Justification of Logarithmic Loss via the Benefit of Side Information
Jiantao Jiao, Student Member, IEEE, Thomas A. Courtade, Member, IEEE, Kartik Venkat, Student Member, IEEE, and Tsachy Weissman, Fellow, IEEE

Abstract—We consider a natural measure of relevance: the reduction in optimal prediction risk in the presence of side information. For any given loss function, this relevance measure captures the benefit of side information for performing inference on a random variable under this loss function. When such a measure satisfies a natural data processing property, and the random variable of interest has alphabet size greater than two, we show that it is uniquely characterized by the mutual information, and the corresponding loss function coincides with logarithmic loss. In doing so, our work provides a new characterization of mutual information, and justifies its use as a measure of relevance. When the alphabet is binary, we characterize the only admissible forms the measure of relevance can assume while obeying the specified data processing property. Our results naturally extend to measuring the causal influence between stochastic processes, where we unify different causality measures in the literature as instantiations of directed information.

Index Terms—Axiomatic characterizations, causality measures, data processing, directed information, logarithmic loss.

I. INTRODUCTION

IN STATISTICAL decision theory, it is often a controversial issue to choose the appropriate loss function. One popular loss function is called logarithmic loss, defined as follows. Let \( \mathcal{X} = \{x_1, x_2, \ldots, x_n\} \) be a finite set with \( |\mathcal{X}| = n \), let \( \Gamma_n \) denote the set of probability measures on \( \mathcal{X} \), and let \( \mathbb{R} \) denote the extended real line.

Definition 1 (Logarithmic Loss): Logarithmic loss \( \ell_{\log} : \mathcal{X} \times \Gamma_n \to \mathbb{R} \) is defined by

\[
\ell_{\log}(x, P) = \log \frac{1}{P(x)},
\]

where \( P(x) \) denotes the probability of \( x \) under measure \( P \).

Logarithmic loss has enjoyed numerous applications in various fields. For instance, its usage in statistics dates back to Good [1], and it has found a prominent role in learning.

Manuscript received March 20, 2015; revised May 21, 2015; accepted July 7, 2015. Date of publication July 30, 2015; date of current version September 11, 2015. This work was supported in part by the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-0939370. Jiantao Jiao and Kartik Venkat were partially supported by two Stanford Graduate Fellowships. The material in this paper was presented in part at the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA.

J. Jiao, K. Venkat, and T. Weissman are with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA (e-mail: jiantao@stanford.edu; kvenkat@stanford.edu; tsachy@stanford.edu).

T. Courtade is with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720 USA (e-mail: courtade@eecs.berkeley.edu).

Communicated by H. H. Permuter, Associate Editor for Shannon Theory. Digital Object Identifier 10.1109/TIT.2015.2462848

of quantifying the predictive benefit of side information is closely connected to the notion of proper scoring rules and the literature on probability forecasting in statistics. The survey by Gneiting and Raftery [7] provides a good overview.

Having introduced the yardstick in (2), we now reformulate the question of interest: Which loss function(s) \( \ell \) can be used to define \( C(\ell, P_{XY}) \) in a meaningful way? Of course, “meaningful” is open to interpretation, but it is desirable that \( C(\ell, P_{XY}) \) be well-defined, at minimum. This motivates the following axiom:

**Data Processing Axiom:** For all distributions \( P_{XY} \), the quantity \( C(\ell, P_{XY}) \) satisfies

\[
C(\ell, P_{T_1 Y}) \leq C(\ell, P_{XY})
\]

whenever \( T(X) \in X \) is a statistically sufficient transformation of \( X \) for \( Y \).

We remind the reader that the statement ‘\( T \) is a statistically sufficient transform of \( X \) for \( Y \)’ means that the following two Markov chains hold:

\[
T \rightarrow X \rightarrow Y, \quad X \rightarrow T \rightarrow Y
\]

That is, \( T(X) \) preserves all of the information \( X \) contains about \( Y \).

