right) \tag{5.19}$$

that

$$\begin{aligned} \pi_n(\rho) &\geq \inf_{\widehat{P}_n} \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \sup_{P_X : P_X^l(f^{-1}) = \underline{\alpha}^l} \mathbb{E}_{\underline{\alpha}^l}\left[D\left(P_X || \widehat{P}_n\left(Z^n\right)\right)\right] \\ &\geq \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \inf_{\widehat{P}_n} \sup_{P_X : P_X^l(f^{-1}) = \underline{\alpha}^l} \mathbb{E}_{\underline{\alpha}^l}\left[D\left(P_X || \widehat{P}_n\left(Z^n\right)\right)\right] \\ &\geq \sup_{(\alpha,\alpha_l,\ldots,\alpha_{k-1})\in\Delta_{k-l+1}} \inf_{R\in\Delta_r} \sup_{P_X : P_X^l(f^{-1}) = \underline{\alpha}^l} D\left(P_X || R\right). \end{aligned} \tag{5.20}$$

Now, observe in (5.20) 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.

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

for some $(\beta, \beta_l, \ldots, \beta_{k-1}) \in \Delta_{k-l+1}$. Then in (5.20), for a fixed $(\alpha, \alpha_l, \ldots, \alpha_{k-1}) \in \Delta_{k-l+1}$,

$$\begin{aligned} &\inf_{R \in \Delta_r} \sup_{P_X : P_X^l(f^{-1}) = \underline{\alpha}^l} D\left(P_X||R\right) \\ &= \inf_{(\beta, \beta_l, \ldots, \beta_{k-1}) \in \Delta_{k-l+1}} \alpha \log \frac{\alpha}{\frac{\beta}{\left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right|}} + \sum_{j=l}^{k-1} \alpha_j \log \frac{\alpha_j}{\frac{\beta^j}{|f^{-1}(j)|}} \\ &= \inf_{(\beta, \beta_l, \ldots, \beta_{k-1}) \in \Delta_{k-l+1}} \alpha \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right| + \sum_{j=l}^{k-1} \alpha_j \log \left|f^{-1}(j)\right| \\ &\qquad\qquad + D\left((\alpha, \alpha_l, \ldots, \alpha_{k-1}) \,||(\beta, \beta_l, \ldots, \beta_{k-1})\right) \\ &= \alpha \log \left|\bigcup_{l'=0}^{l-1} f^{-1}(l')\right| + \sum_{j=l}^{k-1} \alpha_j \log \left|f^{-1}(j)\right| \end{aligned} \tag{5.21}$$

with the minimum attained by $(\beta, \beta_l, \ldots, \beta_{k-1}) = (\alpha, \alpha_l, \ldots, \alpha_{k-1})$. Combining (5.20) and (5.21),

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

$$= \log \left| \bigcup_{l'=0}^{l-1} f^{-1}(l') \right| \tag{5.22}$$

with the maximum attained by

$$\alpha = 1, \alpha_l = \cdots = \alpha_{k-1} = 0 \tag{5.23}$$

upon recalling (5.13). This establishes (5.17) with the obvious replacement by the right-side therein of the right-side of (5.22).

Turning to (5.16), observe that with $l = k$ and $0 \leq \rho \leq 1/k$, we get from (5.22) that $\pi_n(\rho) \geq \log r$. With Proposition 5.1, (5.16) follows. ■

The results of Theorem 5.3 are interpreted as follows. Theorem 5.3 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 (5.12), $\pi_n(\rho)$ is at least $\omega(\rho) = \max\limits_{\mathcal{Z}_l \subset \mathcal{Z}} \log \sum\limits_{j \in \mathcal{Z}_l} |f^{-1}(j)|$, 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 (5.20), and (5.23)) and ρ-QR W_l as in (5.18). 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 (5.19). This helps explain the form of $\omega(\rho)$. We note at this point that Theorem 5.5 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 5.3, together with Theorem 5.4, will establish that $\lim\limits_{n} \pi_n(\rho) = \omega(\rho)$ for $0.5 < \rho \leq 1$.

5.4. Distribution ρ-Privacy

Our main Theorems 5.4 and 5.5 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, recalling Definition 2.2, add-noise ρ-QRs are material in the converse proof.

Definition 5.2. 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 5.3. Consider any partition of $\mathcal{Z}$ into $k' \leq k$ 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* $\widehat{P}_n : \mathcal{Q}'^{(n)} \to \Delta_r$, $n \geq 1$, is such that for some $\gamma_n > 0$, $\hat{\gamma}_n > 0$ and $c_n > 0$, $n \geq 1$, with

$$\lim_n \gamma_n = 0, \quad \lim_n \hat{\gamma}_n = 0, \quad \lim_n c_n = 0 \quad \text{and} \quad \frac{\hat{\gamma}_n}{c_n} = o\left(\frac{1}{n}\right) \quad \text{implying} \quad \lim_n \frac{\hat{\gamma}_n}{c_n} = 0, \tag{5.24}$$

it holds for $Q'^{(n)} \neq Q''^{(n)}$ on $\mathcal{Z}'$ with $\text{var}\left(Q'^{(n)}, Q''^{(n)}\right) \leq \gamma_n$ that

$\text{var}\left(\widehat{P}_n\left(Q'^{(n)}\right), \widehat{P}_n\left(Q''^{(n)}\right)\right) \leq \hat{\gamma}_n$, where $\text{var}(\cdot,\cdot)$ denotes variational distance (in $\Delta_{k'}$ or Δ_r); and for each $Q'^{(n)} \in \mathcal{Q}'^{(n)}$, $\widehat{P}_n\left(Q'^{(n)}\right)(x) \geq c_n,\ x \in \mathcal{X}$. Denote the class of all such estimators by $\mathcal{S}_n = \mathcal{S}_n(k'),\ n \geq 1$.

Remark: A smooth estimator has the feature that QRs with neighboring types lead to proximate pmf estimates by the querier. Its second feature of full support $\mathcal{X}$ is motivated by Remark (iii) following Definition 5.1.

Definition 5.4. A *k-sparse pmf* P_X^{sp} on $\mathcal{X}$ is defined by

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

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

Definition 5.5. Let $\mathcal{V}(\rho)$ be the set of all stochastic matrices $V : \mathcal{Z} \to \mathcal{Z}$ with $V(j|j) \geq \rho,\ j \in \mathcal{Z}$. For each $V \in \mathcal{V}(\rho)$, set

$$\Delta_k(V) \triangleq \{\underline{\alpha} \in \Delta_k : \underline{\alpha} = \underline{\beta}V \text{ for some } \underline{\beta} \in \Delta_k\}. \tag{5.25}$$

Recall from Lemma 2.1 that for an add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$, there exists a ρ-QR $W = W(V) : \mathcal{X} \to \mathcal{Z}$ with identical rows for all $x \in f^{-1}(i),\ i \in \mathcal{Z}$, such that $\pi_\rho(W) = \pi_\rho(V)$. Throughout the rest of the chapter, for an add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$, we shall denote by W^V the corresponding ρ-QR $W(V) : \mathcal{X} \to \mathcal{Z}$.

Remarks:

(i) For any P_X in Δ_r and add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$ with the corresponding ρ-QR $W^V : \mathcal{X} \to \mathcal{Z}$, it follows that $P_X W^V = P_X \left(f^{-1}\right) V$, both being in Δ_k.

(ii) For $V \in \mathcal{V}(\rho),\ 0.5 < \rho \leq 1$, V is diagonally-dominated so that V^{-1} exists [63, Theorem 3.3.9].

The following (information geometric) notion will be pertinent for our converse Theorem 5.4. For $Q^{(n)}$ in $\mathcal{Q}^{(n)}$, and $V \in \mathcal{V}(\rho),\ 0.5 < \rho \leq 1$, let

$$\widetilde{Q}\left(Q^{(n)}\right) \triangleq \arg \min_{Q \in \Delta_k(V)} D\left(Q^{(n)} || Q\right) \tag{5.26}$$

be the reverse I-projection of $Q^{(n)}$ on $\Delta_k(V)$; and for all $\rho > 0$, the minimum exists by [19, 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 $V(j|j) \geq \rho,\ j \in \mathcal{Z}$. Noting by (5.25) that $\widetilde{Q}\left(Q^{(n)}\right) V^{-1}$ lies in Δ_k, let $\kappa_n\left(Q^{(n)}\right)$ be its positivized[2] version in Δ_k defined as

$$\kappa_n\left(Q^{(n)}\right)(j) = \frac{n\left(\widetilde{Q}\left(Q^{(n)}\right) V^{-1}\right)(j) + 1}{n + k}, \quad j \in \mathcal{Z}. \tag{5.27}$$

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

If the user chooses an add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$, then $Z_1, \ldots, Z_n$ are i.i.d. with (common) pmf $P_X W^V = P_X(f^{-1})V$ (see (5.11)) and $P_X(f^{-1})V$ belongs to $\Delta_k(V)$ (see Definition 5.5). 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 $\widetilde{Q}\left(Q^{(n)}\right)$ (5.26). Therefore, if the querier is restricted to using a locally uniform estimator (see

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

Definition 5.2), a natural choice for $\beta^{(n)}$ as an attendant proxy for $P_X(f^{-1})$ is κ_n given by (5.27) and this plays a role in our converse result below.

We now state Theorems 5.4 and 5.5 whose proofs are contained in Section 5.5. Hereafter, we make Assumption (5.13) without loss of essential generality; this assumption is made only for the sake of notational convenience. In particular, the upper bound in Theorem 5.4 for $\pi_n(\rho)$, $0.5 < \rho \leq 1$, tends to the lower bound in Theorem 5.3 as $n \to \infty$. Theorem 5.5 gives a lower bound for $\pi_n(\rho),\ 1/k < \rho \leq 1$, that approaches, as $n \to \infty$, worst-case privacy in Theorem 5.3. *A notable characteristic of Theorems 5.3, 5.4 and 5.5 is that for all* $0 \leq \rho \leq 1$, *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 $0.5 < \rho \leq 1$, a converse (upper) bound for $\pi_n(\rho),\ n \geq 1$, and thereby for $\lim\limits_{n}\ \pi_n(\rho)$, is given by

Theorem 5.4. *For* $0.5 < \rho \leq 1$ *and every* $n \geq 1$,

$$\pi_n(\rho) \leq \omega(\rho) + \Gamma_n(\rho) = \max_{j \in \mathcal{Z}} \log \left| f^{-1}(j) \right| + \Gamma_n(\rho), \tag{5.28}$$

where

$$\Gamma_n(\rho) \triangleq \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q^{(n)}} \right) D \left(\underline{\alpha} V^{-1} || \kappa_n \left(Q^{(n)} \right) \right). \tag{5.29}$$

Furthermore,

$$\lim_{n}\ \Gamma_n(\rho) = 0 \ \textit{and}\ \lim_{n} \pi_n(\rho) = \max_{j \in \mathcal{Z}} \log \left| f^{-1}(j) \right|. \tag{5.30}$$

Remarks:

(i) In (5.28), note that $\omega(\rho) = \max_{j \in \mathcal{Z}} \log |f^{-1}(j)|$ by (5.12); and additionally under (5.13), $\omega(\rho) = \log |f^{-1}(0)|$.

(ii) In general, a closed-form expression is not available for the reverse I-projection $\widetilde{Q}\left(Q^{(n)}\right)$ in (5.26); an iterative method for computing it is described in [19, Example 5.1]. Hence, $\kappa_n\left(Q^{(n)}\right)$ in (5.27) and $\Gamma_n(\rho)$ in (5.29) lack explicit expressions.

The following achievability result is for $1/k < \rho \leq 1$; for $0 \leq \rho \leq 1/k$, Theorem 5.3 above already characterizes $\pi_n(\rho)$.

Theorem 5.5. *Let $1/k < \rho \leq 1$. For appropriate add-noise ρ-QRs $V = V(\rho)$, it holds that for the (restricted) class of smooth estimators for the querier*

$$\begin{aligned} \inf_{\widehat{P}_n \in \mathcal{S}_n} \sup_{P_X} \pi_n\left(\rho, W^V, P_X, \widehat{P}_n\right) &\geq \left(\omega(\rho) + \Lambda_n(\rho)\right) \lambda_n(\rho) \\ &= \left(\log \sum_{j=0}^{l-1} |f^{-1}(j)| + \Lambda_n(\rho)\right) \lambda_n(\rho), \quad \frac{1}{l+1} < \rho \leq \frac{1}{l}, \ \ 1 \leq l \leq k-1, \end{aligned} \tag{5.31}$$

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

$$\Lambda_n(\rho) \triangleq \begin{cases} \log\left(1+\dfrac{\sum\limits_{j=l}^{\lfloor\frac{k}{l}\rfloor l-1}\left|f^{-1}(j)\right|}{e\sum\limits_{j=0}^{l-1}\left|f^{-1}(j)\right|}\dfrac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{\lfloor\frac{k}{l}\rfloor l-l}\right)\right\rceil}{n},\, l\rho\right\}-l\left(\frac{1-l\rho}{\lfloor\frac{k}{l}\rfloor l-l}\right)}{l\rho-l\left(\frac{1-l\rho}{\lfloor\frac{k}{l}\rfloor l-l}\right)}\right)-\frac{\hat{\gamma}_n}{c_n}, & \\ \qquad\qquad \sum\limits_{j=l}^{\lfloor\frac{k}{l}\rfloor l-1}|f^{-1}(j)| \le \sum\limits_{j=0}^{l-1}|f^{-1}(j)| & \\ \log\left(\dfrac{\sum\limits_{j=l}^{\lfloor\frac{k}{l}\rfloor l-1}\left|f^{-1}(j)\right|}{\sum\limits_{j=0}^{l-1}\left|f^{-1}(j)\right|}\right)\dfrac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{\lfloor\frac{k}{l}\rfloor l-l}\right)\right\rceil}{n},\, l\rho\right\}-l\left(\frac{1-l\rho}{l\lfloor\frac{k}{l}\rfloor-l}\right)}{l\rho-l\left(\frac{1-l\rho}{\lfloor\frac{k}{l}\rfloor l-l}\right)}-\frac{\hat{\gamma}_n}{c_n}, & \\ \qquad\qquad \sum\limits_{j=l}^{\lfloor\frac{k}{l}\rfloor l-1}|f^{-1}(j)| > \sum\limits_{j=0}^{l-1}|f^{-1}(j)| & \end{cases} \tag{5.32}$$

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

$$\Lambda_n(\rho) \triangleq \log\left(1+\frac{|f^{-1}(l)|}{e\sum\limits_{j=0}^{l-1}|f^{-1}(j)|}\frac{\frac{\lceil n(1-l\rho)\rceil}{n}-(1-l\rho)}{l\rho}\right)-\frac{\hat{\gamma}_n}{c_n} \tag{5.33}$$

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

$$\lambda_n(\rho) \triangleq 1-\frac{3e^{\left(\frac{4\left(\lfloor\frac{k}{l}\rfloor+k-\lfloor\frac{k}{l}\rfloor l-1\right)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}} \quad \textit{with } \zeta > 1. \tag{5.34}$$

Furthermore

$$\lim_n \Lambda_n(\rho) = 0, \quad \lim_n \lambda_n(\rho) = 1, \quad \frac{1}{k} < \rho \le 1 \tag{5.35}$$

and

$$\lim_{n} \inf_{\widehat{P}_n \in \mathcal{S}_n} \sup_{P_X} \pi_n\left(\rho, W^V, P_X, \widehat{P}_n\right) \geq \omega(\rho)$$
$$= \log \sum_{j=0}^{l-1} |f^{-1}(j)|, \quad \frac{1}{l+1} < \rho \leq \frac{1}{l}, \ \ 1 \leq l \leq k-1. \quad (5.36)$$

Remarks:

(i) The proof of Theorem 5.5 will show achievability with the user's choice of P_X taking the form of appropriate sparse pmfs. Note that the left-side of (5.31) serves as a lower bound for $\pi_n(\rho)$ for the class of smooth querier's estimators.

(ii) In (5.31) and (5.36), $\omega(\rho) = \log \sum_{j=0}^{l-1} |f^{-1}(j)|$ by (5.12) and (5.13).

(iii) Our result in Theorem 5.5 must be qualified. In (5.31), the $\log$ terms in (5.32), (5.33) 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 (5.31) strictly exceeds $\omega(\rho)$ for all large and suitable (but for those from the mentioned set) n.

The proofs of Theorems 5.4 and 5.5 are provided in Sections 5.5.1 and 5.5.2, respectively.

We close this section by interpreting the results of Theorems 5.3, 5.4 and 5.5 when particularized to $f : \mathcal{X} \to \mathcal{Z} = \mathcal{X}$ being a one-to-one mapping. Then a ρ-QR $W : \mathcal{X} \to \mathcal{X}$ is an $r \times r$-stochastic matrix with diagonal elements $\geq \rho$. Loosely speaking,

(a) for $0 \leq \rho \leq 0.5$, it is clear that no accurate estimation of P_X from $Z_1, \ldots, Z_n$ – in the sense of the right-side of (5.3) tending to 0 as $n \to \infty$ – is possible by the querier;

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

In this context, by Theorem 5.3, for all $n \geq 1$,

$$\pi_n(\rho) \begin{cases} = \omega(\rho) = \log r, & 0 \leq \rho \leq \frac{1}{r} \\ \geq \omega(\rho) = \log l, & \frac{1}{l+1} < \rho \leq \frac{1}{l}, \ \ 1 \leq l \leq r-1 \end{cases} \tag{5.37}$$

which, since $\omega(\rho) > 0$ for $0 \leq \rho \leq 0.5$ by (5.37), reinforces (a) above. Next, $\omega(\rho) = 0$ for $0.5 < \rho \leq 1$ by (5.37), and Theorem 5.4 gives that for every $n \geq 1$,

$$\pi_n(\rho) \leq \Gamma_n(\rho)$$

by (5.28), (5.29), where the inner and outer suprema in (5.29) 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 (5.30), in keeping with (b) above. However, by Theorem 5.5, 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 (5.32), (5.33) and (5.34), respectively, with $k = r$ and $|f^{-1}(j)| = 1, \ j = 0, \ldots, r-1$.

5.5. Converse and Achievability Theorems

The following technical Lemmas 5.6 and 5.7 are pertinent to the proofs of Theorems 5.4 and 5.5, respectively. Their proofs are relegated to Appendix D.1.

Lemma 5.6. *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

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

with equality iff P is a k-point mass with

$$P(x_j') = P(A_j) \quad \textit{for some } x_j' \in A_j,\ j \in \mathcal{Z}. \tag{5.38}$$

Lemma 5.7. *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.

5.5.1. Converse Proof

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 (5.3). 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 (5.3) of locally uniform estimators.