In words, the Data Processing Axiom stipulates that processing the data \( X \rightarrow T \) cannot boost the predictive benefit of the side information.\(^1\)

To convince the reader that the Data Processing Axiom is a natural requirement, suppose instead that the Data Processing Axiom did not hold. Since \( X \) and \( T \) are mutually sufficient statistics for \( Y \), this would imply that there is no unique value which quantifies the benefit of side information \( Y \) for the random variable of interest. Thus, the Data Processing Axiom is needed for the benefit of side information to be well-defined.

Although the Data Processing Axiom may seem to be a benign requirement, it has far-reaching implications for the form \( C(\ell, P_{XY}) \) can take. This is captured by our first main result:

**Theorem 1:** Let \( n \geq 3 \). Under the Data Processing Axiom, the function \( C(\ell, P_{XY}) \) is uniquely determined by the mutual information,

\[
C(\ell, P_{XY}) = I(X; Y),
\]

up to a multiplicative factor.

The following corollary immediately follows from Theorem 1.

**Corollary 1:** Let \( n \geq 3 \). Under the Data Processing Axiom, the benefit of additional side information \( Y \) for inference on \( X \) with common side information \( W \), i.e.

\[
\inf_{\hat{X}_1(W)} \mathbb{E}_P[\ell(X, \hat{X}_1)] - \inf_{\hat{X}_2(W)} \mathbb{E}_P[\ell(X, \hat{X}_2)],
\]

is uniquely determined by the conditional mutual information,

\[
I(X; Y|W),
\]

up to a multiplicative factor.

\(^1\)In fact, the Data Processing Axiom is weaker than this general data processing statement since it only addresses statistically sufficient transformations of \( X \).

Thus, up to a multiplicative factor, we see that logarithmic loss generates the only measure of predictive benefit (defined according to (2)) which satisfies the Data Processing Axiom. In other words, Theorem 1 provides a definitive answer to Question 1 under the framework we have described, and also highlights the special role played by logarithmic loss.

Theorem 1 shows that mutual information uniquely quantifies the reduction of prediction risk due to side information. Note that the characterization of mutual information afforded by Theorem 1 does not explicitly require any of the mathematical properties of mutual information, such as the chain rule, or invariance to one-to-one transformations of both \( X \) and \( Y \). Thus, beyond the operational implications of our result, Theorem 1 has strong implications for axiomatic characterization of information measures from a mathematical standpoint. On this point, we note that Csiszár, in his survey [8] names the axiomatic result of Aczél et al. [9] as “intuitively most appealing” in characterizing the entropy in terms of symmetry, expansibility, additivity, and subadditivity, whereas most other known characterizations require recursivity or the sum property. For details we refer to Csiszár [8].

Theorem 1 provides a partial explanation for why mutual information is widely used as an inferential tool across various applications in science and engineering, and is deeply imbedded in fundamental concepts in various disciplines. In statistics, one of the popular criteria for objective Bayesian modeling [10] is to design a prior on the parameter to maximize the mutual information between the parameter and the observations. In machine learning, the so-called *infomax* [11] criterion states that the function that maps a set of input values to a set of output values should be chosen or learned so as to maximize the mutual information between the input and output, subject to a set of specified constraints. This principle has been widely adopted in practice, for example, in decision tree based algorithms in machine learning such as C4.5 [12], one tries to select the feature at each step of tree splitting to maximize the mutual information (called *information gain* principle [13]) between the output and the feature conditioned on previous chosen features. In some applications, mutual information arises naturally as the only answer, for example, the well known Chow–Liu algorithm [14] for learning tree graphical models relies on estimation of the mutual information, which is a natural consequence of maximum likelihood estimation. We also mention genetics [15], image processing [16], computer vision [17], secrecy [18], ecology [19], and physics [20] as fields in which mutual information is widely used. Erkip and Cover [21] argued that mutual information is a natural quantity in the context of portfolio theory, where it emerges as the increase in growth rate due to the presence of side information.

Mutual information and related information theoretic measures are instrumental in various applications. This motivates investigating optimal estimators for these quantities based on data. There exist extensive literature on this subject, and we refer to [22] for a detailed review, as well as the theory and Matlab/Python implementations of entropy and mutual information estimators that achieve the minimax rates in all the regimes of sample size and support size pairs. For the
recent growing literature on information measure estimation in the high-dimensional regime, we refer to [22]–[29].