Proceeding with this reasoning, a crucial facilitating step for the proof of Theorem 5.4 is to show that when the querier uses a locally uniform estimator, the user's actions can be limited to k-sparse pmfs and add-noise ρ-QRs *without loss of distribution privacy.*

Lemma 5.8. *Fix* $0 \leq \rho \leq 1$. *For every* $n \geq 1$ *and* $\beta^{(n)} = \left\{\beta^{(n)}\left(Q^{(n)}\right)\right\}_{Q^{(n)} \in \mathcal{Q}^{(n)}}$,

$$\sup_{W} \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X} \pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right) = \sup_{V} \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X^{sp}} \pi_n\left(\rho, W^V, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right). \tag{5.39}$$

Proof: Since the suprema in the right-side of (5.39) are over restricted sets, it suffices to show that (5.39) holds with "$\leq$." Specifically, we show that for every P_X and ρ-QR W there exist P_X^{sp} and add-noise ρ-QR V such that

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right) \leq \pi_n\left(\rho, W^V, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right). \tag{5.40}$$

To this end, let

$$P_X^{sp}(x) = P_X\left(f^{-1}(j)\right), \quad \text{for some } x \in f^{-1}(j),\ j \in \mathcal{Z} \ \text{(see Definition 5.4)}, \tag{5.41}$$

and let add-noise ρ-QR $V : \mathcal{Z} \to \mathcal{Z}$ be specified as follows:

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

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

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

$$V(j'|j)=\begin{cases}\rho, & j'=j\\ \frac{1-\rho}{k-1}, & j'\neq j\in\mathcal{Z}.\end{cases}$$

The corresponding ρ-QR $W^V:\mathcal{X}\to\mathcal{Z}$ is as follows:

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

$$W^V(j'|x)=\sum_{x'\in f^{-1}(j)}\frac{P_X(x')}{P_X\left(f^{-1}(j)\right)}W(j'|x'),\quad j'\in\mathcal{Z} \tag{5.42}$$

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

$$W^V(j'|x)=\begin{cases}\rho, & j'=j\\ \frac{1-\rho}{k-1}, & j'\neq j\in\mathcal{Z}.\end{cases} \tag{5.43}$$

From (5.41), (5.42) and (5.43), it is clear that for each $j\in\mathcal{Z}$,

$$\begin{aligned}\left(P_XW\right)(j)&=\sum_{x\in\mathcal{X}}P_X(x)W(j|x)\\ &=\sum_{j'\in\mathcal{Z}:P_X\left(f^{-1}(j')\right)>0}\ \sum_{x\in f^{-1}(j')}P_X(x)W(j|x)\\ &=\sum_{j'\in\mathcal{Z}:P_X\left(f^{-1}(j')\right)>0}P_X\left(f^{-1}(j')\right)\sum_{x\in f^{-1}(j')}\frac{P_X(x)}{P_X\left(f^{-1}(j')\right)}W(j|x)\\ &=\sum_{j'\in\mathcal{Z}:P_X\left(f^{-1}(j')\right)>0}P_X^{sp}(x')\,W^V(j|x'),\quad \text{for some } x'\in f^{-1}(j')\\ &=\left(P_X^{sp}W^V\right)(j)\end{aligned} \tag{5.44}$$

where the fourth equality above uses (5.41) and (5.42). Then, using (5.9) and (5.41) - (5.44),

$$\pi_n\left(\rho, W, P_X, \widehat{P}_n^{\beta^{(n)}}\right) = \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \left(P_X^{sp} W^V\right)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X || \widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right). \tag{5.45}$$

Moreover, by Lemma 5.6,

$$\begin{aligned} D\left(P_X || \widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right) &\leq D\left(P_X\left(f^{-1}\right) || \beta^{(n)}\left(Q^{(n)}\right)\right) + \sum_{j \in \mathcal{Z}} P_X\left(f^{-1}(j)\right) \log |f^{-1}(j)| \\ &= D\left(P_X^{sp} || \widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right) \end{aligned} \tag{5.46}$$

by (5.41) and Definition 5.2. By (5.45) and (5.46), and recalling (5.9)

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

which is (5.40). ■

Proof of Theorem 5.4: In (5.3), upon restricting the querier's choice to locally uniform estimators and using Lemma 5.8, we get

$$\pi_n(\rho) \leq \sup_V \inf_{\widehat{P}_n^{\beta^{(n)}}} \sup_{P_X^{sp}} \pi_n\left(\rho, W^V, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right). \tag{5.47}$$

For fixed add-noise ρ-QR V and P_X^{sp}, let

$$\underline{\alpha} = P_X^{sp} W^V = P_X^{sp}\left(f^{-1}\right) V. \tag{5.48}$$

Since $\rho > 0.5$, V^{-1} exists (see Remark (ii) following Definition 5.5). Then, upon fixing $\widehat{P}_n^{\beta^{(n)}}$, too, using (5.9) and (5.48) we get

$$\begin{aligned}\pi_n\left(\rho, W^V, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right) &= \sum_{Q^{(n)}\in\mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X^{sp}||\widehat{P}_n^{\beta^{(n)}}\left(Q^{(n)}\right)\right) \\ &= \sum_{Q^{(n)}\in\mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X^{sp}\left(f^{-1}\right)||\beta^{(n)}\left(Q^{(n)}\right)\right) \\ &\quad + \sum_{j\in\mathcal{Z}} P_X^{sp}\left(f^{-1}(j)\right)\log|f^{-1}(j)| \end{aligned} \tag{5.49}$$

by equality in Lemma 5.6. Next, note from (5.48) that

$$P_X^{sp}\left(f^{-1}\right) = \underline{\alpha}\, V^{-1}. \tag{5.50}$$

Then, from (5.49) and (5.50),

$$\begin{aligned}\pi_n\left(\rho, W^V, P_X^{sp}, \widehat{P}_n^{\beta^{(n)}}\right) &\le \max_{j\in\mathcal{Z}} \log|f^{-1}(j)| \\ &\quad + \sum_{Q^{(n)}\in\mathcal{Q}^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\, V^{-1}\middle|\middle|\beta^{(n)}\left(Q^{(n)}\right)\right). \end{aligned} \tag{5.51}$$

Hence, in (5.47) upon using (5.48) - (5.51),

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

$$+ \sup_{\substack{V:\mathcal{Z}\to\mathcal{Z} \\ V(j'|j')\geq\rho,\ j'\in\mathcal{Z}}} \inf_{\beta^{(n)}\left(Q^{(n)}\right)} \sup_{\underline{\alpha}\in\Delta_k(V)} \sum_{Q^{(n)}\in\mathcal{Q}^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(\underline{\alpha}\, V^{-1} || \beta^{(n)}\left(Q^{(n)}\right)\right).$$

Upon choosing $\beta^{(n)}\left(Q^{(n)}\right) = \kappa_n\left(Q^{(n)}\right)$ (see (5.27)) and by Definition 5.5, which defines $\mathcal{V}(\rho)$, we get

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

which is (5.29).

Next, to show (5.30), 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

$$\begin{aligned}
\Gamma_n(\rho) &= \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}_{\underline{\alpha}} \left[\sum_{j\in\mathcal{Z}} \left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right] \\
&= \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \sum_{j\in\mathcal{Z}} \mathbb{E}_{\underline{\alpha}} \left[\left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right] \\
&\leq \sum_{j\in\mathcal{Z}} \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} \mathbb{E}_{\underline{\alpha}} \left[\left(\underline{\alpha} V^{-1}\right)(j) \log \frac{\left(\underline{\alpha} V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right]. \qquad (5.52)
\end{aligned}$$

Denoting the rvs in $[\cdots]$ in (5.52) above by

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

we show in Appendix D.2 that

$$\lim_{n} \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \mathbb{E}\left[|\Phi_n^j(\underline{\alpha}, V)|\right] = 0, \quad j \in \mathcal{Z}. \tag{5.53}$$

Then, by (5.52) and (5.53), the first assertion in (5.30) obtains. The second assertion in (5.30) follows from (5.52), (5.53) and (5.12), (5.15) with $l = 1$. ■

5.5.2. Achievability Proof

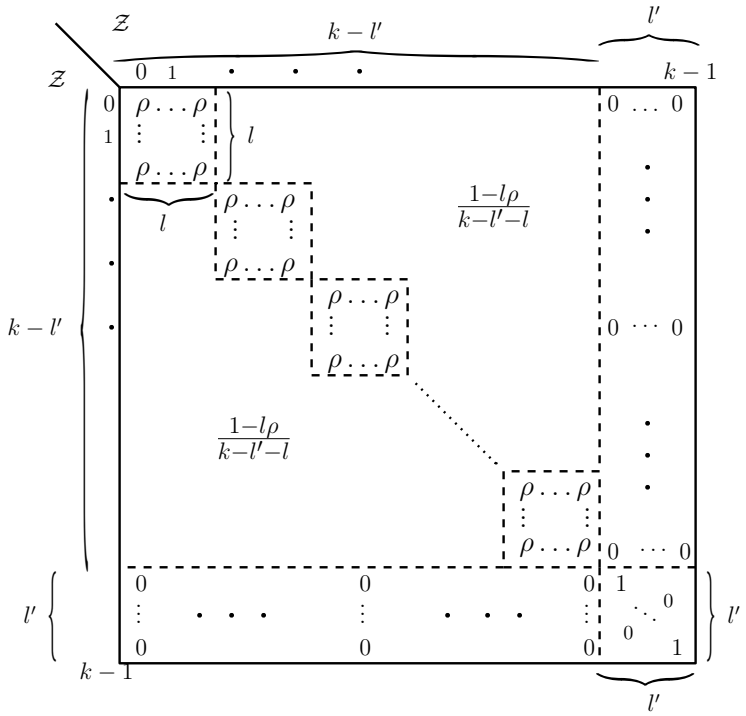


Figure 5.1: $V_1 : \mathcal{Z} \to \mathcal{Z}$

Proof of Theorem 5.5: Fix $1/k < \rho \leq 1$. As in the statement of the theorem, $l = l(\rho)$ is determined by

$$\frac{1}{l+1} < \rho \leq \frac{1}{l}, \quad 1 \leq l \leq k-1. \tag{5.54}$$

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[3] $l > \left\lfloor \frac{k}{2} \right\rfloor$:

1. description of chosen add-noise ρ-QRs $V_1 : \mathcal{Z} \to \mathcal{Z}$ and $V_2 : \mathcal{Z} \to \mathcal{Z}$ for the two cases, respectively;

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 D.3.

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

Step 1: The user selects P_X (to be specified later) and an add-noise ρ-QR $V_1 = V_1(\rho) : \mathcal{Z} \to \mathcal{Z}$ described next. It is assumed that the rows of V_1 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

$$l' = l'(\rho) \triangleq k - \left\lfloor \frac{k}{l} \right\rfloor l. \tag{5.55}$$

Clearly $0 \leq l' < l$. Then, as illustrated in Fig. 5.1, $V_1 : \mathcal{Z} \to \mathcal{Z}$ 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;

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

- 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

$$\left\lfloor \frac{k}{l} \right\rfloor \geq \left\lfloor \frac{k}{\lfloor \frac{k}{2} \rfloor} \right\rfloor \geq \left\lfloor \frac{k}{\frac{k}{2}} \right\rfloor = 2 \quad \text{so that} \quad k - l' - l = \left\lfloor \frac{k}{l} \right\rfloor l - l \geq 2l - l = l \geq 1. \tag{5.56}$$

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 $\lfloor \frac{k}{l} \rfloor$ blocks of l rows that are identical (and distinct among such blocks), with $\lfloor \frac{k}{l} \rfloor$ $l \times l$ 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 $\lfloor \frac{k}{l} \rfloor = \frac{k-l'}{l}$ 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

$$\mathcal{Z}' \triangleq \left\{0, 1, \ldots, \frac{k - l'}{l} - 1, \frac{k - l'}{l}, \ldots \frac{k - l'}{l} + l' - 1\right\} \tag{5.57}$$

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

$$k' = k'(\rho) \triangleq \frac{k - l'}{l} + l' = \left\lfloor \frac{k}{l} \right\rfloor + l' \leq k \tag{5.58}$$

on which $P_X\left(f^{-1}\right) V_1$ can have possibly different probability values. The resulting merged

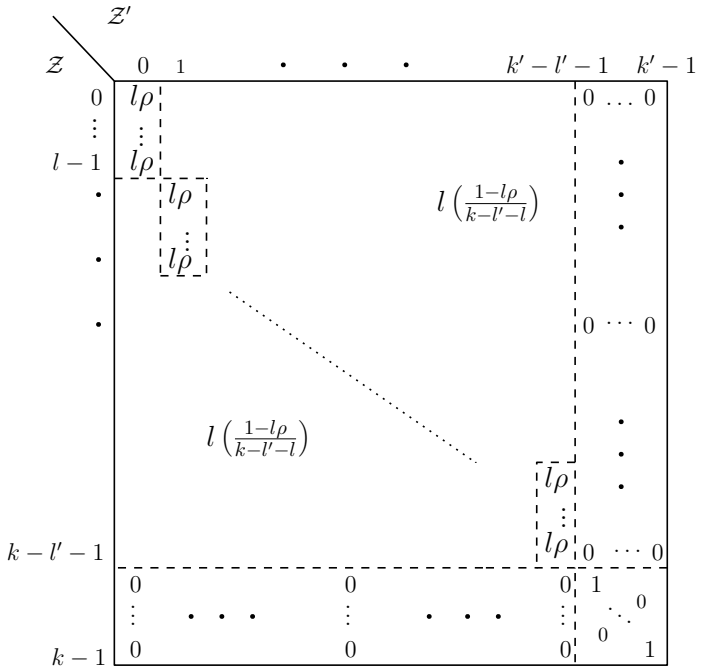


Figure 5.2: $V_1' : \mathcal{Z} \to \mathcal{Z}'$

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. 5.2, and is described as follows.

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

$$V_1'(j'|j)$$
$$= \begin{cases} l\rho, & j' = 0,1,\ldots,k'-l'-1, \quad j = j'\cdot l,\ldots,(j'+1)l-1 \\ l\left(\frac{1-l\rho}{k-l'-l}\right), & j' = 0,1,\ldots,k'-l'-1, \quad j \ne j'\cdot l,\ldots,(j'+1)l-1, \quad j \le k-l'-1 \\ 1, & (j'=k'-l', j=k-l'),\ldots,(j'=k'-1, j=k-1) \\ 0, & \text{otherwise.} \end{cases} \tag{5.59}$$

For the user's choice of $V_1 : \mathcal{Z} \to \mathcal{Z}$ 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 (5.59). Let $\mathcal{Q}'^{(n)}$ denote the set of all types on $\mathcal{Z}'^n$. Then precisely, referring to (5.9), we claim that

$$\begin{aligned}
&\inf_{\widehat{P}_n : \mathcal{Q}^{(n)} \to \Delta_r} \sup_{P_X} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \left(P_X \left(f^{-1}\right) V_1\right)^n \left(\mathcal{T}_{Q^{(n)}}\right) D\left(P_X || \widehat{P}_n \left(Q^{(n)}\right)\right) \\
&\qquad = \inf_{\widehat{P}_n : \mathcal{Q}'^{(n)} \to \Delta_r} \sup_{P_X} \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \left(P_X \left(f^{-1}\right) V_1'\right)^n \left(\mathcal{T}_{Q'^{(n)}}\right) D\left(P_X || \widehat{P}_n \left(Q'^{(n)}\right)\right) \quad (5.60)
\end{aligned}$$

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 (5.57); 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 5.2, the claim in (5.60) follows.

Hereafter in this proof, we restrict attention in (5.60) to smooth estimators $\widehat{P}_n : \mathcal{Q}'^{(n)} \to \Delta_r$. Then, recalling (5.9), we get from (5.60) that

$$\begin{aligned}
&\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \pi_n\left(\rho, W^{V_1}, P_X, \widehat{P}_n\right) \\
&= \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \left(P_X (f^{-1}) V_1'\right)^n \left(\mathcal{T}_{Q'^{(n)}}\right) \; D\left(P_X || \widehat{P}_n \left(Q'^{(n)}\right)\right) \\
&= \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X (f^{-1}) V_1' = \underline{\alpha}} \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q'^{(n)}}\right) \; D\left(P_X || \widehat{P}_n \left(Q'^{(n)}\right)\right). \quad (5.61)
\end{aligned}$$

The sum in the right-side of (5.61) 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,

$$\sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q'^{(n)}}\right) \; D\left(P_X || \widehat{P}_n \left(Q'^{(n)}\right)\right)$$

$$\geq \sum_{Q'^{(n)} \in \mathcal{Q}'^{(n)}:\ \mathrm{var}\left(Q'^{(n)}, Q'^{(n)}(\underline{\alpha})\right) \leq \gamma_n} \underline{\alpha}^n \left(\mathcal{T}_{Q'^{(n)}}\right) \; D\left(P_X || \widehat{P}_n \left(Q'^{(n)}\right)\right) \quad (5.62)$$

where

$$Q'^{(n)}(\underline{\alpha})(j') = \frac{\lceil n\underline{\alpha}(j') \rceil}{n}, \quad j' = 1, \ldots, k'-1 \quad \text{and} \quad Q'^{(n)}(\underline{\alpha})(0) = 1 - \sum_{j' \neq 0} \frac{\lceil n\underline{\alpha}(j') \rceil}{n} \quad (5.63)$$

and γ_n will be specified below. For $Q'^{(n)}(\underline{\alpha})$ in (5.63) 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

$$1 - \sum_{j' \neq 0} \frac{n\underline{\alpha}(j') + 1}{n} = \underline{\alpha}(0) - \frac{k'-1}{n} \geq 0. \quad (5.64)$$

In Appendix D.3, we shall show that $\underline{\alpha} \in \Delta_{k'}$ can be restricted further and n chosen large enough with

$$n \geq N_0(k') = 2k', \quad (5.65)$$

so that (5.64) 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 5.3). Then in the right-side of (5.62), by Lemma 5.7,

$$D\left(P_X||\widehat{P}_n\left(Q'^{(n)}\right)\right) \geq D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\text{var}\left(\widehat{P}_n\left(Q'^{(n)}\right), \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)}{\min\limits_{x\in\mathcal{X}} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}$$

$$\geq D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\hat{\gamma}_n}{c_n}. \tag{5.66}$$

Hence in (5.62), using (5.66),

$$\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}} \underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right)\ D\left(P_X||\widehat{P}_n\left(Q'^{(n)}\right)\right)$$

$$\geq \left[D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\hat{\gamma}_n}{c_n}\right] \sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}:\ \text{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n} \underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right). \tag{5.67}$$

Next, in the right-side of (5.67), with T'_n denoting a $\mathcal{Q}'^{(n)}$-valued rv with underlying pmf $\underline{\alpha}\in\Delta_{k'}$, we get

$$\sum_{Q'^{(n)}\in\mathcal{Q}'^{(n)}:\ \text{var}\left(Q'^{(n)},Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n} \underline{\alpha}^n\left(\mathcal{T}_{Q'^{(n)}}\right) = P\left(\text{var}\left(T'_n, Q'^{(n)}(\underline{\alpha})\right)\leq\gamma_n\right) \tag{5.68}$$

$$= 1 - P\left(\text{var}\left(T'_n, Q'^{(n)}(\underline{\alpha})\right) > \gamma_n\right)$$

$$\geq 1 - P\left(\text{var}\left(T'_n,\underline{\alpha}\right) + \text{var}\left(\underline{\alpha}, Q'^{(n)}(\underline{\alpha})\right)\geq\gamma_n\right) \tag{5.69}$$

$$\geq 1 - P\left(\text{var}\left(T'_n,\underline{\alpha}\right)\geq\gamma_n - \frac{2(k'-1)}{n}\right) \tag{5.70}$$

where (5.69) is by the triangle inequality for $\text{var}(\cdot,\cdot)$, and (5.70) holds since

var $\left(\underline{\alpha}, Q'^{(n)}(\underline{\alpha})\right) \leq \frac{2(k'-1)}{n}$ by (5.63). Denoting

$$\epsilon_n = \gamma_n - \frac{2(k'-1)}{n}, \tag{5.71}$$

we obtain by [21, Lemma 3] that

$$P\left(\text{var}\left(T'_n, \underline{\alpha}\right) \geq \epsilon_n\right) \leq 3e^{\left(-n\frac{\epsilon_n^2}{25}\right)} \tag{5.72}$$

for all n such that

$$\epsilon_n > 0 \quad \text{and} \quad n\epsilon_n^2 \geq 20k'. \tag{5.73}$$

Now, pick

$$\gamma_n = 5\sqrt{\frac{\zeta \ln 2 \log n}{n}}, \quad n \geq 1 \text{ and } \zeta > 1 \tag{5.74}$$

so that $\lim_n \gamma_n = 0$. Then (5.73) 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 $n \geq \max\{N_1(k'), N_2(k')\}$, (5.72) holds, and thereby by (5.71) and (5.74),

$$P\left(\text{var}\left(T'_n, \underline{\alpha}\right) \geq \gamma_n - \frac{2(k'-1)}{n}\right) \leq \frac{3e^{\left(\frac{-4(k'-1)^2}{25n}\right)} e^{\left(\frac{4(k'-1)}{5}\sqrt{\frac{\zeta \ln 2 \log n}{n}}\right)}}{n^\zeta} \leq \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^\zeta} \tag{5.75}$$

so that in (5.68)

$$P\left(\text{var}\left(T_n', Q'^{(n)}(\underline{\alpha})\right) \leq \gamma_n\right) \geq 1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}, \tag{5.76}$$

where the right-side above is nonnegative for $n \geq N_3(k')$. Upon gathering (5.61), (5.62), (5.67), (5.68) and (5.76), we get that for all $n \geq \max\{N_0(k'), N_1(k'), N_2(k'), N_3(k')\}$,

$$\begin{aligned}
&\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \pi_n\left(\rho, W^{V_1}, P_X, \widehat{P}_n\right) \\
&\geq \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_1' = \underline{\alpha}} \left[D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\hat{\gamma}_n}{c_n}\right] \left(1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}\right).
\end{aligned} \tag{5.77}$$

Step 3: It remains to reduce the right-side of (5.77) to (5.31), (5.32), (5.34). The main steps are outlined below and the details are given in Appendix D.3. First, for $\underline{\alpha} \in \Delta_{k'}$, a straightforward manipulation using (5.59) shows that $P_X(f^{-1})V_1' = \underline{\alpha}$ can be written as

$$l\rho P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1} f^{-1}(j)\right) + \left(1 - P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1} f^{-1}(j)\right) - P_X\left(\bigcup_{j=k'-l'}^{k'-1} f^{-1}(j)\right)\right) \times$$

$$l\left(\frac{1-l\rho}{k-l'-l}\right) = \underline{\alpha}(j'), \quad j' = 0, 1, \ldots, k'-l'-1, \tag{5.78}$$

$$\text{and} \quad P_X\left(f^{-1}(j')\right) = \underline{\alpha}(j'), \quad j' = k'-l', \ldots, k'-1. \tag{5.79}$$

Combining (5.78) and (5.79), we get

$$P_X\left(\bigcup_{j=j'l}^{j'(l+1)-1} f^{-1}(j)\right) = \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)\left(1 - \sum_{j=k'-l'}^{k'-1} \underline{\alpha}(j)\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)}, \quad j' = 0, 1, \ldots, k'-l'-1. \tag{5.80}$$

Then in (5.77), fixing $\widehat{P}_n \in \mathcal{S}_n(k')$ and $\underline{\alpha} \in \Delta_{k'}$,

$$\sup_{P_X : P_X(f^{-1})V_1' = \underline{\alpha}} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) = \sup_{P_X : P_X \sim \text{ (5.79), (5.80)}} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \quad (5.81)$$

where $P_X \sim$ (5.79), (5.80) connotes P_X consistent with (5.79) and (5.80). 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:

$$f'^{-1}(j') = \begin{cases} \bigcup_{j=j'l}^{j'(l+1)-1} f^{-1}(j), & j' = 0, 1, \ldots, k' - l' - 1 \\ f^{-1}(k - k' + j'), & j' = k' - l', \ldots, k' - 1 \end{cases} \quad (5.82)$$

and define a k'-sparse pmf P_X^{sp} on $\mathcal{X}$ as in Definition 5.4 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 (5.81) 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 (5.77) with $\underline{\alpha}(j') = 0,\ j' = k' - l', \ldots, k' - 1$. Then a straightforward substitution in (5.77) using (5.81) and (5.82) yields that

$$\begin{aligned} &\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X \sim (5.79),\ (5.80)} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \\ &\qquad \geq \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j') = 0,\ j' = k' - l', \ldots, k' - 1}} \\ &\sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{1}{\min\limits_{x \in f'^{-1}(j')} \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right), \end{aligned} \quad (5.83)$$

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

Step 4: In (5.83), observe that for every $\widehat{P}_n : \mathcal{Q}'^{(n)} \to \mathcal{X}$, there exists a locally uniform estimator (see Definition 5.2, with k' replacing k and f'^{-1} replacing f^{-1}), depending on $\widehat{P}_n$, and specified by

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

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

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

and with the obvious property that

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

Hence, $\inf\limits_{\widehat{P}_n}$ in the right-side of (5.83) can be restricted to $\inf\limits_{\widehat{P}_n^{\beta^{(n)}}}$, and becomes

$$\begin{aligned} &\inf_{\widehat{P}_n^{\beta^{(n)}} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0, \; j'=k'-l', \ldots, k'-1}} \\ &\sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \log \left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{|f'^{-1}(j')|}{\widehat{P}_n^{\beta^{(n)}} \left(Q'^{(n)}(\underline{\alpha}) \right) \left(f'^{-1}(j') \right)} \right). \end{aligned} \tag{5.84}$$

Finally, a further lower bound for (5.84) in Appendix D.3, taken together with (5.77), yields

$$\pi_n(\rho) \geq \left(\log |f'^{-1}(0)| + \Lambda_n(\rho) \right) \lambda_n(\rho) \tag{5.85}$$

where

$$\Lambda_n(\rho) \triangleq \begin{cases} \log\left(1+\frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{e\left|f'^{-1}(0)\right|}\frac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\, l\rho\right\}-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}\right)-\frac{\hat{\gamma}_n}{c_n}, & \sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')| \le |f'^{-1}(0)| \\ \log\left(\frac{\sum_{j'=1}^{k'-l'-1}\left|f'^{-1}(j')\right|}{\left|f'^{-1}(0)\right|}\right)\frac{\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\, l\rho\right\}-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}-\frac{\hat{\gamma}_n}{c_n}, & \sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')| > |f'^{-1}(0)| \end{cases} \tag{5.86}$$

and

$$\lambda_n(\rho) \triangleq 1-\frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}. \tag{5.87}$$

From (5.82), the passage following it, and (5.83), we have that the user-selected P_X is a k'-sparse pmf with associated mapping f' described by (5.82). Additional details of the specific k'-sparse pmf chosen by the user are provided in Appendix D.3.

Thus, for the case $l \le \left\lfloor \frac{k}{2} \right\rfloor$, (5.31) with (5.32), (5.34) follow from (5.85), (5.86), (5.87) upon recalling (5.55), (5.58) and (5.82).

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

Step 1: The user selects an add-noise ρ-QR $V_2 = V_2(\rho) : \mathcal{Z} \to \mathcal{Z}$ under the assumption that the rows of V_2 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

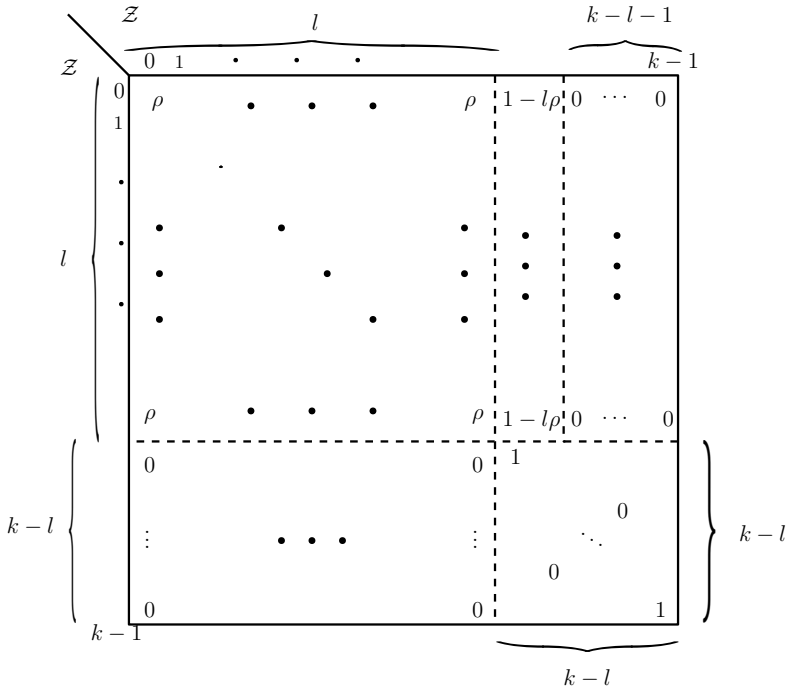


Figure 5.3: $V_2 : \mathcal{Z} \to \mathcal{Z}$

in (5.55), (5.57) and (5.58), respectively. Note that

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

Hence, $l' = k - l \geq 1$ and $k' = 1 + k - l$. As illustrated in Fig. 5.3, $V_2 : \mathcal{Z} \to \mathcal{Z}$ 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 $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ (see passage following (5.56)), 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 $0 \leq j \leq k-1$ and $0 \leq j' \leq k'-1$,

$$V_2'(j'|j) = \begin{cases} l\rho, & j' = 0, \quad j = 0, 1, \ldots, l-1 \\ 1 - l\rho, & j' = 1, \quad j = 0, 1, \ldots, l-1 \\ 1, & (j' = 1, j = l), \ldots, (j' = k'-1, j = k-1) \\ 0, & \text{otherwise.} \end{cases} \tag{5.88}$$

Using identical arguments as in the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ with V_1 and V_1' replaced by V_2 and V_2', respectively, the claim (5.60) holds and we get

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

Following the same steps from (5.61) - (5.77), we get that for all

$n \geq \max\{N_0(k'), N_1(k'), N_2(k'), N_3(k')\}$

$$\inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{P_X} \pi_n \left(\rho, W^{V_2}, P_X, \widehat{P}_n\right)$$
$$\geq \inf_{\widehat{P}_n \in \mathcal{S}_n(k')} \sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} \left[D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) - \frac{\hat{\gamma}_n}{c_n}\right] \left(1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}\right), \tag{5.89}$$

where $N_0(k'), N_1(k'), N_2(k'), N_3(k')$ are described in (5.65), (5.73) - (5.77).

Step 3: In the right-side of (5.89),

$$\sup_{\underline{\alpha} \in \Delta_{k'}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)$$
$$\geq \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right). \tag{5.90}$$

If $\underline{\alpha} \in \Delta_{k'}$ is such that[4] $\underline{\alpha}(j') = 0,\ j' = 2, \ldots, k'-1$, then $P_X(f^{-1})V_2' = \underline{\alpha}$, using (5.88), gives

$$P_X\left(f'^{-1}(0)\right) = \frac{\underline{\alpha}(0)}{l\rho} \tag{5.91}$$
$$P_X\left(f'^{-1}(1)\right) = \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \tag{5.92}$$
$$P_X\left(f'^{-1}(j')\right) = 0, \quad j' = 2, \ldots, k'-1, \tag{5.93}$$

where $f'^{-1} : \mathcal{Z}' \to \mathcal{X}$ is defined in (5.82). Then in the right-side of (5.90),

$$\sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \sup_{P_X : P_X(f^{-1})V_2' = \underline{\alpha}} D\left(P_X || \widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)$$

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

$$= \sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \sup_{P_X: P_X\sim \text{(5.91), (5.92), (5.93)}} D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right). \quad (5.94)$$

The right-side of (5.94) 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

$$\sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \sup_{P_X: P_X\sim \text{(5.91), (5.92), (5.93)}} D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right)$$

$$\geq \sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho}\log\left(\frac{\underline{\alpha}(0)}{l\rho}\frac{1}{\min\limits_{x\in f'^{-1}(0)}\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right)$$

$$+\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\log\left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\frac{1}{\min\limits_{x\in f'^{-1}(1)}\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right). \quad (5.95)$$

Using (5.95) in (5.89), we obtain

$$\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\underline{\alpha}\in\Delta_{k'}}\sup_{P_X: P_X(f^{-1})V_2'=\underline{\alpha}} D\left(P_X||\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)\right) \geq$$

$$\inf_{\widehat{P}_n\in\mathcal{S}_n(k')}\sup_{\substack{\underline{\alpha}\in\Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho}\log\left(\frac{\underline{\alpha}(0)}{l\rho}\frac{1}{\min\limits_{x\in f'^{-1}(0)}\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right)$$

$$+\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\log\left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho}\frac{1}{\min\limits_{x\in f'^{-1}(1)}\widehat{P}_n\left(Q'^{(n)}(\underline{\alpha})\right)(x)}\right).$$

Step 4: Using the same reasoning as in the case $l \leq \left\lfloor \frac{k}{2} \right\rfloor$, we can restrict $\inf\limits_{\widehat{P}_n\in\mathcal{S}_n(k')}$ above to locally

uniform estimators $\inf_{\widehat{P}_n^{\beta(n)} \in \mathcal{S}_n(k')}$ (see Definition 5.2) so that

$$\inf_{\widehat{P}_n^{\beta(n)} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \log \left(\frac{\underline{\alpha}(0)}{l\rho} \frac{|f'^{-1}(0)|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(0)\right)} \right) + \frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho} \log \left(\frac{\underline{\alpha}(1)-(1-l\rho)}{l\rho} \frac{|f'^{-1}(1)|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(1)\right)} \right). \quad (5.96)$$

A further lower bound for (5.96) in Appendix D.3, taken together with (5.89), yields (5.85) where

$$\Lambda_n(\rho) \triangleq \log \left(1 + \frac{|f'^{-1}(1)|}{e|f'^{-1}(0)|} \frac{\frac{\lceil n(1-l\rho) \rceil}{n} - (1-l\rho)}{l\rho} \right) - \frac{\hat{\gamma}_n}{c_n} \quad (5.97)$$

and

$$\lambda_n(\rho) \triangleq 1 - \frac{3e^{\left(\frac{4(k'-1)\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}}. \quad (5.98)$$

From (5.96), we have that the user-selected P_X is a k'-sparse pmf with associated mapping f' described by (5.82). Additional details of the specific k'-sparse pmf chosen by the user are provided in Appendix D.3.

Hence, when $l > \left\lfloor \frac{k}{2} \right\rfloor$, we get (5.31) along with (5.33), (5.34) from (5.85), (5.97), (5.98) upon recalling (5.55), (5.58) and (5.82).

Finally, in both cases $l \leq \left\lfloor \frac{k}{2} \right\rfloor$ and $l > \left\lfloor \frac{k}{2} \right\rfloor$, (5.35) follows afrom (5.32) - (5.34) and (5.24); in particular, in the former case, observe in (5.32) that

$$l \left(\frac{1-l\rho}{\left\lfloor \frac{k}{l} \right\rfloor l - l} \right) = l \left(\frac{1-l\rho}{k-l'-l} \right), \quad \text{by (5.55)}$$

$$\leq l\rho, \quad \text{by (D.18) (in Appendix D.3).}$$

Also, (5.36) is immediate from (5.31) and (5.35). ■

5.6. Special Case: Binary-Valued Function

In this section, we provide in Theorem 5.9 below a characterization of distribution ρ-privacy for the special case of a binary-valued mapping $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$. The lower bound on $\pi_n(\rho),\ 0 \leq \rho \leq 1$, is obtained by utilizing Theorem 5.5. Furthermore, we recall from Remark (ii) following Theorem 5.4 that an explicit upper bound for $\Gamma_n(\rho),\ 0 \leq \rho \leq 1$ – for a general f – is not available. However, for the special case of a binary-valued mapping $f : \mathcal{X} \to \mathcal{Z}$, we obtain a closed-form expression for an upper bound for $\Gamma_n(\rho)$, and therefore, $\pi_n(\rho)$.

Theorem 5.9. *For $f : \mathcal{X} \to \mathcal{Z} = \{0, 1\}$ and for $0.5 < \rho \leq 1$, the following hold.*

(i) For the class of smooth estimators for the querier,

$$\sup_{W} \inf_{\widehat{P}_n \in \mathcal{S}_n} \sup_{P_X} \pi_n \left(\rho, W, P_X, \widehat{P}_n \right) \geq \left(\max_{j \in \{0,1\}} \log |f^{-1}(j)| + \Lambda_n(\rho) \right) \lambda_n(\rho), \tag{5.99}$$

for all n large enough, where

$$\Lambda_n(\rho) \triangleq \log \left(1 + \frac{r - \max\limits_{j \in \{0,1\}} |f^{-1}(j)|}{e \max\limits_{j \in \{0,1\}} |f^{-1}(j)|} \frac{\min \left\{ \frac{\lceil n(1-\rho) \rceil}{n},\ \rho \right\} - (1 - \rho)}{2\rho - 1} \right) - \frac{\hat{\gamma}_n}{c_n} \tag{5.100}$$

and

$$\lambda_n(\rho) \triangleq 1 - \frac{3e^{\left(\frac{4\sqrt{\zeta}}{5\sqrt{e}}\right)}}{n^{\zeta}} \quad \textit{with } \zeta > 1. \tag{5.101}$$

(ii) For every $n \geq 1$,

$$\pi_n(\rho) \leq \max_{j \in \{0,1\}} \log \left| f^{-1}(j) \right| + \Gamma_n(\rho), \tag{5.102}$$

where $\Gamma_n(\rho) = O\left(\frac{\log n}{\sqrt{n}}\right)$ *with*

$$\Gamma_n(\rho) \leq 2\max\left\{\frac{\log(n+2)}{(2\rho-1)n}, \frac{\ln n+1}{2\ln 2(2\rho-1)\sqrt{n}} + \frac{\log n}{2(2\rho-1)\sqrt{n}} + \log\frac{n+2}{n}\right\}$$
$$+ \exp\left[\frac{\sqrt{n+1}}{n} - \frac{n+2}{2n}\right]\frac{2\sqrt{2}\log(n+2)}{(2\rho-1)\sqrt{n}} + 2\log\frac{n+2}{n+1}, \quad \frac{1}{2} \leq \rho \leq 1. \quad (5.103)$$

Proof:

(i) We obtain (5.99), (5.100), (5.101) from a straightforward application of Theorem 5.5.

(ii) See Appendix D.5. ■

5.7. Discussion and Open Problems

A minimum level of distribution ρ-privacy equal to worst-case privacy $\omega(\rho)$, $0 \leq \rho \leq 1$, is guaranteed by Theorem 5.3 since $\pi_n(\rho) \geq \omega(\rho)$ for every $n \geq 1$, with $\omega(\rho)$ being achievable. Under Assumption (5.13), $\omega(\rho) = \log \sum_{j=0}^{l-1} |f^{-1}(j)|$, where l is determined by ρ (see (5.12)). For low recoverability, i.e., $\rho \leq 1/k$, the user can pick a ρ-QR $W : \mathcal{X} \to \mathcal{Z}$ 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 (5.11)) from Z^n as $n \to \infty$. Then, for $\rho > 0.5$, distribution ρ-privacy informally equals $\inf_{g:\Delta_k \to \Delta_r} \sup_{P_X \in \Delta_r} D\left(P_X || g\left(P_X\left(f^{-1}\right)\right)\right)$, where g is an "estimator" of

P_X on the basis of $P_X\left(f^{-1}\right)$. It is shown in Appendix D.4 that

$$\inf_{g:\Delta_k\to\Delta_r}\ \sup_{P_X\in\Delta_r} D\left(P_X||g\left(P_X\left(f^{-1}\right)\right)\right) = \max_{j\in\mathcal{Z}} \log|f^{-1}(j)| \tag{5.104}$$

thereby explaining the value of $\omega(\rho)$ for $\rho > 0.5$ in (5.12) with $l = 1$. Intermediate increasing values of ρ in $(1/k, 0.5]$ give $\omega(\rho) = \log\sum_{j=0}^{l-1}|f^{-1}(j)|$ with l decreasing from $k-1$ to 2 in (5.12), (5.14).

Theorem 5.5 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 an add-noise 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 5.5.

The preceding observations show why distribution ρ-privacy defined in terms of divergence in (5.2) leads to useful insights in Theorems 5.3 and 5.5, complemented by the converse Theorem 5.4 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 5.5) On a

related note, Theorems 5.3 and 5.4 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 5.5, our approach resorts to a smooth estimator for the querier (see Definition 5.3), especially its properties in (5.24)) in order to evade a divergence-borne fly in the ointment in (5.61)-(5.66). However, this raises the question of whether the converse Theorem 5.4, if restricted to such smooth querier's estimators, could lead to an increased upper bound than in (5.28), (5.29). This, too, remains unanswered. Furthermore, the additional restriction placed on large n in Theorem 5.5, as mentioned in Remark (iii) after the theorem statement, is a weakness. We conjecture that the add-noise ρ-QRs $V_1 : \mathcal{Z} \to \mathcal{Z}$ and $V_2 : \mathcal{Z} \to \mathcal{Z}$ in the proof of Theorem 5.5 in Section 5.5.2 are adequate even without this restriction.

In Section 2.8.1, we proposed a framework for investigating data ρ-privacy in the context of differential privacy. Likewise, we conclude this section by suggesting a framework for examining distribution ρ-privacy in the context of differential privacy. From Section 2.8.1, recall the notions of differential privacy, local differential privacy (ϵ-LDP), and why we chose the latter over the former. The same considerations will hold in the case of distribution ρ-privacy as well. Also, recall that a ρ-QR that is ϵ-LDP cannot violate (2.99). What is a characterization of distribution ρ-privacy under the additional requirement that the ρ-QRs have to conform to the ϵ-LDP (2.98) constraint? The problems posed in Section 2.8.1, now in the distribution ρ-privacy setting, are pertinent. Additionally, what will be the corresponding worst-case distribution ρ-privacy under ϵ-LDP restriction? This line of inquiry remains open.

Chapter 6: Closing Remarks

We close by highlighting key features of our approach and results.

All our models for studying data and distribution privacy are structured in a way that is biased intentionally against the user and in favor of the querier – so as to make for a conservative extent of privacy. Precisely, we assume throughout that the querier is aware of the privacy mechanism, i.e., specific ρ-QR used by the user. Additionally, in Sections 2.4 and 5.2, where multiple query responses are elicited from the user, we impose the strict requirement that each of the query responses satisfies the ρ-recoverability constraint rather than a fraction of them. This requirement, too, works against the user.

An advantageous characteristic of all our achievability schemes is that they are of the add-noise type. This involves the user devising the query response by adding to the true function value a noise whose distribution can depend on said value. This makes all our proposed randomization algorithms eminently implementable. Another desirable attribute of our results is, that our (asymptotically) optimal ρ-QRs are "universal" in the sense of not depending on the user's data distribution.

Finally, we close by mentioning how our framework tackles the issues concerning differential privacy raised in Section 1.2. In our data privacy setting in Chapter 2, the user data X can constitute a data vector consisting of multiple users' data. Since privacy is ensured for the entire

data vector, this prevents singling out. Also, the predicate privacy formulation in Section 2.5 addresses the requirement that any PII of the user should not be determined from the QR. This can be done by suitably tuning the predicate mapping to the specific PII that needs to be protected. In all of our privacy mechanisms, the sensitivity of the function does not play a role. Therefore, the problem of the impracticality of determining the sensitivity of a function does not arise.