Interestingly, the assumption that \( n \geq 3 \) in Theorem 1 is essential. When the alphabet of \( X \) is binary, i.e. \( n = 2 \), the Data Processing Axiom no longer mandates the use of logarithmic loss. We have an explicit characterization for the form the measure of relevance (2) can take. The class of solutions for the binary alphabet setting is characterized by the following theorem.

**Theorem 2:** Let \( n = 2 \). Under the Data Processing Axiom, \( C(\ell, P_{XY}) \) must be of the form

\[
C(\ell, P_{XY}) = \sum_y p_y G(p_{X|y}) - G(p_X),
\]

where \( G((p, 1-p)) : \Gamma_2 \to \mathbb{R} \) is a symmetric (invariant to permutations), convex function. Moreover, for any symmetric convex function \( G((p, 1-p)) : \Gamma_2 \to \mathbb{R} \), there exists a loss function \( \ell \) whose corresponding \( C(\ell, P_{XY}) \) satisfies the Data Processing Axiom and is given by (8).

It is worth mentioning that there is an interesting set of observations surrounding the characterization of information measures which is sensitive to the alphabet size being binary or larger. This phenomenon is explored further in [30].

The rest of this paper is organized as follows. In Section III, we explore the connections between our results and the existing literature on causal analysis, including Granger and Sims causality, Geweke’s measure, transfer entropy, and directed information. The proofs of Theorems 1 and 2 are provided in Section IV. Proofs of some auxiliary lemmas are deferred to the appendix.

### III. Causality Measures: An Axiomatic Viewpoint

Inferring causal relationships from observed data plays an indispensable part in scientific discovery. Granger, in his seminal work [31], proposed a predictive test for inferring causal relationships. To state his test, let \( X_t, Y_t, U_t \) be stochastic processes, where \( X_t, Y_t \) are the processes of interest, and \( U_t \) contains all information in the universe accumulated up to time \( t \). Granger’s causality test asserts that \( Y_t \) causes \( X_t \), denoted by \( Y_t \Rightarrow X_t \), if we are better able to predict \( X_t \) using the past information of \( U_t \) than by using all past information in \( U_t \) apart from \( Y_t \). In Granger’s definition, the quality of prediction is measured by the squared error risk achieved by the optimal unbiased least-squares predictor.

In his 1980 paper, Granger [32] introduced a set of operational definitions which made it possible to derive practical testing procedures. For example, he assumes that we must be able to specify \( U_t \) in order to perform causality tests, which is slightly different from his original definition which required knowledge of all information in the universe (which is usually unavailable).

Later, Sims [33] introduced a related concept of causality, which was proved to be equivalent to Granger’s definition in Sims [33], Hosoya [34], and Chamberlain [35] in a variety of settings.

Motivated by Granger’s framework for testing causality using linear prediction, Geweke [36], [37] proposed a causality measure to quantify the extent to which \( Y \) is causing \( X \). Quoting Geweke (emphasis ours):

“The empirical literature abounds with tests of independence and unidirectional causality for various pairs of time series, but there have been virtually no investigations of the degree of dependence or the extent of various kinds of feedback. The latter approach is more realistic in the typical case in which the hypothesis of independence of unidirectional causality is not literally entertained, but it requires that one be able to measure linear dependence and feedback.”

In other words, Geweke makes the important distinction between a causality test which makes a binary decision on whether one process causes another, and a causality measure which quantifies the degree to which one process causes another. Geweke proposed the following measure as a natural starting point:

\[
F_{Y \Rightarrow X} \triangleq \ln \frac{\sigma^2(X_t|Y^{t-1})}{\sigma^2(X_t|X^{t-1}, Y^{t-1})},
\]

where \( \sigma^2(X_t|Y^{t-1}, Y^{t-1}) \) is the variance of the prediction residue when predicting \( X_t \) via the optimal linear predictor constructed from observation \( X^{t-1}, Y^{t-1} \). Note that if \( F_{Y \Rightarrow X} > 0 \), we could conclude \( Y_t \Rightarrow X_t \) according to Granger’s test.