Appendix A:

A.1. Proof of Lemma 2.6

(i) For each $0 \leq \rho \leq 1$,

$$P\left(\text{Bin}(n,\rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right) = \sum_{t=0}^{\left\lfloor \frac{n}{2} \right\rfloor} P\left(T_{\text{Ber}\left(\frac{t}{n}\right)}\right)$$

where $T_{\text{Ber}\left(\frac{t}{n}\right)}$ denotes the set of all n-length binary sequences of "type" $\text{Ber}\left(\frac{t}{n}\right)$, i.e., with t 1s (and $(n-t)$ 0s), so that

$$\max_{0 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor} P\left(T_{\text{Ber}\left(\frac{t}{n}\right)}\right) \leq P\left(\text{Bin}(n,\rho) \leq \left\lfloor \frac{n}{2} \right\rfloor\right) \leq \left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) \max_{0 \leq t \leq \left\lfloor \frac{n}{2} \right\rfloor} P\left(T_{\text{Ber}\left(\frac{t}{n}\right)}\right). \tag{A.1}$$

Using well-known bounds for the probability of all n-length sequences of a given type (cf. [20, Lemma 2.6]), for each $0 \leq \rho \leq 1$, and noting that the number of types for binary sequences of length n equals $n+1$,

$$\frac{1}{n+1} \exp\left[-nD\left(\text{Ber}\left(\frac{t}{n}\right) \middle|\middle| \text{Ber}\left(\rho\right)\right)\right] \leq P\left(T_{\text{Ber}\left(\frac{t}{n}\right)}\right) \leq \exp\left[-nD\left(\text{Ber}\left(\frac{t}{n}\right) \middle|\middle| \text{Ber}\left(\rho\right)\right)\right] \tag{A.2}$$

and noting that for $0.5 \le \rho \le 1$,

$$\min_{0 \le t \le \lfloor \frac{n}{2} \rfloor} D\left(\text{Ber}\left(\frac{t}{n}\right) \middle|\middle| \text{Ber}\left(\rho\right)\right) = D\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}\left(\rho\right)\right) \tag{A.3}$$

we have, by (A.2) and (A.3), from (A.1) that

$$\begin{aligned}\frac{1}{n+1} \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}\left(\rho\right)\right)\right] &\le P\left(\text{Bin}(n,\rho) \le \left\lfloor \frac{n}{2} \right\rfloor\right) \\ &\le \left(\left\lfloor \frac{n}{2} \right\rfloor + 1\right) \exp\left[-nD\left(\text{Ber}\left(\frac{1}{n}\left\lfloor \frac{n}{2} \right\rfloor\right) \middle|\middle| \text{Ber}\left(\rho\right)\right)\right].\end{aligned}$$

(ii) We have that

$$\begin{aligned}P\left(\text{Bin}(n,\rho) \ge \left\lfloor \frac{n}{2} \right\rfloor + 1\right) &= \sum_{t=\lfloor \frac{n}{2} \rfloor + 1}^{n} \binom{n}{t} \rho^t (1-\rho)^{n-t} \\ &= (1-\rho)^n \sum_{t=\lfloor \frac{n}{2} \rfloor + 1}^{n} \binom{n}{t} \left(\frac{\rho}{1-\rho}\right)^t \\ &\le (1-\rho)^n \left(\frac{\rho}{1-\rho}\right)^{\lfloor \frac{n}{2} \rfloor + 1} \sum_{t=\lfloor \frac{n}{2} \rfloor + 1}^{n} \binom{n}{t}, \text{ since } 0 \le \rho \le 0.5 \\ &\le (1-\rho)^n \left(\frac{\rho}{1-\rho}\right)^{\lfloor \frac{n}{2} \rfloor + 1} 2^{n-1} \\ &\le (1-\rho)^n \left(\frac{\rho}{1-\rho}\right)^{\frac{n-1}{2}+1} 2^{n-1} \\ &= \rho \left(2\sqrt{\rho(1-\rho)}\right)^{n-1} \\ &\le \rho, \quad \text{since } 2\sqrt{\rho(1-\rho)} \le 1 \text{ for } 0 \le \rho \le 1.\end{aligned}$$

The assertion follows. ■

A.2. Proof of (2.30)

Since ρ and $\max\limits_{i\in\mathcal{Z}} P\left(f(X)=i\right)$ are obvious lower bounds for the left-side of (2.30), it suffices to show that

$$P(h_{\text{MAP}}\left(F_1(X),\ldots,F_n(X)\right)=f(X)) \geq P\left(\text{Bin}(n,\rho)\geq\left\lfloor\frac{n}{2}\right\rfloor+1\right). \tag{A.4}$$

The proof bears a resemblance to that of Theorem 2.3 above and so we shall refer to pertinent details therein. We have

$$\begin{aligned}
&P(h_{\text{MAP}}\left(F_1(X),\ldots,F_n(X)\right)=f(X)) \\
&\quad=\sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n}\max_{j\in\mathcal{Z}} P\left(f(X)=j\right)P\left(F_1(X)=i_1,\ldots,F_n(X)=i_n|f(X)=j\right).
\end{aligned} \tag{A.5}$$

Since

$$\begin{aligned}
&P\left(F_1(X)=i_1,\ldots,F_n(X)=i_n|f(X)=j\right) \\
&\quad=\sum_{x\in\mathcal{X}} P\left(F_1(X)=i_1,\ldots,F_n(X)=i_n|f(X)=j,X=x\right)P\left(X=x|f(X)=j\right) \\
&\quad=\sum_{x\in f^{-1}(j)}\prod_{t=1}^{n} W_t\left(i_t|x\right)\frac{P_X(x)}{P\left(f(X)=j\right)},
\end{aligned}$$

we get in (A.5) with $\mathcal{A}_l(i)$ in (2.62) that

$$P(h_{\text{MAP}}\left(F_1(X),\ldots,F_n(X)\right)=f(X))$$

$$
\begin{aligned}
&= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} \left(\sum_{x\in f^{-1}(j)} P_X(x) \prod_{t=1}^{n} W_t\left(i_t|x\right) \right) \\
&\geq \sum_{i\in\mathcal{Z}} \sum_{l=\left\lfloor \frac{n}{2} \right\rfloor+1}^{n} \sum_{(i_1,\ldots,i_n)\in\mathcal{A}_l(i)} \max_{j\in\mathcal{Z}} \left(\sum_{x\in f^{-1}(j)} P_X(x) \prod_{t=1}^{n} W_t\left(i_t|x\right) \right) \\
&\geq \sum_{i\in\mathcal{Z}} \sum_{x\in f^{-1}(i)} P_X(x) \left(\sum_{l=\left\lfloor \frac{n}{2} \right\rfloor+1}^{n} \sum_{(i_1,\ldots,i_n)\in\mathcal{A}_l(i)} \prod_{t=1}^{n} W_t\left(i_t|x\right) \right).
\end{aligned}
$$

Mimicking (2.63)-(2.66), observe that the sum above within $(\cdot)$ is bounded below by $P\left(\text{Bin}(n,\rho) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1\right)$. Clearly, (A.4) follows. ■

A.3. Proof of Theorem 2.8

Starting with the converse part, we have that

$$
P(g'_{MAP(W)}\left(Z\right) = Y) \geq P_X\left(h^{-1}(j^*)\right)
$$

and for every ρ-QR $W : \mathcal{X} \to \mathcal{Z}$ in (2.2),

$$
P(g'_{MAP(W)}\left(Z\right) = Y) = \sum_{i\in\mathcal{Z}} \max_{j\in\mathcal{Y}} \sum_{x\in h^{-1}(j)} P_X(x)W(i|x) \geq \rho \sum_{i\in\mathcal{Z}} \max_{j\in\mathcal{Y}} P_X(i,j) = \rho \sum_{i\in\mathcal{Z}} P_X(i,j_i^*)
$$

where the first equality uses

$$
P\left(Y = j|X = x, Z = i\right) = \mathbb{1}\left(j = h(x)\right).
$$

The converse proof is completed similarly as for Theorem 2.2.

Turning to the achievability part, since $\rho_c' < 1$, observe in (2.54) that

$$\sum_{l\in\mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right) \geq \sum_{l\in\mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j^*)\right) > 0.$$

We have that $1 - \pi_\rho'\left(W_o'\right)$ equals

$$\begin{aligned} P(g'_{MAP(W_o')}(Z) = Y) &= \sum_{i\in\mathcal{Z}} \max_{j\in\mathcal{Y}} P\left(Z = i, Y = j\right) \\ &= \sum_{i\in\mathcal{Z}} \max_{j\in\mathcal{Y}} \sum_{x\in h^{-1}(j)} P_X(x) W_o'(i|x). \end{aligned} \tag{A.6}$$

When $\rho_c' = 1$, we get in (A.6), upon using (2.53), that

$$P(g'_{MAP(W_o')}(Z) = Y) = \sum_{i\in\mathcal{Z}} \max_{j\in\mathcal{Y}} \sum_{x\in h^{-1}(j)\cap f^{-1}(i)} P_X(x) = \sum_{i\in\mathcal{Z}} P_X\left(i, j_i^*\right). \tag{A.7}$$

When $\rho_c' < 1$, for each $i \in \mathcal{Z}$ the summand in (A.6), upon using (2.54), is

$$\begin{aligned} &\max_{j\in\mathcal{Y}} \left[\sum_{x\in h^{-1}(j)\cap f^{-1}(i)} P_X(x) W_o'(i|x) + \sum_{x\in h^{-1}(j)\setminus f^{-1}(i)} P_X(x) W_o'(i|x) \right] \\ &= \max_{j\in\mathcal{Y}} \left[\sum_{x\in h^{-1}(j)\cap f^{-1}(i)} P_X(x) \left\{ \max\{\rho_c', \rho\} + (1 - \max\{\rho_c', \rho\}) \frac{P_X\left(i, j_i^*\right) - P_X(i, j)}{\sum_{l\in\mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)} \right\} \right. \\ &\left. + \sum_{x\in h^{-1}(j)\setminus f^{-1}(i)} P_X(x) \left\{ (1 - \max\{\rho_c', \rho\}) \frac{P_X\left(i, j_i^*\right) - P_X(i, j)}{\sum_{l\in\mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)} \right\} \right] \\ &= \max_{j\in\mathcal{Y}} \left[\max\{\rho_c', \rho\} P_X(i, j) + (1 - \max\{\rho_c', \rho\}) \frac{P_X\left(i, j_i^*\right) - P_X(i, j)}{\sum_{l\in\mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)} P_X\left(h^{-1}(j)\right) \right]. \end{aligned} \tag{A.8}$$

It suffices to show that the right-side of (A.8) is bounded above by $\max\{\rho_c', \rho\} P_X\left(i, j_i^*\right)$ for each $i \in \mathcal{Z}$; this is done below. Then, in fact, the right-side of (A.8) equals $\max\{\rho_c', \rho\} P_X\left(i, j_i^*\right)$ as seen by setting $j = j_i^*$ in the term within $[\cdots]$.

First consider the case when $\max\{\rho_c', \rho\} < 1$. It is seen from (2.52) that for each $j \in \mathcal{Y}$,

$$\frac{\max\{\rho_c', \rho\}}{1 - \max\{\rho_c', \rho\}} \geq \frac{\rho_c'}{1 - \rho_c'} = \frac{P_X\left(h^{-1}(j^*)\right)}{\sum\limits_{l \in \mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j^*)\right)} \geq \frac{P_X\left(h^{-1}(j)\right)}{\sum\limits_{l \in \mathcal{Z}} P_X\left(l, j_l^*\right) - P_X\left(h^{-1}(j)\right)}. \tag{A.9}$$

Using (A.9) in (A.8), and since $P_X\left(h^{-1}(j)\right) > 0$, $j \in \mathcal{Y}$, we get that the right-side of (A.8) is bounded above by $\max\{\rho_c', \rho\} P_X\left(i, j_i^*\right)$. Also, this is true trivially when $\max\{\rho_c', \rho\} = 1$. Hence, we get that for each $i \in \mathcal{Z}$, the right-side of (A.8) equals $\max\{\rho_c', \rho\} P_X\left(i, j_i^*\right)$. This, combined with (A.6)-(A.8), yields

$$\pi_\rho'\left(W_o'\right) = 1 - \max\{\rho_c', \rho\} \sum_{i \in \mathcal{Z}} P_X\left(i, j_i^*\right).$$

This completes the proof of the theorem. ■

A.4. Proof of Proposition 2.11(i)

The following two lemmas are pertinent. Recall from (2.14) that $x^* = \arg \max\limits_{x \in \mathcal{X}} P_X(x)$ is in $f^{-1}\left(i^*\right)$ for some (fixed) $i^* \in \mathcal{Z}$.

Lemma A.4.1. *For $V_o : \mathcal{Z} \to \mathcal{Z}$ in (2.17),*

(i) when $\rho_c < \rho \leq 1$, no two rows can be identical;

(ii) when $0 \leq \rho \leq \rho_c$, if the rows $V_o(\cdot|j)$ and $V_o(\cdot|j')$, $j \neq j'$, are identical, then each coincides

with the row $V_o(\cdot|i^*)$*, in which case* $P_X(x_j^*) = P_X(x_{j'}^*) = P_X(x^*)$*. Furthermore, the number of identical rows of* V_o *cannot exceed* $\left\lfloor \frac{1}{\rho_c} \right\rfloor$.

Proof: With $0 \leq \rho \leq 1$, if the rows of $V_o : \mathcal{Z} \to \mathcal{Z}$ corresponding to $j \neq j'$ in $\mathcal{Z}$ are identical, then

$$V(i|j) = V(i|j'), \quad i \in \mathcal{Z} \setminus \{j, j'\}$$

i.e.,

$$(1 - \max\{\rho_c, \rho\}) \frac{P_X(x_i^*)}{\sum_{l \neq j} P_X(x_l^*)} = (1 - \max\{\rho_c, \rho\}) \frac{P_X(x_i^*)}{\sum_{l' \neq j'} P_X(x_{l'}^*)}, \quad i \in \mathcal{Z} \setminus \{j, j'\}$$

whence

$$P_X\left(x_j^*\right) = P_X\left(x_{j'}^*\right); \tag{A.10}$$

and furthermore

$$V(i|j) = V(i|j'), \quad i \in \{j, j'\}$$

which, using (A.10), gives straightforwardly that

$$\max\{\rho_c, \rho\} = \frac{P_X(x_i^*)}{\sum_{l \in \mathcal{Z}} P_X(x_l^*)}, \quad i \in \{j, j'\}. \tag{A.11}$$

(i) When $\rho > \rho_c$, recalling (2.15)

$$\frac{P_X(x_i^*)}{\sum_{l \in \mathcal{Z}} P_X(x_l^*)} \leq \frac{P_X(x^*)}{\sum_{l \in \mathcal{Z}} P_X(x_l^*)} = \rho_c < \max\{\rho_c, \rho\}$$

which violates (A.11) for $i \in \{j, j'\}$, so that no two rows of $V_o : \mathcal{Z} \to \mathcal{Z}$ can be identical.

(ii) When $0 \leq \rho \leq \rho_c$, suppose that the rows $V_o(\cdot|j)$ and $V_o(\cdot|j')$ are identical for some $j \neq j'$. Then (A.11) holds which, upon recalling (2.15), is tantamount to

$$P_X(x_j^*) = P_X(x_{j'}^*) = P_X(x^*) = P_X(x_{i^*}^*). \tag{A.12}$$

To show for $j \neq i^*$ that $V_o(i|j) = V_o(i|i^*)$, $i \in \mathcal{Z}$, consider first $i \in \{j, i^*\}$. Then, using (A.12),

$$V_o(j|j) = \rho_c, \quad V_o(i^*|j) = (1-\rho_c)\frac{P_X(x_{i^*}^*)}{\sum\limits_{l\neq j} P_X(x_l^*)} = (1-\rho_c)\frac{P_X(x^*)}{\sum\limits_{l\in\mathcal{Z}} P_X(x_l^*) - P_X(x_j^*)} = \rho_c,$$

and similarly,

$$V_o(j|i^*) = (1-\rho_c)\frac{P_X(x_j^*)}{\sum\limits_{l\in\mathcal{Z}} P_X(x_l^*) - P_X(x_{i^*}^*)} = \rho_c, \quad V_o(i^*|i^*) = \rho_c.$$

And for $i \in \mathcal{Z} \setminus \{j, i^*\}$,

$$V_o(i|j) = (1-\rho_c)\frac{P_X(x_i^*)}{\sum\limits_{l\in\mathcal{Z}} P_X(x_l^*) - P_X(x_j^*)} = \frac{P_X(x_i^*)}{\sum\limits_{l\in\mathcal{Z}} P_X(x_l^*)} = V_o(i|i^*).$$

Lastly, if the number of identical rows of $V_o : \mathcal{Z} \to \mathcal{Z}$ is α, then $\alpha P_X(x^*) \leq \sum\limits_{l\in\mathcal{Z}} P_X(x_l^*)$, whence $\alpha \leq \left\lfloor \frac{1}{\rho_c} \right\rfloor$.

■

For $S \subseteq \mathcal{Z}$, let

$$j_S = \arg \max_{l \in S} P_X(x_l^*), \quad R_S = (\mathcal{Z} \setminus S) \cup \{j_S\}, \tag{A.13}$$

where j_S and R_S need not be unique. Let $\tilde{f}_{R_S}(X)$ be a R_S-valued rv with pmf

$$P\left(\tilde{f}_{R_S}(X) = i\right) = \frac{P_X(x_i^*)}{\sum_{l \in R_S} P_X(x_l^*)}, \quad i \in R_S. \tag{A.14}$$

Consider the stochastic matrix $V_{R_S} : R_S \to \mathcal{Z}$ given by

$$V_{R_S} = \{V(i|j), i \in \mathcal{Z}, j \in R_S\} \tag{A.15}$$

and let $\left\{\tilde{Z}_t^{R_S}\right\}_{t=1}^n$ be conditionally mutually independent $\mathcal{Z}$-valued rvs conditioned on $\tilde{f}_{R_S}(X)$, with

$$P_{\tilde{Z}_t^{R_S}|\tilde{f}_{R_S}(X)} = V_{R_S}, \quad t = 1, \ldots, n. \tag{A.16}$$

Let $C(V_{R_S})$ be the Chernoff radius restricted to R_S, i.e., with the minimum in (2.79) being instead over all $j \neq j'$ in R_S.

Lemma A.4.2. *For $0 \leq \rho \leq 1$, consider add-noise ρ-QRs $\{F_t(X)\}_{t=1}^n$ with (2.29) holding for every $n \geq 1$, where $V_t = V$, $t \geq 1$. If $V : \mathcal{Z} \to \mathcal{Z}$ has identical rows $\{V(\cdot|j), j \in S\}$, then*

$$\pi_\rho(V^n) - \left(1 - \sum_{i \in R_S} P_X(x_i^*)\right) \doteq \exp\left[-nC(V_{R_S})\right]$$

for R_S and V_{R_S} in (A.13) and (A.15), respectively.

Remark: If the rows of $V_{R_S} : R_S \to \mathcal{Z}$ are distinct in Lemma A.4.2, then $C\left(V_{R_S}\right) > 0$. If the rows of $V : \mathcal{Z} \to \mathcal{Z}$ are distinct, then $S = \phi$, $R_S = \mathcal{Z}$ and $V_{R_S} = V$.

Proof:

$$
\begin{aligned}
P\left(g_{\text{MAP}(V^n)}\left(Z_1, \ldots, Z_n\right) = X\right) &= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{x\in\mathcal{X}} \; P_X(x) \prod_{t=1}^{n} V\left(i_t | f(x)\right) \\
&= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{\substack{x\in\cup f^{-1}(j) \\ j\in\mathcal{Z}}} \; P_X(x) \prod_{t=1}^{n} V\left(i_t | f(x)\right) \\
&= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in\mathcal{Z}} \; P_X\left(x_j^*\right) \prod_{t=1}^{n} V\left(i_t | j\right) \\
&= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in(\mathcal{Z}\setminus S)\cup S} \; P_X\left(x_j^*\right) \prod_{t=1}^{n} V\left(i_t | j\right) \\
&= \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in R_S} \; P_X(x_j^*) \prod_{t=1}^{n} V\left(i_t | j\right) \qquad \text{(A.17)} \\
&= \left(\sum_{i\in R_S} P_X\left(x_i^*\right)\right) \sum_{(i_1,\ldots,i_n)\in\mathcal{Z}^n} \max_{j\in R_S} \frac{P_X(x_j^*)}{\sum\limits_{i\in R_S} P_X\left(x_i^*\right)} \prod_{t=1}^{n} V\left(i_t | j\right) \\
&= \left(\sum_{i\in R_S} P_X\left(x_i^*\right)\right) P\left(g_{\text{MAP}\left(V_{R_S}^n\right)}\left(\tilde{Z}_1^{R_S}, \ldots, \tilde{Z}_n^{R_S}\right) = \tilde{f}_{R_S}(X)\right)
\end{aligned}
$$

(A.18)

where (A.17) is by the identicality of the rows $\{V\left(\cdot|j\right),\ j \in S\}$, and $\tilde{f}_{R_S}(X)$ and $\{\tilde{Z}_t^{R_S}\}_{t=1}^n$ are as in (A.14) and (A.16), respectively. The assertion follows by applying [44, Theorem 2] to (A.18).