It has long been observed that the restriction to optimal linear predictors in testing causality is not necessary. In fact, Chamberlain [35] proved a general equivalence between Granger and Sims’ causality tests by replacing linear predictors with conditional independence tests. However, the natural generalization of (9) wasn’t clear until Gourieroux et al. [38] proposed the so-called *Kullback causality measures* in 1987. It is now well-known that Kullback causality measures are equivalent to (9) under linear Gaussian models (e.g. Barnett et al. [39]).

Using information theoretic terms, Kullback causality measures are nothing but the directed information introduced by Massey [40], and motivated by Marko [41]. Using modern notation, the directed information from \( X^n \) to \( Y^n \) is defined as

\[
I(X^n \rightarrow Y^n) \triangleq \sum_{i=1}^n I(X^i; Y^i|Y^{i-1})
\]

\[= H(Y^n) - H(Y^n|X^n), \]

where \( H(Y^n|X^n) \) is the causally conditional entropy, defined by

\[
H(Y^n|X^n) \triangleq \sum_{i=1}^n H(Y_i|Y^{i-1}, X^i).
\]

Massey and Massey [42] established the pleasing conservation law of directed information:

\[
I(X^n; Y^n) = I(X^n \rightarrow Y^n) + I(Y^{n-1} \rightarrow X^n)
\]

\[= I(X^{n-1} \rightarrow Y^n) + I(Y^{n-1} \rightarrow X^n)
\]

\[+ \sum_{i=1}^n I(X_i; Y_i|X^{i-1}, Y^{i-1}), \]

where \( I(X; Y|Z) \) stands for the directed information between \( X \) and \( Y \) conditional on \( Z \).
which implies that the extent to which process $X_t$ influences process $Y_t$ and vice-versa always sum to the total mutual information between the two processes. Since $I(Y^{n-1} \to X^n)$ can be expressed as

$$I(Y^{n-1} \to X^n) = \sum_{i=1}^{n} H(X_i|X_{i-1}^{i-1}) - H(X_i|X_{i-1}^{i-1}, Y_{i-1}^{i-1}),$$

$X_i$ being conditionally independent of $Y_{i-1}$ given $X_{i-1}$ is equivalent to $I(Y^{n-1} \to X^n) = 0$. This corresponds precisely to the definition of general Granger non-causality. Permuter et al. [43] showed various applications of directed information in portfolio theory, data compression, and hypothesis testing in the presence of causality constraints. Amblard and Michel [44] reviewed the intimate connections between Granger causality and directed information theory.

We remark that, for practical applications, the directed information between stochastic processes can be computed using the universal estimators proposed in [45], which exhibit near-optimal statistical properties.

Finally, we note that the notion of transfer entropy in the physics literature, which was proposed by Schreiber [46] in 2000, turns out to be equivalent to directed information.

To connect our present discussion on causality measures to Theorem 1, we recall that the directed information rate [47] in 2000, turns out to be equivalent to directed information. As shown in Lemma 1, functional $C(\ell, P_{XY})$ is closely related to the notion of $\Phi$-entropy. We refer to Boucheron et al. [49, Ch. 14] for a nice survey on the usage of $\Phi$-entropies in proving concentration inequalities.

The next lemma asserts that we only need to consider symmetric (invariant to permutations) functions $V(\cdot)$.

Lemma 2: Under the Data Processing Axiom, there exists a symmetric finite convex function $G : \Gamma_n \to \mathbb{R}$, such that

$$C(\ell, P_{XY}) = \left( \sum_y P_T(y) G(P_{X|Y=y}) \right) - G(P_X),$$

and $G(\cdot)$ is equal to $V(\cdot)$ in Lemma 1 up to a linear translation:

$$G(P) = V(P) + (c, P),$$

where $c \in \mathbb{R}^n$ is a constant vector.

The proof of Lemma 2 follows by applying a permutation to the space $\mathcal{X}$ and applying the Data Processing Axiom. Details are deferred to the appendix.