■

Turning to the proof of Proposition 2.11(i), first observe by Theorem 2.5 that for $0 \le \rho \le 0.5$ and *every* $n \ge 1$,

$$\pi_\rho\left(V_2^n\right) - \left(1 - \sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right)\right)$$
$$\geq \sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right) - \max\left\{P_X(x^*), \sum_{i=0}^{\left\lfloor \frac{k}{\lfloor \frac{1}{\rho}\rfloor}\right\rfloor - \mathbb{1}\left(k \bmod \lfloor \frac{1}{\rho}\rfloor = 0\right)} P_X\left(x^*_{i\lfloor \frac{1}{\rho}\rfloor}\right)\right\} > 0. \quad \text{(A.19)}$$

We consider two cases: $\rho > \rho_c$ and $0 \leq \rho \leq \rho_c$. When $\rho > \rho_c$, by Lemma A.4.1(i), all the rows of $V_o : \mathcal{Z} \to \mathcal{Z}$ are distinct so that $C(V_o) > 0$. Then, by (2.95),

$$\lim_n \ \pi_\rho\left(V_o^n\right) - \left(1 - \sum_{i\in\mathcal{Z}} P_X\left(x_i^*\right)\right) = 0$$

which upon comparison with (A.19), yields (2.91) in this case.

In the case $0 \leq \rho \leq \rho_c$, $V_o : \mathcal{Z} \to \mathcal{Z}$ can contain identical rows. By Lemma A.4.1(ii) and upon invoking assumption (2.35) without loss of generality, the identical rows must be those corresponding to $\{0, 1, \ldots, a-1\}$ (with the remaining rows being all distinct), where $a \leq \left\lfloor \frac{1}{\rho_c} \right\rfloor$ is the number of identical rows. By applying Lemma A.4.2, with $S = \{0, 1, \ldots, a-1\}$, $j_S = 0$ and observing that $C\left(\left(V_o\right)_{R_S}\right) > 0$, we get

$$\lim_n \ \pi_\rho\left(V_o^n\right) = 1 - \sum_{i\in R_S} P_X\left(x_i^*\right)$$
$$= \begin{cases} 1 - P_X\left(x^*\right), & a = k \Leftrightarrow \left\lfloor \frac{1}{\rho_c} \right\rfloor = k \\ 1 - \sum\limits_{i\in\{0,a,a+1,\ldots,k-1\}} P_X\left(x_i^*\right), & a < k \Leftrightarrow \left\lfloor \frac{1}{\rho_c} \right\rfloor < k \end{cases}$$

$$
\begin{aligned}
&\leq \begin{cases} 1 - P_X\left(x^*\right), & \left\lfloor \frac{1}{\rho_c} \right\rfloor = k \\ 1 - \sum\limits_{i \in \left\{0, \left\lfloor \frac{1}{\rho_c} \right\rfloor, \left\lfloor \frac{1}{\rho_c} \right\rfloor + 1, \ldots, k-1\right\}} P_X\left(x_i^*\right), & \left\lfloor \frac{1}{\rho_c} \right\rfloor < k \end{cases} \\
&\leq \begin{cases} 1 - P_X\left(x^*\right), & \rho_c = \frac{1}{k} \\ 1 - \sum\limits_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho_c} \right\rfloor} \right\rfloor} P_X\left(x^*_{i\left\lfloor \frac{1}{\rho_c} \right\rfloor}\right), & k \bmod \left\lfloor \frac{1}{\rho_c} \right\rfloor \neq 0, \quad \frac{1}{k} < \rho_c \leq 0.5 \\ 1 - \sum\limits_{i=0}^{\left\lfloor \frac{k}{\left\lfloor \frac{1}{\rho_c} \right\rfloor} \right\rfloor - 1} P_X\left(x^*_{i\left\lfloor \frac{1}{\rho_c} \right\rfloor}\right), & k \bmod \left\lfloor \frac{1}{\rho_c} \right\rfloor = 0, \quad \frac{1}{k} < \rho_c \leq 0.5 \end{cases} \\
&= \pi_{\rho_c}\left(V_2^n\right) \\
&\leq \pi_{\rho}\left(V_2^n\right), \quad 0 \leq \rho \leq \rho_c,
\end{aligned}
$$

which, upon recalling by Theorem 2.5 that $\pi_\rho\left(V_2^n\right)$ is the same for all n, establishes (2.91). ■

Appendix B: Proof of Lemma 3.2

Proof of Lemma 3.2:

(i) We need to show that

$$\Lambda_\rho \cap f^{-1}(i) = \left[f^{-1}(i)\right]_{|\Lambda_\rho \cap f^{-1}(i)|}, \; i \in \mathcal{Z}. \tag{B.1}$$

Writing the term within $[\cdot]$ in (3.3) with $\Lambda = \Lambda_\rho$ as

$$\sum_{i\in\mathcal{Z}} \left[P_X\left(\underbrace{\Lambda_\rho \cap f^{-1}(i)}\right) + \rho P_X\left(\underbrace{\underbrace{\left[f^{-1}(i) \setminus \Lambda_\rho \cap f^{-1}(i)\right]_{\min\{l-|\Lambda_\rho|, |f^{-1}(i)\setminus\Lambda_\rho|\}}}}\right)\right]. \tag{B.2}$$

In (B.2), for each $i \in \mathcal{Z}$, focusing on the term within $[\cdot]$, if (B.1) is violated, there exists an element in $\underbrace{\cdot}$ of higher P_X-probability than the minimum P_X-probability element in $\underbrace{\cdot}$. Swapping them would lead to a higher value of $[\cdot]$ since $\rho \leq 1$, thereby contradicting the optimality of Λ_ρ in (3.3). Therefore, (B.1) holds.

(ii) Assume

$$l - |\Lambda_\rho| > |f^{-1}(0) \setminus \Lambda_\rho| \tag{B.3}$$

and

$$l - |\Lambda_\rho| \leq |f^{-1}(1) \setminus \Lambda_\rho|.$$

Let

$$\left|\Lambda_\rho \cap f^{-1}(i)\right| = a_i, \quad i \in \{0,1\},$$

which give

$$|\Lambda_\rho| = \sum_{i\in\{0,1\}} a_i \tag{B.4}$$

and

$$|f^{-1}(i) \setminus \Lambda_\rho| = |f^{-1}(i)| - a_i, \quad i \in \{0,1\}, \tag{B.5}$$

and using Lemma 3.2(i),

$$\Lambda_\rho = \left[f^{-1}(1)\right]_{a_1} \cup \left[f^{-1}(0)\right]_{a_0}. \tag{B.6}$$

Substituting (B.4), (B.5) in (B.3), we get

$$l - |f^{-1}(0)| > a_1. \tag{B.7}$$

Consider the set $\tilde{\Lambda}_\rho$ given by

$$\tilde{\Lambda}_\rho = \left[f^{-1}(1)\right]_{l-|f^{-1}(0)|} \cup \left[f^{-1}(0)\right]_{a_0}. \tag{B.8}$$

Since $l - |f^{-1}(0)| > a_1 \geq 0$, $|f^{-1}(1)| > l - |f^{-1}(0)|$ and $\left|\tilde{\Lambda}_\rho\right| = l - |f^{-1}(0)| + a_0 \leq l$, $\Lambda = \tilde{\Lambda}_\rho$ is a valid choice for the expression within $[\cdot]$ in (3.3). We claim that choosing $\Lambda = \tilde{\Lambda}_\rho$ gives a larger value for the expression within $[\cdot]$ in (3.3), thereby contradicting the optimality of Λ_ρ, and, in turn, proving that (B.3) cannot hold. To establish the claim above, with $\Lambda = \Lambda_\rho$ in the expression

within $[\cdot]$ in (3.3), and using (B.6), we get

$$\begin{aligned}[\cdot] =& P_X\left([f^{-1}(0)]_{a_0}\right) + \rho P_X\left(\left[f^{-1}(0) \setminus [f^{-1}(0)]_{a_0}\right]_{|f^{-1}(0)|-a_0}\right) + \\ & P_X\left([f^{-1}(1)]_{a_1}\right) + \rho P_X\left(\left[f^{-1}(1) \setminus [f^{-1}(1)]_{a_1}\right]_{l-a_1-a_0}\right); \end{aligned} \tag{B.9}$$

and upon choosing $\Lambda = \tilde{\Lambda}_\rho$ in $[\cdot]$ in (3.3), and using (B.8), we get

$$\begin{aligned}[\cdot] =& P_X\left([f^{-1}(0)]_{a_0}\right) + \rho P_X\left(\left[f^{-1}(0) \setminus [f^{-1}(0)]_{a_0}\right]_{|f^{-1}(0)|-a_0}\right) + \\ & P_X\left([f^{-1}(1)]_{l-|f^{-1}(0)|}\right) + \rho P_X\left(\left[f^{-1}(1) \setminus [f^{-1}(1)]_{l-|f^{-1}(0)|}\right]_{|f^{-1}(0)|-a_0}\right). \end{aligned} \tag{B.10}$$

Observe that in (B.9), (B.10), by (B.7), $[f^{-1}(1)]_{a_1} \subset [f^{-1}(1)]_{l-|f^{-1}(0)|}$, and since $\rho \leq 1$, the claim holds.

Similar arguments apply if we assume

$$l - |\Lambda_\rho| > |f^{-1}(1) \setminus \Lambda_\rho| \text{ and } l - |\Lambda_\rho| \leq |f^{-1}(0) \setminus \Lambda_\rho|$$

or

$$l - |\Lambda_\rho| > |f^{-1}(1) \setminus \Lambda_\rho| \text{ and } l - |\Lambda_\rho| > |f^{-1}(0) \setminus \Lambda_\rho|.$$

Therefore, (3.6) is true.

(iii) Consider $1 - \pi_u^{(l)}(\rho) = \max\limits_{0 \leq l' \leq l} \alpha(\rho, l')$ where

$$\alpha(\rho, l') = \max_{\substack{\Lambda \subset \mathcal{X}: \\ |\Lambda| = l'}} \beta(\rho, l', \Lambda)$$

$$\beta\left(\rho, l', \Lambda\right) = P_X(\Lambda) + \rho \sum_{i \in \mathcal{Z}} P_X\left(\left[f^{-1}(i) \setminus \Lambda\right]_{\min\{l-l', |f^{-1}(i)\setminus\Lambda|\}}\right),$$

where $|\Lambda| = l'$. For each fixed $0 \leq l' \leq l$ and fixed $\Lambda \subset \mathcal{X}$ with $|\Lambda| = l'$, $\beta\left(\rho, l', \Lambda\right)$ is affine and nondecreasing in ρ. Hence, $\alpha\left(\rho, l'\right)$ – as the maximum of finitely many affine and nondecreasing functions in ρ – is piecewise affine, continuous and nondecreasing in ρ. In turn, $1 - \pi_u^{(l)}(\rho)$ – as the maximum of $l+1$ such functions $\alpha\left(\rho, l'\right)$ – also is piecewise affine, continuous and nondecreasing in ρ. The values of $\pi_u^{(l)}(\rho)$ at the end points $\rho = 0$ and $\rho = 1$ in (3.7) follow from a straightforward calculation.

(iv) For $l' = 0$, $\alpha(\rho, 0)$ is linear in ρ with $\alpha(0,0) = 0$ and $\alpha(1,0) = \sum_{i \in \mathcal{Z}} P_X\left(\left[f^{-1}(i)\right]_{\min\{l, |f^{-1}(i)|\}}\right)$; and for $l' = l$, $\alpha(\rho, l) \equiv P_X\left(L_l^*\right)$. And for $0 < l' < l$, $\alpha\left(\rho, l'\right)$ is piecewise affine, continuous and nondecreasing in $\rho \in [0,1]$ as noted in the proof of (iii). Further, observe that for $0 \leq l_1' < l_2' \leq l$,

$$\alpha\left(0, l_1'\right) \leq \alpha\left(0, l_2'\right) \text{ while } \alpha\left(1, l_1'\right) \geq \alpha\left(1, l_2'\right)$$

where the latter is immediate upon examining

$$\alpha\left(1, l'\right) = \max_{\substack{\Lambda \subset \mathcal{X}: \\ |\Lambda| = l'}} \left[P_X(\Lambda) + \sum_{i \in \mathcal{Z}} P_X\left(\left[f^{-1}(i) \setminus \Lambda\right]_{\min\{l-l', |f^{-1}(i)\setminus\Lambda|\}}\right)\right]$$

and observing that $\alpha\left(1, l'\right) \leq \alpha\left(1, l' - 1\right)$, etc. The claim in (iv) follows.

(v) The claim follows readily from $|\Lambda_\rho|$ taking values in $\{0, 1, \ldots, l\}$, property (iv), and ρ ranging continuously in $[0,1]$.

■

Appendix C:

C.1. Calculation of var(AX) and mmse $(X|AX)$

We have

$$\text{var}(AX) = \text{tr}\left(AA^T\right) = \text{tr}\left(USV^TVS^TU^T\right) = \text{tr}\left(USS^TU^T\right) = \text{tr}\left(SS^T\right) = \sum_{i=1}^{r} s_i^2.$$

Next, noting that X and $AX = USV^TX$ are jointly Gaussian, we have

$$\begin{aligned}
&\text{mmse}\left(X|AX\right) = \text{mmse}\left(X|USV^TX\right) \\
&= \mathbb{E}\left[\left\|X - \mathbb{E}\left[X\left(USV^TX\right)^T\right]\left(\mathbb{E}\left[USV^TX\left(USV^TX\right)^T\right]\right)^{-1}USV^TX\right\|^2\right] \\
&= \mathbb{E}\left[\left(X - \mathbb{E}\left[X\left(USV^TX\right)^T\right]\left(\mathbb{E}\left[USV^TX\left(USV^TX\right)^T\right]\right)^{-1}USV^TX\right)^T X\right] \\
&= \text{tr}\left(\mathbb{E}\left[XX^T\right]\right) \\
&\qquad - \text{tr}\left(\mathbb{E}\left[X\left(USV^TX\right)^T\right]\left(\mathbb{E}\left[\left(USV^TX\right)\left(USV^TX\right)^T\right]\right)^{-1}\mathbb{E}\left[USV^TXX^T\right]\right) \\
&= \text{tr}\left(I_n\right) - \text{tr}\left(I_nVS^TU^T\left(USV^TI_nVS^TU^T\right)^{-1}USV^TI_n\right) \\
&= n - \text{tr}\left(S^T\left(SS^T\right)^{-1}S\right) = n - r.
\end{aligned}$$

C.2. Proofs of Lemmas 4.2, 4.3

Proof of Lemma 4.2: Recalling (4.4), we have

$$\mathbb{E}\left[\|AX-Z\|^2\right] = \mathbb{E}\left[\left\|U\left(U^TAX-U^TZ\right)\right\|^2\right] = \mathbb{E}\left[\left\|SV^TX-U^TZ\right\|^2\right],$$

from which we get

$$\begin{aligned}
&\sup_{P_{Z|X}:\mathbb{E}\left[\|AX-Z\|^2\right]\le\rho} \inf_g \mathbb{E}\left[\|X-g(Z)\|^2\right] \\
&= \sup_{P_{Z|X}:\mathbb{E}\left[\|SV^TX-U^TZ\|^2\right]\le\rho} \inf_g \mathbb{E}\left[\left\|X-g(U^TZ)\right\|^2\right] \\
&= \sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\le\rho} \inf_g \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right], \quad \text{since } U \text{ is orthonormal.}
\end{aligned}$$

■

Proof of Lemma 4.3: Since the supremum in the right-side of (4.11) is over a restricted set compared with the left-side, it suffices to show that (4.11) holds with "$\le$," i.e.,

$$\sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\le\rho} \inf_g \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right] \le \sup_{\substack{P_{\tilde{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^TX-\tilde{Z}\right\|^2\right]\le\rho \\ \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right]\le s_i^2, \\ i=1,\ldots,r}} \inf_g \mathbb{E}\left[\left\|X-g(\tilde{Z})\right\|^2\right]. \tag{C.1}$$

Since S contains only r nonzero rows, SV^TX in the left-side of (4.11) is a $\mathbb{R}^m$-valued rv containing at most r nonzero elements. Recalling that $\tilde{S}$ is the $r\times n$-matrix consisting of the

nonzero rows of S, it is easily seen that

$$\sup_{P_{\bar{Z}|X}:\mathbb{E}\left[\left\|SV^TX-\bar{Z}\right\|^2\right]\leq\rho}\ \inf_g\ \mathbb{E}\left[\left\|X-g(\bar{Z})\right\|^2\right]=\sup_{P_{\check{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^TX-\check{Z}\right\|^2\right]\leq\rho}\ \inf_g\ \mathbb{E}\left[\left\|X-g(\check{Z})\right\|^2\right] \tag{C.2}$$

where $\check{Z}$ is a $\mathbb{R}^r$-valued rv denoting a ρ-QR under recoverability of $\tilde{S}V^TX$. For every $\mathbb{R}^r$-valued rv $\check{Z}=\left[\check{Z}_1,\ldots,\check{Z}_r\right]^T$, consider the $\mathbb{R}^r$-valued rv $\tilde{Z}$ given by

$$\tilde{Z}=\left[\check{Z}_1\mathbb{1}\left(\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_1\right|^2\right]\leq s_1^2\right),\ldots,\check{Z}_r\mathbb{1}\left(\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_r\right|^2\right]\leq s_r^2\right)\right]^T. \tag{C.3}$$

Observe that

$$\begin{aligned}\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\tilde{Z}\right)_i\right|^2\right]&=\begin{cases}\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_i\right|^2\right], & \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_i\right|^2\right]\leq s_i^2\\ s_i^2, & \mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_i\right|^2\right]>s_i^2\end{cases}\\&\leq\mathbb{E}\left[\left|\left(\tilde{S}V^TX-\check{Z}\right)_i\right|^2\right],\quad i=1,\ldots,r,\end{aligned} \tag{C.4}$$

from which, owing to the constraint under the supremum in the right-side of (C.2), we get

$$\mathbb{E}\left[\left\|\tilde{S}V^TX-\tilde{Z}\right\|^2\right]\leq\mathbb{E}\left[\left\|\tilde{S}V^TX-\check{Z}\right\|^2\right]\leq\rho. \tag{C.5}$$

Since

$$X\multimap\!\circ\!-\check{Z}\multimap\!\circ\!-\tilde{Z},$$

and using data processing inequality for MMSE [77], [75], we get

$$\inf_g \mathbb{E}\left[\left\|X - g(\check{Z})\right\|^2\right] \leq \inf_g \mathbb{E}\left[\left\|X - g(\tilde{Z})\right\|^2\right]. \tag{C.6}$$

We have shown that for every $\mathbb{R}^r$-valued rv $\check{Z}$ that satisfies the ρ-recoverability constraint, there exists another $\mathbb{R}^r$-valued rv $\tilde{Z}$ (C.3) that also satisfies the ρ-recoverability constraint (C.5) and additionally, due to (C.4), meets the constraints

$$\mathbb{E}\left[\left|\left(\tilde{S}V^T X - \tilde{Z}\right)_i\right|^2\right] \leq s_i^2, \quad i = 1, \ldots, r. \tag{C.7}$$

Therefore, using (C.5), (C.6), (C.7), we get

$$\sup_{P_{\tilde{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^T X - \tilde{Z}\right\|^2\right] \leq \rho} \inf_g \mathbb{E}\left[\left\|X - g(\check{Z})\right\|^2\right] \leq \sup_{\substack{P_{\tilde{Z}|X}:\mathbb{E}\left[\left\|\tilde{S}V^T X - \tilde{Z}\right\|^2\right] \leq \rho \\ \mathbb{E}\left[\left|\left(\tilde{S}V^T X - \tilde{Z}\right)_i\right|^2\right] \leq s_i^2, \\ i=1,\ldots,r}} \inf_g \mathbb{E}\left[\left\|X - g(\tilde{Z})\right\|^2\right],$$

which along with (C.2) gives (C.1). ■

C.3. Verification that $\tilde{Z}_o$ satisfies (4.13)

For $i = 1, \ldots, r$,

$$\begin{aligned}
\mathbb{E}\left[\left|\left(\tilde{S}V^T X - \tilde{Z}_o\right)_i\right|^2\right] &= \mathbb{E}\left[\left|\left(\tilde{S}V^T X - D_a \tilde{S}V^T X - D_{no} N\right)_i\right|^2\right] \\
&= \mathbb{E}\left[\left|\left(\tilde{S}V^T X - D_a \tilde{S}V^T X\right)_i\right|^2\right] + \rho_i - \frac{\rho_i^2}{s_i^2} \\
&= \frac{\rho_i^2}{s_i^2} + \rho_i - \frac{\rho_i^2}{s_i^2} = \rho_i
\end{aligned} \tag{C.8}$$

$$\leq s_i^2.$$

Next,

$$\begin{aligned}
\mathbb{E}\left[\left\|\tilde{S}V^TX - \tilde{Z}_o\right\|^2\right] &= \sum_{i=1}^{r} \mathbb{E}\left[\left|\left(\tilde{S}V^TX - D_a\tilde{S}V^TX - D_{no}N\right)_i\right|^2\right] \\
&= \sum_{i=1}^{r} \rho_i, \quad \text{using (C.8)} \\
&= \rho.
\end{aligned}$$

Appendix D:

D.1. Proofs of Lemmas 5.6 and 5.7

Proof of Lemma 5.6: Assume first that

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

Then

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

Equality holds above iff $H\left(P(\mathcal{A})\right) = H(P)$ which is tantamount to (5.38).