Now we are in the position to begin the proof of Theorem 1 in earnest.

A. The Case $n \geq 3$

It suffices to consider the case when the side information $Y$ is binary valued, i.e., $Y \in \{1, 2\}$. We will show that the Data Processing Axiom mandates the usage of the logarithmic loss even when we constrain ourselves to this situation.

Define $\alpha \equiv \mathbb{P}[Y = 1]$. Take $P_{X|1}^{(l)}, P_{X|2}^{(l)}$ to be two probability distributions on $\mathcal{X}$ parametrized in the following way:

$$P_{X|1}^{(l)} = \lambda_1 \lambda_2 (1 - t), r - \lambda_1, p_4, \ldots, p_n$$

$$P_{X|2}^{(l)} = \lambda_{2, t} (1 - (t), r - \lambda_2, p_4, \ldots, p_n),$$

where $r \equiv 1 - \sum_{i \geq 4} p_i, t \in [0, 1], 0 \leq \lambda_1 < \lambda_2 \leq r$.

Taking $P_{X|1} \equiv P_{X|1}^{(l)}, P_{X|2} \equiv P_{X|2}^{(l)}$, it follows from Lemma 1 that

$$C(\ell, P_{XY}) = \alpha V(P_{X|1}^{(l)}) + (1 - \alpha) V(P_{X|2}^{(l)}) - V(\alpha P_{X|1}^{(l)} + (1 - \alpha) P_{X|2}^{(l)}).$$

Note that the following transformation $T(X)$ is a statistically sufficient transformation of $X$ for $Y$:

$$T(X) = \begin{cases} x_1 & X \in \{x_1, x_2\}, \\ X & \text{otherwise}. \end{cases}$$
The Data Processing Axiom implies that for all \( a \in [0, 1], t \in [0, 1] \) and legitimate \( \lambda_2 \triangleright \lambda_1 \geq 0, \)
\[
aV(P_{\lambda_1}^{(t)}) + (1 - a)V(P_{\lambda_2}^{(t)}) - V(aP_{\lambda_1}^{(t)} + (1 - a)P_{\lambda_2}^{(t)}) \\
= aV(P_{\lambda_1}^{(t)}) + (1 - a)V(P_{\lambda_2}^{(t)}) - V(aP_{\lambda_1}^{(t)} + (1 - a)P_{\lambda_2}^{(t)}).
\] (24)

We now define the function
\[
R(\lambda, t) \triangleq V(P_{\lambda}^{(t)}),
\] (25)
where we note that the bi-variate function \( R(\lambda, t) \) implicitly depends on the parameters \( p_4, p_5, \ldots, p_n \), which we shall fix for the rest of this proof. Thus, \( R(\lambda, t) = R(\lambda, t; p_4, p_5, \ldots, p_n) \).

Note that by definition,
\[
R(a\lambda_1 + (1 - a)\lambda_2, t) = V(aP_{\lambda_1}^{(t)} + (1 - a)P_{\lambda_2}^{(t)}),
\] (26)
hence we know that
\[
arR(\lambda_1, t) + (1 - a)R(\lambda_2, t) - R(a\lambda_1 + (1 - a)\lambda_2, t)
= aR(\lambda_1, t) + (1 - a)R(\lambda_2, t) - R(a\lambda_1 + (1 - a)\lambda_2, t).
\] (27)

Taking \( \lambda_1 = 0, \lambda_2 = r = 1 - \sum_{i=4} p_i \). We define \( \tilde{R}(\lambda, t) \triangleq R(\lambda, t) - \lambda U(t) \), where
\[
U(t) = \frac{R(t)}{r}.
\] (28)

It follows that
\[
\tilde{R}(0, t) = V(P_0^{(t)}), \quad \tilde{R}(r, t) = 0, \quad \forall t \in [0, 1],
\] (29)
and we note that \( V(P_0^{(t)}) \) in fact does not depend on \( t \).