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 5.7: We have

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

Hence,

$$\begin{aligned} |D(P||Q) - D(P||Q_o)| &\leq \sum_{x \in support\ (Q_o)} \frac{P(x)}{Q_o(x)}\ |Q(x) - Q_o(x)| \\ &\leq \frac{1}{Q_o^{min}}\ \text{var}\,(Q, Q_o) \end{aligned}$$

so that

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

whence

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

■

D.2. Proof of (5.53)

To establish (5.53), we write for any $\epsilon > 0$,

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

since

$$\begin{aligned}
\left|\Phi_n^j\left(\underline{\alpha}, V\right)\right| &\leq \left|\left(\underline{\alpha}V^{-1}\right)(j) \log \frac{\left(\underline{\alpha}V^{-1}\right)(j)}{\kappa_n(T_n)(j)}\right| \\
&\leq 1. \log \frac{1}{1/(n+k)} = \log(n+k), \quad \text{by (5.27)}.
\end{aligned}$$

Since $\epsilon > 0$ is arbitrary, (5.53) will follow from (D.1) if for any $\epsilon > 0$,

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

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

$$\begin{aligned}
&\log(n+k)\sup_{V\in\mathcal{V}(\rho)}\sup_{\underline{\alpha}\in\Delta_k(V)} P\left(|\Phi_n^j(\underline{\alpha},V)|>\epsilon\right)\\
&=\log(n+k)\sup_{V\in\mathcal{V}(\rho)}\sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\left|\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}\right|>\epsilon\right)\\
&\le\log(n+k)\sup_{V\in\mathcal{V}(\rho)}\sup_{\underline{\alpha}\in\Delta_k(V)} P\left(\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}>\epsilon\right)\\
&\qquad+\log(n+k)\sup_{V\in\mathcal{V}(\rho)}\sup_{\underline{\alpha}\in\Delta_k(V)} P\left(-\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}>\epsilon\right).
\end{aligned}\tag{D.2}$$

Considering the first term in the right-side above and noting by (5.27) that $\kappa_n(T_n)(j)\ge 1/(n+k)$, clearly the probability equals 0 if $\epsilon\ge\underline{\alpha}\nu_j\log(n+k)$ so that it suffices to consider

$$\underline{\alpha}\nu_j\log(n+k)>\epsilon\quad\text{or}\quad\underline{\alpha}\nu_j>\frac{\epsilon}{\log(n+k)}.\tag{D.3}$$

Then, in (D.2),

$$\begin{aligned}
P\left(\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}>\epsilon\right)&=P\left(\kappa_n(T_n)(j)<\underline{\alpha}\nu_j 2^{-\frac{\epsilon}{\underline{\alpha}\nu_j}}\right)\\
&\le P\left(\kappa_n(T_n)(j)<\underline{\alpha}\nu_j 2^{-\epsilon}\right)\\
&\le P\left(\widetilde{Q}(T_n)\nu_j<\underline{\alpha}\nu_j 2^{-\epsilon}\left(1+\frac{k}{n}\right)\right),\quad\text{by (5.27)}\\
&\le P\left(\left|\widetilde{Q}(T_n)\nu_j-\underline{\alpha}\nu_j\right|\ge\underline{\alpha}\nu_j\left(1-2^{-\epsilon}\left(1+\frac{k}{n}\right)\right)\right)\\
&=P\left(\left|\widetilde{Q}(T_n)\nu_j-\underline{\alpha}\nu_j\right|\ge\underline{\alpha}\nu_j\left(1-2^{-\epsilon}\left(1+\frac{k}{n}\right)\right)^+\right)
\end{aligned}\tag{D.4}$$

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 $V\in\mathcal{V}(\rho)$,

$\|V^{-1}\|_1 \triangleq \max_{1\le j\le k} \|\nu_j\|_1$. Then, in (D.4),

$$\left|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j\right| \le \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \|\nu_j\|_1 \le \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \|V^{-1}\|_1 \le \left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \frac{k}{2\rho - 1} \tag{D.5}$$

since for a strictly diagonally-dominated $V \in \mathcal{V}(\rho)$, we have by [72, Theorem 1] and [51, Section 3, Theorem 1] that $\|V^{-1}\|_1 \le k/(2\rho-1)$, noting that $\rho > 0.5$. Furthermore,

$$\begin{aligned}
\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 &\le \left\|\widetilde{Q}(T_n) - T_n\right\|_1 + \|T_n - \underline{\alpha}\|_1 \\
&\le \sqrt{2\ln 2}\left(\sqrt{D\left(T_n||\widetilde{Q}(T_n)\right)} + \sqrt{D\left(T_n||\alpha\right)}\right), \quad \text{by [18, Lemma 11.6.1]} \\
&\le 2\sqrt{2\ln 2\, D\left(T_n||\alpha\right)}, \quad \text{by (5.26)}.
\end{aligned} \tag{D.6}$$

Hence, in (D.4), by (D.5), (D.6),

$$\begin{aligned}
&P\left(\underline{\alpha}\nu_j \log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \\
&\le P\left(\sqrt{D\left(T_n||\underline{\alpha}\right)} \ge \frac{(2\rho-1)}{2k\sqrt{2\ln 2}}\underline{\alpha}\nu_j\left(1 - 2^{-\epsilon}\left(1+\frac{k}{n}\right)\right)^+\right) \\
&\le P\left(D\left(T_n||\underline{\alpha}\right) \ge \frac{(2\rho-1)^2}{8k^2\ln 2}\frac{\epsilon^2}{\log^2(n+k)}\left(\left(1 - 2^{-\epsilon}\left(1+\frac{k}{n}\right)\right)^+\right)^2\right)
\end{aligned} \tag{D.7}$$

using (D.3). Denoting the threshold above by $\tau_1(\rho,\epsilon,n)$, straightforward manipulation yields that

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

with

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

for all $n\geq N_1(\epsilon,k,c)=k/((1-c)2^{\epsilon}-1)$. Then, in (D.7) for all $n\geq N_1(\epsilon,k,c)$, by [18, Theorem 11.2.1], the first term in the right-side of (D.2) is

$$\begin{aligned}
&\leq \log(n+k)P\left(D\left(T_n||\underline{\alpha}\right)\geq\frac{c_1(\rho,\epsilon)}{\log^2(n+k)}\right)\\
&\leq \log(n+k)\exp\left[-n\left(\frac{c_1(\rho,\epsilon)}{\log^2(n+k)}-k\frac{\log(n+1)}{n}\right)\right]\\
&\leq \exp\left[-\left(c_1(\rho,\epsilon)\frac{n}{\log^2(n+k)}-(k+1)\log(n+k)\right)\right]
\end{aligned}\tag{D.8}$$

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

$$\lim_n\ \log(n+k)\sup_{V\in\mathcal{V}(\rho)}\sup_{\underline{\alpha}\in\Delta_k(\rho)}P\left(\underline{\alpha}\nu_j\log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)}>\epsilon\right)=0.\tag{D.9}$$

Turning to the second term in the right-side of (D.2), 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

$$-\underline{\alpha}\nu_j\log\underline{\alpha}\nu_j>\epsilon\ \text{ for }\ 0<\epsilon<0.5,\tag{D.10}$$

we get

$$P\left(-\underline{\alpha}\nu_j \log \frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) \leq P\left(\kappa_n(T_n)(j) > \underline{\alpha}\nu_j 2^{\epsilon}\right)$$
$$= P\left(\widetilde{Q}(T_n)\nu_j > \underline{\alpha}\nu_j 2^{\epsilon}\left(1+\frac{k}{n}\right) - \frac{1}{n}\right)$$
$$\leq P\left(|\widetilde{Q}(T_n)\nu_j - \underline{\alpha}\nu_j| \geq \underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right) - \frac{1}{n}\right)$$
$$\leq P\left(\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \left\|V^{-1}\right\|_1 \geq \underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right) - \frac{1}{n}\right),$$

by the first inequality in (D.5)

$$\leq P\left(\left\|\widetilde{Q}(T_n) - \underline{\alpha}\right\|_1 \geq \left(\underline{\alpha}\nu_j\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right) - \frac{1}{n}\right)\frac{2\rho-1}{k}\right),$$

by the last inequality in (D.5)

$$\leq P\left(\sqrt{D\left(T_n||\underline{\alpha}\right)} \geq \frac{(2\rho-1)}{2k\sqrt{2\ln 2}}\left(t^*(\epsilon)\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right) - \frac{1}{n}\right)^+\right), \quad \text{by (D.6) and (D.10)} \tag{D.11}$$

$$= P\left(D\left(T_n||\underline{\alpha}\right) \geq \frac{(2\rho-1)^2}{8k^2\ln 2}\left(\left(t^*(\epsilon)\left(2^{\epsilon}\left(1+\frac{k}{n}\right)-1\right) - \frac{1}{n}\right)^+\right)^2\right) \tag{D.12}$$

where $t^*(\epsilon)$ in (D.11) is the solution of $-t\log t = \epsilon$ for $t \in [0, 0.5)$. Denoting by $\tau_2(\rho, \epsilon, n)$ the threshold in (D.12), 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 (D.2) upon treating the probability in (D.12) in the manner of (D.8), and observing

that

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

we have

$$\lim_n \log(n+k) \sup_{V\in\mathcal{V}(\rho)} \sup_{\underline{\alpha}\in\Delta_k(V)} P\left(-\underline{\alpha}\nu_j \log\frac{\underline{\alpha}\nu_j}{\kappa_n(T_n)(j)} > \epsilon\right) = 0. \tag{D.13}$$

Upon combining (D.9) and (D.13), we get (5.53).

D.3. Lower Bound for (5.84), (5.96) and Proof of (5.64), (5.65)

Lower bound for (5.84): We first bound (5.84) below by restricting the supremum further according to

$$\begin{aligned}
&\inf_{\widehat{P}_n^{\beta(n)}\in\mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ \underline{\alpha}(j')=0,\ j'=k'-l',\ldots,k'-1}} \sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{|f'^{-1}(j')|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)}\right) \\
\geq &\inf_{\widehat{P}_n^{\beta(n)}\in\mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha}\in\Delta_{k'}:\\ l\left(\frac{1-l\rho}{k-l'-l}\right)\leq\underline{\alpha}(j')\leq\min\left\{\frac{\left\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\right\rceil}{n},\, l\rho\right\},\ j'=1,\ldots,k'-l'-1\\ \underline{\alpha}(j')=0,\ j'=k'-l',\ldots,k'-1}} \sum_{j'=0}^{k'-l'-1} \frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \log\left(\frac{\underline{\alpha}(j') - l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho - l\left(\frac{1-l\rho}{k-l'-l}\right)} \frac{|f'^{-1}(j')|}{\widehat{P}_n^{\beta(n)}\left(Q'^{(n)}(\underline{\alpha})\right)\left(f'^{-1}(j')\right)}\right).
\end{aligned} \tag{D.14}$$

Observe from (5.63) 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 (D.14). Hence, with

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

for some $\underline{\beta}=\{\beta_0,\beta_1,\ldots,\beta_{k'-1}\}\in\Delta_{k'}$, the right-side of (D.14)

$$\geq\inf_{\underline{\beta}\in\Delta_{k'}}\sup_{\underline{\alpha}\in\Delta_{k'}\sim\text{right-side of (D.14)}}\left\{\sum_{j'=0}^{k'-l'-1}\frac{\underline{\alpha}(j')-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}\log\left(\frac{\underline{\alpha}(j')-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}\frac{|f'^{-1}(j')|}{\beta_{j'}}\right)\right\}. \tag{D.15}$$

For each fixed $\underline{\beta}\in\Delta_{k'}$, we further bound below the expression in (D.15) 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 (5.56), (5.57)) specified by

$$\underline{\alpha}_1=\left(l\rho,l\left(\frac{1-l\rho}{k-l'-l}\right),\ldots,l\left(\frac{1-l\rho}{k-l'-l}\right),0,\ldots,0\right) \tag{D.16}$$

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

$$\underline{\alpha}_t(j')=\begin{cases}l\rho-\left(\min\left\{\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n},\ l\rho\right\}-l\left(\frac{1-l\rho}{k-l'-l}\right)\right), & j'=0\\ l\left(\frac{1-l\rho}{k-l'-l}\right), & j'=1,\ldots,t-2,t,\ldots,k'-l'-1\\ \min\left\{\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n},\ l\rho\right\}, & j'=t-1\\ 0, & j'\geq k'-l'.\end{cases} \tag{D.17}$$

A description of the $k'-l'-1$ values above is as follows: For $t=2,\ldots,k'-l'$, $\underline{\alpha}_t(t-1)=$

$\min\left\{\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n},\ l\rho\right\}, \underline{\alpha}_t(1)=\cdots=\underline{\alpha}_t(t-2)=\underline{\alpha}_t(t)=\cdots=\underline{\alpha}_t(k'-l'-1)=l\left(\frac{1-l\rho}{k-l'-l}\right)$ 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 (D.15), i.e., the right-side of (5.78) under (D.16), (D.17), 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

$$\begin{aligned} l\left(\frac{1-l\rho}{k-l'-l}\right) &\leq l\frac{(1-l\rho)}{l}, \quad \text{since from (5.56), } k-l'-l\geq l \\ &\leq l\rho, \quad \text{using } l\rho\geq l/(l+1)\geq 1/2 \text{ from (5.54)}, \end{aligned} \tag{D.18}$$

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

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

and

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

This completes the verification.

Now set

$$\mu_n \triangleq \frac{\min\left\{\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n},\ l\rho\right\}-l\left(\frac{1-l\rho}{k-l'-l}\right)}{l\rho-l\left(\frac{1-l\rho}{k-l'-l}\right)}. \tag{D.19}$$

Then the supremum in (D.15) reduces to a maximum over $k'-l'$ choices of $\underline{\alpha}_t,\ t=1,\ldots,k'-l'$,

given by (D.16), (D.17). Then, with μ_n as in (D.19), the right-side of (D.15) is bounded below as

$$\geq \inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{ \log\frac{|f'^{-1}(0)|}{\beta_0}, \mu_n \log\left(\mu_n\frac{|f'^{-1}(1)|}{\beta_1}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{|f'^{-1}(0)|}{\beta_0}\right), \right.$$
$$\left. \ldots, \mu_n \log\left(\mu_n\frac{|f'^{-1}(k'-l'-1)|}{\beta_{k'-l'-1}}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{|f'^{-1}(0)|}{\beta_0}\right) \right\} \quad \text{(D.20)}$$

where the tth term, $1 \leq t \leq k'-l'$ is obtained by evaluating the expression within $\{\cdot\}$ in (D.15) at $\underline{\alpha}_t$. Moreover, the right-side of (D.20) is

$$= \inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{ \log\frac{|f'^{-1}(0)|}{\beta_0}, \right.$$
$$\left. \max_{1\leq j'\leq k'-l'-1} \left\{ \mu_n \log\left(\mu_n\frac{|f'^{-1}(j')|}{\beta_{j'}}\right) + (1-\mu_n)\log\left((1-\mu_n)\frac{|f'^{-1}(0)|}{\beta_0}\right)\right\}\right\}. \quad \text{(D.21)}$$

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' (5.82) 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 (D.21), it is sufficient to consider $\underline{\beta} \in \Delta_{k'}$ such that

$$\beta_{k'-l'} = \cdots = \beta_{k'-1} = 0. \quad \text{(D.22)}$$

For every $0 \leq \beta_0 \leq 1$, we solve the inner $\inf\ \max$ in (D.21), which, using (D.22), is equivalent to

$$\inf_{\substack{\beta_1,\ldots,\beta_{k'-l'-1}: \\ \beta_{j'}\geq 0,\ j'=1,\ldots,k'-l'-1 \\ \sum_{j'=1}^{k'-l'-1}\beta_{j'}=1-\beta_0}} \max_{1\leq j'\leq k'-l'-1} \frac{|f'^{-1}(j')|}{\beta_{j'}}. \quad \text{(D.23)}$$

We claim that

$$\max_{1\le j'\le k'-l'-1} \frac{|f'^{-1}(j')|}{\beta_{j'}} \ge \frac{\sum_{j''=1}^{k'-l'-1} |f'^{-1}(j'')|}{1-\beta_0} \tag{D.24}$$

since, if

$$\begin{aligned}
\max_{1\le j'\le k'-l'-1} \frac{|f'^{-1}(j')|}{\beta_{j'}} &< \frac{\sum_{j''=1}^{k'-l'-1} |f'^{-1}(j'')|}{1-\beta_0} \\
\text{i.e., } \frac{|f'^{-1}(j')|}{\beta_{j'}} &< \frac{\sum_{j''=1}^{k'-l'-1} |f'^{-1}(j'')|}{1-\beta_0}, \quad j'=1,\dots,k'-l'-1 \\
|f'^{-1}(j')| &< \frac{\beta_{j'}}{1-\beta_0} \sum_{j''=1}^{k'-l'-1} |f'^{-1}(j'')|, \quad j'=1,\dots,k'-l'-1,
\end{aligned}$$

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

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

which is a contradiction. Also, by choosing

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

we get

$$\inf_{\substack{\beta_1,\dots,\beta_{k'-l'-1}: \\ \beta_{j'}\ge 0,\ j'=1,\dots,k'-l'-1 \\ \sum_{j'=1}^{k'-l'-1}\beta_{j'}=1-\beta_0}} \max_{1\le j'\le k'-l'-1} \frac{|f'^{-1}(j')|}{\beta_{j'}} \le \frac{\sum_{j''=1}^{k'-l'-1} |f'^{-1}(j'')|}{1-\beta_0}. \tag{D.25}$$

Thus, the expression in (D.23) equals the (common) right-sides of (D.24), (D.25), using which

the lower bound in (D.21) becomes

$$\inf_{0\le\beta_0\le 1} \max\left\{\log\frac{|f'^{-1}(0)|}{\beta_0},\right.$$
$$\left.\mu_n\log\left(\frac{\mu_n\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|}{1-\beta_0}\right)+(1-\mu_n)\log\left((1-\mu_n)\frac{|f'^{-1}(0)|}{\beta_0}\right)\right\}. \quad \text{(D.26)}$$

The first term in (D.26) is decreasing in $0\le\beta_0\le 1$ and the second term is convex in $0\le\beta_0\le 1$ since it can be written as

$$D\left(\text{Ber}(\mu_n)||\text{Ber}(1-\beta_0)\right)+\mu_n\log\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|+(1-\mu_n)\log|f'^{-1}(0)| \quad \text{(D.27)}$$

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

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

and[1] 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 $|f'^{-1}(0)|\ge\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$ and $|f'^{-1}(0)|<\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$.

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

$$\beta_0''\ge\beta_0'$$

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

i.e.,

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

which is

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

because $(1-\mu_n)^{\frac{1}{\mu_n}}\leq 1$ and $|f'^{-1}(0)|\geq\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$. Then $\inf_{0\leq\beta_0\leq 1}$ in (D.26) is attained as a minimum at $\beta_0=\beta_0''$, and becomes

$$\log|f'^{-1}(0)|+\log\left(1+\frac{\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|}{|f'^{-1}(0)|}(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}}\mu_n\right), \tag{D.28}$$

with μ_n as in (D.19).

(ii) $|f'^{-1}(0)|<\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$: We have that (D.26) is bounded below as

$$\begin{aligned}&\geq\inf_{0\leq\beta_0\leq 1}D\left(\text{Ber}(1-\mu_n)||\text{Ber}(\beta_0)\right)+\mu_n\log\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|+(1-\mu_n)\log|f'^{-1}(0)|\\&=\log|f'^{-1}(0)|+\mu_n\log\frac{\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|}{|f'^{-1}(0)|}.\end{aligned} \tag{D.29}$$

Note that the second $\log$ term in (D.29) is positive.

From (D.28) along with the observation that $(1-\mu_n)^{\frac{1-\mu_n}{\mu_n}}\geq 1/e$ and (D.29), we obtain the desired lower bound for (5.84) which along with (5.77) and (D.19) gives (5.85), (5.86), (5.87).

Lower bound for (5.96): Turning next to the task of bounding (5.96) below, we have

$$\begin{aligned}
&\inf_{\widehat{P}_n^{\beta^{(n)}} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \log \left(\frac{\underline{\alpha}(0)}{l\rho} \frac{|f'^{-1}(0)|}{\widehat{P}_n^{\beta^{(n)}} \left(Q'^{(n)}(\underline{\alpha}) \right) \left(f'^{-1}(0) \right)} \right) \\
&\qquad + \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \log \left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{|f'^{-1}(1)|}{\widehat{P}_n^{\beta^{(n)}} \left(Q'^{(n)}(\underline{\alpha}) \right) \left(f'^{-1}(1) \right)} \right) \\
\geq &\inf_{\widehat{P}_n^{\beta^{(n)}} \in \mathcal{S}_n(k')} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ 1-l\rho \leq \underline{\alpha}(1) \leq \frac{\lceil n(1-l\rho) \rceil}{n} \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \frac{\underline{\alpha}(0)}{l\rho} \log \left(\frac{\underline{\alpha}(0)}{l\rho} \frac{|f'^{-1}(0)|}{\widehat{P}_n^{\beta^{(n)}} \left(Q'^{(n)}(\underline{\alpha}) \right) \left(f'^{-1}(0) \right)} \right) \\
&\qquad + \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \log \left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{|f'^{-1}(1)|}{\widehat{P}_n^{\beta^{(n)}} \left(Q'^{(n)}(\underline{\alpha}) \right) \left(f'^{-1}(1) \right)} \right).
\end{aligned} \tag{D.30}$$

In this case, too, observe from (5.63) 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 (D.30). Hence, with

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

for some $\underline{\beta} = \{\beta_0, \beta_1, \ldots, \beta_{k'-1}\} \in \Delta_{k'}$, the right-side of (D.30)

$$\begin{aligned}
\geq &\inf_{\underline{\beta} \in \Delta_{k'}} \sup_{\substack{\underline{\alpha} \in \Delta_{k'}: \\ 1-l\rho \leq \underline{\alpha}(1) \leq \frac{\lceil n(1-l\rho) \rceil}{n} \\ \underline{\alpha}(j')=0,\ j'=2,\ldots,k'-1}} \left\{ \frac{\underline{\alpha}(0)}{l\rho} \log \left(\frac{\underline{\alpha}(0)}{l\rho} \frac{|f'^{-1}(0)|}{\beta_0} \right) \right. \\
&\qquad \left. + \frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \log \left(\frac{\underline{\alpha}(1) - (1 - l\rho)}{l\rho} \frac{|f'^{-1}(1)|}{\beta_1} \right) \right\}.
\end{aligned} \tag{D.31}$$

We further bound (D.31) below by replacing the supremum by a maximum of the expression

within $\{\cdot\}$ in (D.31) evaluated at two points $\underline{\alpha}_1, \underline{\alpha}_2$ given by

$$\begin{aligned}\underline{\alpha}_1 &= (l\rho, 1-l\rho, 0, \ldots, 0)\\ \underline{\alpha}_2 &= \left(1 - \frac{\lceil n(1-l\rho)\rceil}{n}, \frac{\lceil n(1-l\rho)\rceil}{n}, 0, \ldots, 0\right).\end{aligned} \tag{D.32}$$

When $\underline{\alpha} = \underline{\alpha}_1$, the coefficients of the log terms in (D.31) 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

$$\theta_n = \frac{\frac{\lceil n(1-l\rho)\rceil}{n} - (1-l\rho)}{l\rho}, \tag{D.33}$$

the expression in (D.31) is bounded below by

$$\inf_{\underline{\beta}\in\Delta_{k'}} \max\left\{\log\frac{|f'^{-1}(0)|}{\beta_0}, \theta_n \log\left(\theta_n\frac{|f'^{-1}(1)|}{\beta_1}\right) + (1-\theta_n)\log\left((1-\theta_n)\frac{|f'^{-1}(0)|}{\beta_0}\right)\right\}, \tag{D.34}$$

where the two terms within $\{\cdot\}$ in (D.34) are obtained by evaluating the term within $\{\cdot\}$ in (D.31) 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' (5.82) and $P_X\left(f'^{-1}\right) = \underline{\alpha}_t,\ t = 1, 2$.

For every $\underline{\beta} \in \Delta_{k'},\ \beta_2, \ldots, \beta_{k'-1}$ do not appear in (D.34), so that it suffices to consider $\underline{\beta} \in \Delta_{k'}$ that satisfies

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

whereby (D.34) becomes

$$\inf_{0\le\beta_0\le 1} \max\left\{\log\frac{|f'^{-1}(0)|}{\beta_0}, \theta_n\log\left(\theta_n\frac{|f'^{-1}(1)|}{1-\beta_0}\right)+(1-\theta_n)\log\left((1-\theta_n)\frac{|f'^{-1}(0)|}{\beta_0}\right)\right\}. \tag{D.35}$$

Observe that (D.35) is the same as (D.26) with μ_n replaced by θ_n and $\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$ by $|f'^{-1}(1)|$. Since, by the assumption in (5.13), $|f'^{-1}(0)|\ge|f'^{-1}(1)|$, applying the same steps from (D.26) - (D.28) for the case $l\le\lfloor\frac{k}{2}\rfloor$ and $|f'^{-1}(0)|\ge\sum_{j'=1}^{k'-l'-1}|f'^{-1}(j')|$, we get that (D.35) equals

$$\log|f'^{-1}(0)|+\log\left(1+\frac{|f'^{-1}(1)|}{|f'^{-1}(0)|}(1-\theta_n)^{\frac{1-\theta_n}{\theta_n}}\theta_n\right). \tag{D.36}$$

From[2] (D.36) and the fact that $(1-\theta_n)^{\frac{1-\theta_n}{\theta_n}}\ge 1/e$, we get the desired lower bound for (5.96) which along with (5.89) and (D.33) gives (5.85), (5.97), (5.98).

Proof of (5.64)**,** (5.65): To show (5.64), (5.65) for the case $l\le\lfloor\frac{k}{2}\rfloor$, we have from (D.16), (D.17) that

$$\begin{aligned}\min_{t=1,\dots,k'-l'}\underline{\alpha}_t(0) &= l\rho-\left(\min\left\{\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n},\ l\rho\right\}-l\left(\frac{1-l\rho}{k-l'-l}\right)\right)\\ &\ge l\rho-\left(\frac{\lceil nl\left(\frac{1-l\rho}{k-l'-l}\right)\rceil}{n}-l\left(\frac{1-l\rho}{k-l'-l}\right)\right)\\ &\ge l\rho-\frac{1}{n}\ge\frac{1}{2}-\frac{1}{n}\quad\text{since from (5.54), } l\rho\ge\frac{l}{l+1}\ge\frac{1}{2},\end{aligned}$$

[2]When $\theta_n=0$, the expression in (D.36) reduces to $\log|f^{-1}(0)|$.

so that the last inequality in (5.64) holds if

$$\frac{1}{2} - \frac{1}{n} - \frac{k'-1}{n} = \frac{1}{2} - \frac{k'}{n} \geq 0 \quad \text{i.e.,} \quad n \geq N_0(k') = 2k'. \tag{D.37}$$

Next, for the case $l > \left\lfloor \frac{k}{2} \right\rfloor$, from (D.32),

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

and, in this case too, (D.37) holds. ■

D.4. Proof of (5.104)

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

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

the left-side of (5.104) is maximized by P_X being a point-mass on any $x \in f^{-1}(0)$. Then, (5.104) holds with "$\leq$."

Next, the reverse inequality "$\geq$" in (5.104) obtains from mimicking the steps in (5.20) with $l = 1$. ■

D.5. Proof of Theorem 5.9

By Theorem 5.4, with $0.5 < \rho \leq 1$, we have for every $n \geq 1$ that

$$\pi_n(\rho) \leq \omega(\rho) + \Gamma_n(\rho) = \max_{j \in \{0,1\}} \log \left| f^{-1}(j) \right| + \Gamma_n(\rho), \tag{D.38}$$

where

$$\Gamma_n(\rho) = \sup_{V \in \mathcal{V}(\rho)} \sup_{\underline{\alpha} \in \Delta_k(V)} \sum_{Q^{(n)} \in \mathcal{Q}^{(n)}} \underline{\alpha}^n \left(\mathcal{T}_{Q^{(n)}} \right) \; D \left(\underline{\alpha} V^{-1} || \kappa_n \left(Q^{(n)} \right) \right). \tag{D.39}$$

Each $V \in \mathcal{V}(\rho)$ can be written as

$$V(0|0) = 1 - V(1|0) = \rho_0, \quad V(1|1) = 1 - V(0|1) = 1 - \rho_1, \quad \text{for some } \rho \leq \rho_0, \rho_1 \leq 1. \tag{D.40}$$

Then, $\underline{\alpha} = [1 - \alpha, \alpha] \in \Delta_2(V)$ must satisfy

$$1 - \rho_0 \leq \alpha \leq \rho_1, \tag{D.41}$$

since for any $\underline{\beta} = [1 - \beta, \beta] \in \Delta_2$ and $V \in \mathcal{V}(\rho)$ as in (D.40),

$$\underline{\alpha} = \underline{\beta} V = \left[1 - \left(\left(\rho_0 + \rho_1 + 1 \right) \beta + 1 - \rho_0 \right), \left(\rho_0 + \rho_1 + 1 \right) \beta + 1 - \rho_0 \right]$$

implies that

$$1 - \rho_0 \leq \alpha \leq \rho_1.$$

Moreover, in (D.39),

$$\underline{\alpha}V^{-1} = [1-\alpha \;\; \alpha]\begin{bmatrix} \rho_0 & 1-\rho_0 \\ 1-\rho_1 & \rho_1 \end{bmatrix}^{-1} = \left[1 - \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}, \;\; \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right]. \tag{D.42}$$

Also, $\mathcal{Q}^{(n)} = \left\{\left(1-\frac{i}{n}, \frac{i}{n}\right),\ 0 \le i \le n\right\}$. Using (D.40), (D.41) and (D.42) in (D.39), we get

$$\Gamma_n(\rho) = \sup_{\rho \le \rho_0, \rho_1 \le 1} \; \sup_{1-\rho_0 \le \alpha \le \rho_1} \sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha) = i\right) \; D\left(\text{Ber}\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right) \middle|\middle| \text{Ber}\left(\kappa_n(i)\right)\right), \tag{D.43}$$

where $\kappa_n(i) \triangleq \kappa_n\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right)$. For a given $V \in \mathcal{V}(\rho)$ in (D.40), we have from (5.26) that

$$\widetilde{Q}\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right) = \arg \min_{1-\rho_0 \le \alpha \le \rho_1} D\left(\text{Ber}\left(\frac{i}{n}\right) \middle|\middle| \text{Ber}\left(\alpha\right)\right), \quad 0 \le i \le n.$$

Clearly, when $1-\rho_0 \le \frac{i}{n} \le \rho_1$,

$$\widetilde{Q}\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right) = \arg \min_{1-\rho_0 \le \alpha \le \rho_1} D\left(\text{Ber}\left(\frac{i}{n}\right) \middle|\middle| \text{Ber}\left(\alpha\right)\right) = \frac{i}{n}, \quad 1-\rho_0 \le \frac{i}{n} \le \rho_1.$$

When $\frac{i}{n} > \rho_1$, note that for $\alpha \in [1-\rho_0, \rho_1]$,

$$\frac{d}{d\alpha} D\left(\text{Ber}\left(\frac{i}{n}\right) \middle|\middle| \text{Ber}\left(\alpha\right)\right) = \frac{1}{\ln 2}\left(\frac{1-\frac{i}{n}}{1-\alpha} - \frac{\frac{i}{n}}{\alpha}\right) < 0,$$

so that $D\left(\text{Ber}\left(\frac{i}{n}\right) \middle|\middle| \text{Ber}\left(\alpha\right)\right)$ is decreasing in $\alpha \in [1-\rho_0, \rho_1]$. Therefore,

$$\widetilde{Q}\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right) = \arg \min_{1-\rho_0 \le \alpha \le \rho_1} D\left(\text{Ber}\left(\frac{i}{n}\right) \middle|\middle| \text{Ber}\left(\alpha\right)\right) = \rho_1, \qquad \frac{i}{n} > \rho_1.$$

Similarly, when $\frac{i}{n} < 1-\rho_0$, we can show that $D\left(\text{Ber}\left(\frac{i}{n}\right)\middle|\middle|\text{Ber}\left(\alpha\right)\right)$ is increasing in $\alpha \in [1-\rho_0, \rho_1]$, and therefore,

$$\widetilde{Q}\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right) = \arg\min_{1-\rho_0 \le \alpha \le \rho_1} D\left(\text{Ber}\left(\frac{i}{n}\right)\middle|\middle|\text{Ber}\left(\alpha\right)\right) = 1-\rho_0, \quad \frac{i}{n} < 1-\rho_0.$$

Finally,

$$\widetilde{Q}\left(\left(1-\frac{i}{n}, \frac{i}{n}\right)\right) = \begin{cases} \rho_1, & \frac{i}{n} > \rho_1 \\ \frac{i}{n}, & 1-\rho_0 \le \frac{i}{n} \le \rho_1 \\ 1-\rho_0, & \frac{i}{n} < 1-\rho_0, \end{cases} \tag{D.44}$$

so that from (5.27), using (D.44),

$$\kappa_n(i) = \begin{cases} \frac{n+1}{n+2}, & \frac{i}{n} > \rho_1 \\ \frac{n\left(\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)+1}{n+2}, & 1-\rho_0 \le \frac{i}{n} \le \rho_1 \\ \frac{1}{n+2} & \frac{i}{n} < 1-\rho_0. \end{cases} \tag{D.45}$$

We have from (D.39),

$$\begin{aligned} \Gamma_n(\rho) \le & \sup_{\rho \le \rho_0, \rho_1 \le 1} \sup_{1-\rho_0 \le \alpha \le \rho_1} \sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha) = i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{\kappa_n(i)} \\ & + \sup_{\rho \le \rho_0, \rho_1 \le 1} \sup_{1-\rho_0 \le \alpha \le \rho_1} \sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha) = i\right) \left(1-\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right) \log \frac{1-\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{1-\kappa_n(i)}. \end{aligned} \tag{D.46}$$

We shall now obtain an upper bound on the first term of the right-side of (D.46).

By using (D.45) in the first term of the right-side of (D.46), we get

$$
\begin{aligned}
&\sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{\kappa_n(i)} \\
&= \sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{1}{\kappa_n(i)} + \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \\
&= P\left(\text{Bin}(n,\alpha)<n(1-\rho_0)\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log(n+2) \\
&+ \left(\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{1}{\kappa_n(i)} \right) \mathbb{1}\left(\lceil n(1-\rho_0)\rceil \le \lfloor n\rho_1\rfloor\right) \\
&+ P\left(\text{Bin}(n,\alpha)>n\rho_1\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{n+2}{n+1} + \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \\
&\le P\left(\text{Bin}(n,\alpha)\le \lceil n(1-\rho_0)\rceil\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log(n+2) \\
&+ \left(\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{1}{\kappa_n(i)} \right) \mathbb{1}\left(\lceil n(1-\rho_0)\rceil+1 \le \lfloor n\rho_1\rfloor\right) \\
&+ P\left(\text{Bin}(n,\alpha)>\lfloor n\rho_1\rfloor\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{n+2}{n+1} + \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}, \qquad \text{(D.47)}
\end{aligned}
$$

where the inequality above uses $\kappa_n\left(\lceil n(1-\rho_0)\rceil\right) \ge 1/(n+2)$ in (D.45). In (D.47), if $\lceil n(1-\rho_0)\rceil + 1 \le \lfloor n\rho_1\rfloor$, then

$$
\begin{aligned}
&\sup_{1-\rho_0\le\alpha\le\rho_1} \sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{1}{\kappa_n(i)} \\
&+ \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \\
&= \max\left\{ \sup_{1-\rho_0\le\alpha\le 1-\rho_0+\frac{1}{n}} \sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{1}{\kappa_n(i)} \right. \\
&\left. + \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}, \right.
\end{aligned}
$$

$$\sup_{1-\rho_0+\frac{1}{n}\le\alpha\le\rho_1} \sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}$$
$$+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\Bigg\}. \tag{D.48}$$

In the first term within $\{\cdot\}$ in (D.48), $\lceil n(1-\rho_0)\rceil+1 \le \lfloor n\rho_1\rfloor$ implies $1-\rho_0+\frac{1}{n}\le\rho_1\le 1$. Considering the first term within $\{\cdot\}$ in (D.48),

$$\begin{aligned}
&\sup_{1-\rho_0\le\alpha\le 1-\rho_0+\frac{1}{n}} \sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}\\
&+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&\le \sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right)\left(\frac{1-\rho_0+\frac{1}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)\log(n+2),\\
&\qquad\qquad \text{using (D.45) and } \alpha\le 1-\rho_0+\frac{1}{n}\\
&\le \frac{\log(n+2)}{(2\rho-1)n}, \qquad \text{since } \rho_0\ge\rho,\ \rho_1\ge\rho.
\end{aligned} \tag{D.49}$$

Next, in the second term within $\{\cdot\}$ in (D.48),

$$\begin{aligned}
&\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&=\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&+\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&+\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right) \left(-\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)\log\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}.
\end{aligned} \tag{D.50}$$

We claim that the sum of the second and fourth terms in the right-side of (D.50) has the following

upper bound:

$$\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}$$
$$+\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\left(-\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)\log\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\le\frac{\ln n+1}{2\ln 2(2\rho-1)\sqrt{n}}. \tag{D.51}$$

Next, considering the remaining two terms in the right-side of (D.50),

$$\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}$$
$$+\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}$$
$$=\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\left(\frac{1}{\kappa_n(i)}\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)+\right.$$
$$\left.\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)$$
$$+P\left(\mathrm{Bin}(n,\alpha)=\lceil n(1-\rho_0)\rceil\right)\frac{\frac{\lceil n(1-\rho_0)\rceil}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\frac{\lceil n(1-\rho_0)\rceil}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}$$
$$\le\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\alpha-\frac{i}{n}}{\rho_0+\rho_1-1}\log\frac{1}{\left(\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}$$
$$+\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\left(\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{\kappa_n(i)},$$
$$\text{since if } \lceil n(1-\rho_0)\rceil+1\le\lfloor n\rho_1\rfloor,\ \log\frac{\frac{\lceil n(1-\rho_0)\rceil}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\le 0$$
$$\le\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\left|\alpha-\frac{i}{n}\right|}{\rho_0+\rho_1-1}\log\frac{1}{\left(\frac{\frac{\lceil n(1-\rho_0)\rceil+1}{n}-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}$$
$$+\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\left(\frac{n+2}{n}\frac{i-n(1-\rho_0)}{i-n(1-\rho_0)+\rho_0+\rho_1-1}\right),$$

using (D.45)

$$\leq \frac{\log\left(n(\rho_0+\rho_1-1)\right)}{\rho_0+\rho_1-1}\sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha)=i\right)\left|\alpha-\frac{i}{n}\right|$$
$$+\log\frac{n+2}{n}\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}$$
$$\leq \frac{\log n}{2\rho-1}\mathbb{E}\left[\left|\alpha-\frac{\text{Bin}(n,\alpha)}{n}\right|\right]+\log\frac{n+2}{n}, \tag{D.52}$$

where the inequality in (D.52) is obtained using $\rho \leq \rho_0, \rho_1 \leq 1$ and the expectation is with respect to $\text{Bin}(n,\alpha)$. We have by Jensen's inequality [39] that

$$\mathbb{E}\left[\left|\alpha-\frac{\text{Bin}(n,\alpha)}{n}\right|\right] \leq \sqrt{\mathbb{E}\left[\left|\alpha-\frac{\text{Bin}(n,\alpha)}{n}\right|^2\right]} = \sqrt{\frac{\alpha(1-\alpha)}{n}}, \tag{D.53}$$

so that (D.52) is bounded above by

$$\leq \frac{\log n}{2(2\rho-1)\sqrt{n}}+\log\frac{n+2}{n}. \tag{D.54}$$

Using (D.49), (D.54) in (D.48), we get that if $\lceil n(1-\rho_0)\rceil+1 \leq \lfloor n\rho_1\rfloor$,

$$\sup_{1-\rho_0\leq\alpha\leq\rho_1}\sum_{i=\lceil n(1-\rho_0)\rceil+1}^{\lfloor n\rho_1\rfloor} P\left(\text{Bin}(n,\alpha)=i\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{1}{\kappa_n(i)}$$
$$+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}$$
$$\leq \max\left\{\frac{\log(n+2)}{(2\rho-1)n}, \frac{\ln n+1}{2\ln 2(2\rho-1)\sqrt{n}}+\frac{\log n}{2(2\rho-1)\sqrt{n}}+\log\frac{n+2}{n}\right\}. \tag{D.55}$$

Next, in (D.47),

$$
\begin{aligned}
& P\left(\text{Bin}(n,\alpha) \le \lceil n(1-\rho_0) \rceil\right) \ \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log(n+2) \\
& \le P\left(\text{Bin}(n,\alpha) \le n(1-\rho_0)+1\right) \ \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log(n+2) \\
& \le \exp^{\left[-2n\left(\alpha-(1-\rho_0)-\frac{1}{n}\right)^2\right]} \ \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log(n+2), \quad \text{using Hoeffding's inequality [36].}
\end{aligned}
\tag{D.56}
$$

Let $\alpha-(1-\rho_0) = t$ in (D.56). Straightforward calculations show that $\exp^{\left[-2n\left(t-\frac{1}{n}\right)^2\right]} t$ is maximized at $t = \frac{1+\sqrt{n+1}}{2n}$ and (D.56) is bounded above by

$$
\begin{aligned}
& \le \exp\left[\frac{\sqrt{n+1}}{n}-\frac{n+2}{2n}\right]\frac{1+\sqrt{n+1}}{2n}\frac{\log(n+2)}{2\rho-1}, \quad \text{since } \rho_1 \ge \rho,\ \rho_0 \ge \rho \\
& \le \exp\left[\frac{\sqrt{n+1}}{n}-\frac{n+2}{2n}\right]\frac{\sqrt{2n}+\sqrt{2n}}{2n}\frac{\log(n+2)}{2\rho-1} \\
& \le \exp\left[\frac{\sqrt{n+1}}{n}-\frac{n+2}{2n}\right]\frac{\sqrt{2}\log(n+2)}{(2\rho-1)\sqrt{n}}.
\end{aligned}
\tag{D.57}
$$

Finally, in (D.47),

$$
P\left(\text{Bin}(n,\alpha) > \lfloor n\rho_1 \rfloor\right)\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{n+2}{n+1} \le \log\frac{n+2}{n+1}. \tag{D.58}
$$

Using (D.55), (D.57) and (D.58) in (D.47), the first term in the right-side of (D.46) is bounded above by

$$
\sup_{\rho\le\rho_0,\rho_1\le 1}\ \sup_{1-\rho_0\le\alpha\le\rho_1}\ \sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha)=i\right)\ \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{\kappa_n(i)}
$$

$$
\begin{aligned}
&\leq \exp\left[\frac{\sqrt{n+1}}{n} - \frac{n+2}{2n}\right] \frac{\sqrt{2}\log(n+2)}{(2\rho-1)\sqrt{n}} \\
&+ \max\left\{\frac{\log(n+2)}{(2\rho-1)n}, \frac{\ln n + 1}{2\ln 2(2\rho-1)\sqrt{n}} + \frac{\log n}{2(2\rho-1)\sqrt{n}} + \log\frac{n+2}{n}\right\} \\
&\times \mathbb{1}\left(\lceil n(1-\rho_0)\rceil + 1 \leq \lfloor n\rho_1 \rfloor\right) + \log\frac{n+2}{n+1} \\
&\leq \max\left\{\frac{\log(n+2)}{(2\rho-1)n}, \frac{\ln n + 1}{2\ln 2(2\rho-1)\sqrt{n}} + \frac{\log n}{2(2\rho-1)\sqrt{n}} + \log\frac{n+2}{n}\right\} \\
&+ \exp\left[\frac{\sqrt{n+1}}{n} - \frac{n+2}{2n}\right] \frac{\sqrt{2}\log(n+2)}{(2\rho-1)\sqrt{n}} + \log\frac{n+2}{n+1}.
\end{aligned} \tag{D.59}
$$

Turning to the second term in the right-side of (D.46),

$$
\begin{aligned}
&\sup_{\rho\leq\rho_0,\rho_1\leq 1} \sup_{1-\rho_0\leq\alpha\leq\rho_1} \sum_{i=0}^{n} P\left(\mathrm{Bin}(n,\alpha)=i\right) \left(1 - \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right) \log\frac{1-\left(\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\right)}{1-\kappa_n(i)} \\
&= \sup_{\rho\leq\rho_0,\rho_1\leq 1} \sup_{1-\rho_0\leq\alpha\leq\rho_1} \sum_{i=0}^{n} P\left(\mathrm{Bin}(n,1-\alpha)=i\right) \frac{(1-\alpha)-(1-\rho_1)}{\rho_0+\rho_1-1} \log\frac{\left(\frac{(1-\alpha)-(1-\rho_1)}{\rho_0+\rho_1-1}\right)}{1-\kappa_n(i)}.
\end{aligned} \tag{D.60}
$$

In (D.60), let $\hat{i} = n - i$ and $\hat{\alpha} = 1 - \alpha$. Then, (D.60) is

$$
\sup_{\rho\leq\rho_0,\rho_1\leq 1} \sup_{1-\rho_1\leq\hat{\alpha}\leq\rho_0} \sum_{\hat{i}=0}^{n} P\left(\mathrm{Bin}(n,\hat{\alpha})=\hat{i}\right) \frac{\hat{\alpha}-(1-\rho_1)}{\rho_0+\rho_1-1} \log\frac{\left(\frac{\hat{\alpha}-(1-\rho_1)}{\rho_0+\rho_1-1}\right)}{1-\kappa_n(n-\hat{i})}. \tag{D.61}
$$

Observe from (D.45) that

$$
1-\kappa_n(n-\hat{i}) = \begin{cases} \frac{n+1}{n+2}, & \frac{\hat{i}}{n} > \rho_0 \\ \frac{n\left(\frac{\frac{\hat{i}}{n}-(1-\rho_1)}{\rho_0+\rho_1-1}\right)+1}{n+2}, & 1-\rho_1 \leq \frac{\hat{i}}{n} \leq \rho_0 \\ \frac{1}{n+2} & \frac{\hat{i}}{n} < 1-\rho_1. \end{cases}
$$

Therefore (D.61) is identical to the first term in the right-side of (D.46) with ρ_0 and ρ_1 interchanged and hence is also bounded above by (D.59). Finally, we get that

$$\Gamma_n(\rho) \leq 2 \max \left\{ \frac{\log(n+2)}{(2\rho-1)n}, \frac{\ln n + 1}{2 \ln 2 (2\rho-1)\sqrt{n}} + \frac{\log n}{2(2\rho-1)\sqrt{n}} + \log \frac{n+2}{n} \right\} + \exp\left[\frac{\sqrt{n+1}}{n} - \frac{n+2}{2n} \right] \frac{2\sqrt{2}\log(n+2)}{(2\rho-1)\sqrt{n}} + 2 \log \frac{n+2}{n+1},$$

which along with (D.38) yield (5.102), (5.103).

It remains to show the claim (D.51). Given $\rho_0, \rho_1 \geq \rho > 0.5$, let $q_\alpha : [1-\rho_0, \rho_1] \to \mathbb{R}$ be the first order Taylor polynomial of

$$-\frac{y-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{y-(1-\rho_0)}{\rho_0+\rho_1-1}, \quad 1-\rho_0 \leq y \leq \rho_1,$$

at $1-\rho_0+\frac{1}{n} \leq \alpha \leq \rho_1$, given by

$$q_\alpha(y) = -\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} - \frac{\ln \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} + 1}{\ln 2(\rho_0+\rho_1-1)}(y-\alpha), \quad 1-\rho_0 \leq y \leq \rho_1. \tag{D.62}$$

The left-side of (D.51) is

$$\begin{aligned} &\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1} \\ &- \sum_{i=\lceil n(1-\rho_0) \rceil}^{\lfloor n\rho_1 \rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right) \frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1} \\ &= \sum_{i=\lceil n(1-\rho_0) \rceil}^{\lfloor n\rho_1 \rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right) \left(-\frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1} \log \frac{\frac{i}{n}-(1-\rho_0)}{\rho_0+\rho_1-1} - q_\alpha\left(\frac{i}{n}\right) \right) \end{aligned} \tag{D.63}$$

$$+\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ q_\alpha\left(\frac{i}{n}\right)+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}. \tag{D.64}$$

Since $-\frac{y-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{y-(1-\rho_0)}{\rho_0+\rho_1-1}$ is a concave function of $1-\rho_0\le y\le\rho_1$, using [11, Lemma 2],

$$-\frac{y-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{y-(1-\rho_0)}{\rho_0+\rho_1-1}-q_\alpha(y)\le 0,$$

so that (D.64) is bounded above by

$$\begin{aligned}
&\sum_{i=\lceil n(1-\rho_0)\rceil}^{\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ q_\alpha\left(\frac{i}{n}\right)+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&=\sum_{i=0}^{n} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ q_\alpha\left(\frac{i}{n}\right)+\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\\
&-\sum_{i:i<\lceil n(1-\rho_0)\rceil\ \vee\ i>\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ q_\alpha\left(\frac{i}{n}\right).
\end{aligned} \tag{D.65}$$

From (D.62),

$$q_\alpha(y)\ge-\frac{\left|\ln\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}+1\right|\,|y-\alpha|}{\ln 2\,(\rho_0+\rho_1-1)}$$

and

$$\sum_{i=0}^{n} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ q_\alpha\left(\frac{i}{n}\right)=-\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}\log\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1},$$

from which (D.65) is bounded above by

$$\begin{aligned}
&\left(\sum_{i:i<\lceil n(1-\rho_0)\rceil\ \vee\ i>\lfloor n\rho_1\rfloor} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ \left|\frac{i}{n}-\alpha\right|\right)\ \frac{\left|\ln\frac{\alpha-(1-\rho_0)}{\rho_0+\rho_1-1}+1\right|}{\ln 2\,(\rho_0+\rho_1-1)}\\
&\le\left(\sum_{i=0}^{n} P\left(\mathrm{Bin}(n,\alpha)=i\right)\ \left|\frac{i}{n}-\alpha\right|\right)\ \frac{\ln\frac{\rho_0+\rho_1-1}{\alpha-(1-\rho_0)}+1}{\ln 2\,(\rho_0+\rho_1-1)}
\end{aligned}$$

$$\leq \left(\sum_{i=0}^{n} P\left(\text{Bin}(n,\alpha) = i\right) \left| \frac{i}{n} - \alpha \right| \right) \frac{\ln n + 1}{\ln 2\,(2\rho - 1)}, \tag{D.66}$$

where the inequality in (D.66) uses $1 \geq \rho_0, \rho_1 \geq \rho$ and $\alpha \geq 1 - \rho_0 + \frac{1}{n}$. Next, using (D.53) in (D.66) we get that (D.66) is bounded above by

$$\leq \frac{\ln n + 1}{2 \ln 2\,(2\rho - 1)\sqrt{n}}$$

which completes the proof. ■

Bibliography

[1] J. Acharya, Y. Liu and Z. Sun, "Discrete distribution estimation under user-level local differential privacy," in *International Conference on Artificial Intelligence and Statistics*, vol. 206, 2023.

[2] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *ACM SIGMOD International Conference on Management of Data*, pp. 439-450, May 2000.

[3] S. Asoodeh, F. Alajaji and T. Linder, "Privacy-aware MMSE estimation," in *IEEE International Symposium on Information Theory (ISIT),* pp. 1989-1993, July 2016.

[4] S. Asoodeh, M. Diaz, F. Alajaji and T. Linder, "Information extraction under privacy constraints," *Information*, 2016; 7(1):15.

[5] S. Asoodeh, M. Diaz, F. Alajaji and T. Linder, "Estimation efficiency under privacy constraints," *IEEE Transactions on Information Theory,* vol. 65, no. 3, pp. 1512 - 1534, 2019.

[6] R. Bassily, A. Groce, J. Katz and A. Smith, "Coupled-world privacy: Exploiting adversarial uncertainty in statistical data privacy," in *Foundations of Computer Science*, pp. 439-448, Oct. 2013.

[7] R. Bassily and A. Smith, "Local, private, efficient protocols for succinct histograms," in *ACM Symposium on Theory of Computing*, pp. 127-135, June 2015.

[8] A. Blum, C. Dwork, F. McSherry and K. Nissim, "Practical privacy: The SuLQ framework," in *ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp 128-138, June 2005.

[9] A. Blum, K. Ligett and A. Roth, "A learning theory approach to non-interactive database privacy," in *ACM Symposium on Theory of Computing,* pp 609-618, May 2008.

[10] D. Braess, J. Forster, T. Sauer and H.U. Simon, "How to achieve minimax expected Kullback-Leibler distance from an unknown finite distribution," in *International Conference on Algorithmic Learning Theory*, pp. 380-394, Nov. 2002.

[11] D. Braess and T. Sauer, "Bernstein polynomials and learning theory," *Journal of Approximation Theory,* vol. 128, pp. 187-206, April 2004.

[12] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Allerton Conference on Communication, Control and Computing,* pp. 1401-1408, Oct. 2012.

[13] F. du Pin Calmon, A. Makhdoumi, M. Médard, M. Varia, M. Christiansen, and K. R. Duffy, "Principal inertia components and applications," *IEEE Transactions on Information Theory*, vol. 63, no. 8, pp. 5011–5038, 2017.

[14] T. H. Chan, M. Li, E. Shi, and W. Xu, "Differentially private continual monitoring of heavy hitters from distributed streams," in *International Conference on Privacy Enhancing Technologies Privacy Enhancing Technologies*, pp. 140–159, July 2012.

[15] W. N. Chen, P. Kairouz and A. Özgür, "Breaking the communication-privacy-accuracy trilemma," *IEEE Transactions on Information Theory,* vol. 69, no. 2, pp. 1261-1281, Feb. 2023.

[16] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *Annals of Statistics*, vol. 23, pp. 493-507, Dec. 1952.

[17] T.M. Cover, "Admissibility properties of Gilbert's encoding for unknown source probabilities," *IEEE Transactions on Information Theory*, pp. 216-217, Jan 1972.

[18] T.M. Cover and J.A. Thomas, *Elements of information theory*, 2nd edition, Wiley, 2006.

[19] I. Csiszár and P. C. Shields, "Information theory and statistics: A tutorial," *Foundations and Trends in Communications and Information Theory*, vol. 1, no. 4, pp 417-528, 2004.

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

[21] L. Devroye, "The equivalence in L1 of weak, strong and complete convergence of kernel density estimates," *Annals of Statistics*, vol. 11, pp. 896-904, Dec 1984.

[22] M. Diaz, P. Kairouz, J. Liao and L. Sankar, "Neural network-based estimation of the MMSE," in *IEEE International Symposium on Information Theory*, pp. 1023-1028, 2021.

[23] M. Diaz, H. Wang, F. P. Calmon and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 1949-1978, April 2020.

[24] J. C. Duchi, M. J. Wainwright and M. I. Jordan, "Local privacy and minimax bounds: Sharp rates for probability Estimation," in *Advances in Neural Information Processing Systems,* pp. 1529–1537, 2013.

[25] G. T. Duncan and D. Lambert, "Disclosure-limited data dissemination," *Journal of the American Statistical Association*, vol. 81, no. 393, pp. 25-27, March 1986.

[26] C. Dwork, "Differential privacy," in *International Colloquium on Automata, Languages and Programming,* pp 1-12, Springer, July 2006.

[27] C. Dwork, F. McSherry, K. Nissim and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference,* pp. 265-284, Springer, 2006.

[28] U. Erlingsson, V. Pihur and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *ACM SIGSAC Conference on Computer and Communications Security*, pp. 1054–1067, Nov. 2014.

[29] T. van Erven and P. Harremöes, "Rényi divergence and Kullback-Leibler divergence," *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3797-3820, July 2014.

[30] A. Evfimievski, R. Agrawal, R. Srikant and J. Gehrke, "Privacy preserving mining of association rules," in *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 217-228, July 2002.

[31] A. Evfimievski, J. Gehrke and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," in *ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 211-222, June 2003.

[32] S. E. Fienberg, U. E. Makov and R. J. Steele, "Disclosure limitation using perturbation and related methods for categorical data," *Journal of Official Statistics*, vol. 14, no. 4, pp. 485-502, Dec. 1998.

[33] Q. Geng, W. Ding, R. Guo and S. Kumar, "Tight analysis of privacy and utility tradeoff in approximate differential privacy," in *International Conference on Artificial Intelligence and Statistics,* pp. 89-99, 2020.

[34] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory,* vol. 62, no. 2, pp. 925-951, Feb. 2016.

[35] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *ACM Symposium on Theory of Computing*, pp. 705-714, June 2010.

[36] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association,* vol. 58, no. 301, pp. 13–30, 1963.

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

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

[39] J. L. W. V. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Mathematica*, 30 (1): 175–193, 1906.

[40] P. Kairouz, K. Bonawitz and D. Ramage, "Discrete distribution estimation under local privacy," in *International Conference on Machine Learning*, pp. 2436-2444, June 2016.

[41] P. Kairouz, S. Oh and P. Viswanath, "Extremal mechanisms for local differential privacy," in *Advances in Neural Information Processing Systems*, pp. 2879–2887, Dec. 2014.

[42] P. Kairouz, S. Oh and P. Viswanath, "The composition theorem for differential privacy," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 4037-4049, June 2017.

[43] S. Kamath, A. Orlitsky, V. Pichapati, and A. T. Suresh, "On learning distributions from their samples," in *Conference on Learning Theory*, pp. 1066-1100, July 2015.

[44] F. Kanaya and T. S. Han, "The asymptotics of posterior entropy and error probability for bayesian estimation," *IEEE Transactions on Information Theory,* vol. 41, no. 6, pp. 1988-1992, Nov. 1995.

[45] S. P. Kasivisiwanathan and A. Smith, "On the semantics of differential privacy: A Bayesian formulation," *Journal of Privacy and Confidentiality,* vol. 6, no. 1, Aug. 2014.

[46] R.E. Krichevsky, "The performance of universal encoding," *IEEE Transactions on Information Theory*, vol. 27, no. 2, pp. 199-207, March 1998.

[47] N. Li, T. Li and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *IEEE International Conference on Data Engineering*, pp. 106-115, April 2007.

[48] A. Makhdoumi and N. Fawaz, "Privacy-utility tradeoff under statistical uncertainty," in *Allerton Conference on Communication, Control and Computing*, pp. 1627-1634, 2013.

[49] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Symposium on Foundations of Computer Science*, pp. 94-103, Oct. 2007.

[50] I. Mironov, "Rényi differential privacy," in *IEEE Computer Security Foundations Symposium*, pp. 263-275, 2017.

[51] N. Morača, "Bounds for norms of the matrix inverse and the smallest singular value," *Linear Algebra and its Applications*, vol. 429, pp. 2589-2601, 2008.

[52] A. Nageswaran, "Gaussian data privacy under linear function recoverability," in *IEEE International Symposium on Information Theory*, pp. 632-636, June 2022.

[53] A. Nageswaran, "Gaussian data privacy under linear function recoverability," submitted to *IEEE Transactions on Information Theory*, 2023.

[54] A. Nageswaran and P. Narayan, "Data privacy for a ρ-recoverable function," in *IEEE International Symposium on Information Theory*, pp. 1046-1050, June 2018.

[55] A. Nageswaran and P. Narayan, "Data privacy for a ρ-recoverable function," *IEEE Transactions on Information Theory*, vol. 65, no. 6, pp. 3470-3488, June 2019.

[56] A. Nageswaran and P. Narayan, "Predicate privacy and list privacy for a ρ-recoverable function," in *IEEE International Symposium on Information Theory*, pp. 2139-2143, July 2019.

[57] A. Nageswaran and P. Narayan, "'Distribution privacy under function recoverability," in *IEEE International Symposium on Information Theory*, pp. 890-895, June 2020.

[58] A. Nageswaran and P. Narayan, "Distribution privacy under function ρ-recoverability," in *IEEE International Symposium on Information Theory*, pp. 3332-333, July 2021.

[59] A. Nageswaran and P. Narayan, "Distribution privacy under function recoverability," *IEEE Transactions on Information Theory*, vol. 68, no. 5, pp. 3317-3339, May 2022.

[60] A. Nageswaran and P. Narayan, "List privacy under function recoverability," submitted to *IEEE Transactions on Information Theory*, 2023.

[61] L. Paninski, "Variational minimax estimation of discrete distributions under KL loss," in *Neural Information Processing Systems*, pp.1033–1040, Dec 2004.

[62] A. Pastore and M. Gastpar, "Locally differentially-private randomized response for discrete distribution learning," *Journal on Machine Learning Research*, vol. 22, pp. 1-56, July 2021.

[63] A. R. Rao and P. Bhimasankaram, *Linear Algebra*, 2nd edition, Hindustan Book Agency, 2000.

[64] D. Rebollo-Monedero, J. Forné and J. Domingo-Ferrer, "From t-closeness-like privacy to postrandomization via information theory," *IEEE Transactions on Knowledge and Data Engineering*, pp. 1623-1636, 2010.

[65] A. Rényi, "On measures of entropy and information," in *Berkeley Symposium on Mathematical Statistics and Probability*, vol. 1, pp. 547-561, July 1961.

[66] L. Sankar, S. R. Rajagopalan and H. V. Poor, "Utility-privacy tradeoff in databases: An information-theoretic approach," *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 6, 2013.

[67] C. Schieler and P. Cuff, "The henchman problem: Measuring secrecy by the minimum distortion in a list," *IEEE Transactions on Information Theory,* vol. 62, no. 6, pp. 3436-3450, 2016.

[68] A. Smith, "Privacy-preserving statistical estimation with optimal convergence rates," in *ACM Symposium on Theory of Computing*, pp. 813-822, June 2011.

[69] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 5, pp. 557-570, Oct. 2002.

[70] H. Tyagi, Personal communication, 2018.

[71] H. Tyagi, Personal communication, 2023.

[72] J.M. Varah, "A lower bound for the smallest singular value of a matrix," *Linear Algebra and its Applications,* vol. 11, pp. 3-5, 1975.

[73] L. Wasserman and S. Zhou, "A statistical framework for differential privacy," *Journal of the American Statistical Association,* vol. 105, pp. 375-389, 2010.

[74] Y. Wang, S. Aeron, A. S. Rakin, T. Koike-Akino and P. Moulin, "Robust machine learning via privacy/ rate-distortion theory," in *IEEE International Symposium on Information Theory*, pp. 1320-1325, 2021.

[75] Y. Wu and S. Vérdu, "Functional properties of minimum mean-square error and mutual information," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1289-1301, March 2012.

[76] M. Ye and A. Barg, "Optimal schemes for discrete distribution estimation under locally differential privacy," *IEEE Transactions on Information Theory*, vol. 64, no. 8, pp. 5662-5676, Aug. 2018.

[77] R. Zamir, "A proof of the Fisher information inequality via a data processing argument," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1246-1250, May 1998.