With the help of (29), we plug \( R(\lambda, t) = \tilde{R}(\lambda, t) + \lambda U(t) \) into (27), and obtain
\[
\tilde{R}((1 - a)r, t) = \tilde{R}((1 - a)r, 1), \quad \forall a \in [0, 1], t \in [0, 1].
\] (30)

In other words, there exists a function \( E : [0, 1] \to \mathbb{R} \), such that
\[
\tilde{R}(\lambda, t) = E(\lambda).
\] (31)

Since \( R(\lambda, t) = \tilde{R}(\lambda, t) + \lambda U(t) \), we know that there exist real-valued functions \( E, U \) (indexed by \( p_4, \ldots, p_n \)) such that
\[
R(\lambda, t) = \lambda U(t) + E(\lambda).
\] (32)

Expressing \( \lambda, t \) in terms of \( p_1, p_2 \), we have
\[
\lambda = p_1 + p_2, \quad t = \frac{p_1}{p_1 + p_2}.
\] (33)

By definition of \( R(\lambda, t) \), we can re-write (32) as
\[
V(p_1, p_2, p_3, p_4, \ldots, p_n)
= (p_1 + p_2)U \left( \frac{p_1}{p_1 + p_2}; p_4, \ldots, p_n \right) + E(p_1 + p_2; p_4, \ldots, p_n).
\] (34)

By Lemma 2, we know that there exists a symmetric (permutation invariant) finite convex function \( G : \Gamma_n \to \mathbb{R} \), such that
\[
G(P) = V(P) + \langle c, P \rangle.
\] (35)

In other words, we have proved that \( G \) is of the form
\[
G(P) = (p_1 + p_2)U \left( \frac{p_1}{p_1 + p_2}; p_4, \ldots, p_n \right) + E(p_1 + p_2; p_4, \ldots, p_n) + \langle c, P \rangle.
\] (36)

For notational simplicity, we define
\[
Y(p_1, p_2) \triangleq G(P),
\] (37)
where we again note that \( Y(p_1, p_2; p_4, \ldots, p_n) \) is a bi-variate function parametrized by \( p_4, p_5, \ldots, p_n \). This gives
\[
Y(p_1, p_2) = (p_1 + p_2)U \left( \frac{p_1}{p_1 + p_2} \right) + E(p_1 + p_2) + c_1 p_1 + c_2 p_2 + c_3 (r - p_1 - p_2).
\] (38)

Since \( G(P) \) is a symmetric function, we know that if we exchange \( p_1 \) and \( p_3 \) in \( G(P) \), the value of \( G(P) \) will not change. In other words, for \( r = p_1 + p_2 + p_3 \), we have
\[
(r - p_3)U \left( \frac{p_1}{r - p_3} \right) + E(r - p_3) + c_1 p_1 + c_2 p_2 + c_3 p_3
= (r - p_1)U \left( \frac{p_3}{r - p_1} \right) + E(r - p_1) + c_1 p_3 + c_2 p_2 + c_3 p_1,
\] (39)
which is equivalent to
\[
(r - p_3)U \left( \frac{p_1}{r - p_3} \right) + E(r - p_3) + (c_3 - c_1)p_3
= (r - p_1)U \left( \frac{p_3}{r - p_1} \right) + E(r - p_1) + (c_3 - c_1)p_1.
\] (40)

Defining \( \tilde{E}(x) \triangleq E(r - x) + (c_3 - c_1)x \), we have
\[
(r - p_3)U \left( \frac{p_1}{r - p_3} \right) + \tilde{E}(p_3)
= (r - p_1)U \left( \frac{p_3}{r - p_1} \right) + \tilde{E}(p_1).
\] (41)

Interestingly, we can solve for general solutions of the above functional equation, which has connections to the so-called fundamental equation of information theory:

Lemma [50]-[52]: The most general measurable solution of
\[
f(x) + (1 - x)g \left( \frac{y}{1 - x} \right) = h(y) + (1 - y)k \left( \frac{x}{1 - y} \right),
\] (42)
for \( x, y \in [0, 1] \) with \( x + y \in [0, 1] \), where \( f, h : [0, 1] \to \mathbb{R} \) and \( g, k : [0, 1] \to \mathbb{R} \), has the form
\[
f(x) = aH_2(x) + b_1 x + d,
\] (43)
\[
g(y) = aH_2(y) + b_2 y + b_1 - b_4,
\] (44)
\[
h(x) = aH_2(x) + b_3 x + b_1 + b_2 - b_3 - b_4 + d,
\] (45)
\[
k(y) = aH_2(y) + b_4 y + b_3 - b_2,
\] (46)
for \( x \in [0, 1], y \in [0, 1] \), where \( H_2(x) = -x \ln x - (1 - x) \ln(1 - x) \) is the binary Shannon entropy and \( a, b_1, b_2, b_3, b_4, \) and \( d \) are arbitrary constants.
Remark 1: If \( f = g = h = k \) in (43)-(46), the corresponding functional equation is called the ‘fundamental equation of information theory.’

In order to apply the above lemma to our setting, we define

\[ q_i = p_i / r, \quad i = 1, 2, 3 \tag{47} \]

and \( h(x) = \tilde{E}(r x) / r \). Then we know

\[ (1 - q_1) U \left( \frac{q_1}{1 - q_3} \right) + h(q_1) = (1 - p_1) U \left( \frac{q_3}{1 - q_1} \right) + h(q_1). \tag{48} \]

Applying the general solution of (42), setting \( f = h \), \( g = k = U \), we have

\[ b_1 = b_3, b_2 = b_4. \tag{49} \]

Thus,

\[ h(x) = a H_2(x) + b_1 x + d, \]
\[ U(y) = a H_2(y) + b_2 y + b_1 - b_2. \tag{50, 51} \]

By the definition of \( h(x) \) and \( \tilde{E}(x) \), we have that

\[ E(x) = r a H_2(x) + (b_1 + c_1 - c_3)(r - x) + d. \tag{52} \]

Plugging the general solutions to \( U(x), E(x) \) into (38), and redefining the constants, we have

\[ Y(p_1, p_2) = A \left( p_1 \ln p_1 + p_2 \ln p_2 + (r - p_1 - p_2) \ln(r - p_1 - p_2) \right) + B p_1 + C p_2 + D. \tag{53} \]

Note that the constants \( A, B, C, D \) are functions of \( p_4, \ldots, p_n \). Therefore, we have the following general representation of the symmetric function \( G(P) \):

\[ G(P) = A(p_4, \ldots, p_n) \left( p_1 \ln p_1 + p_2 \ln p_2 + p_3 \ln p_3 \right) + B(p_4, \ldots, p_n) p_1 + C(p_4, \ldots, p_n) p_2 + D(p_4, \ldots, p_n), \tag{54} \]

where we have made the dependence on \( p_4 \ldots p_n \) explicit. Now we utilize the property that \( Y(p_1, p_2) \) is invariant to permutations. Exchanging \( p_1, p_2 \), we obtain that \( B \equiv C \). Exchanging \( p_1, p_3 \), we obtain that \( B \equiv C \equiv 0 \).

Doing an arbitrary permutation on \( p_4, \ldots, p_n \), since \( p_1, p_2, p_3 \) enjoy two degrees of freedom, we know that \( A(p_4, \ldots, p_n), D(p_4, \ldots, p_n) \) are symmetric functions.

Exchanging \( p_1, p_4 \) and comparing the coefficients for \( p_2 \) in \( p_2 \), we know that

\[ A(p_4, p_5, \ldots, p_n) = A(p_1, p_5, \ldots, p_n), \tag{55} \]

since \( A \) is symmetric, and thus we can conclude that \( A \) is a constant. Now exchanging \( p_1, p_4 \) gives us

\[ A p_1 \ln p_1 - A p_4 \ln p_4 = D(p_1, p_5, \ldots, p_n) \tag{56} \]

Taking partial derivatives with respect to \( p_1 \) (we vary \( p_2 \) simultaneously to ensure \( P \) still lies on the simplex) on both sides of (56), we obtain

\[ A \left( \ln p_1 + 1 \right) = \frac{\partial}{\partial p_1} D(p_1, p_5, \ldots, p_n). \tag{57} \]

Integrating on both sides with respect to \( p_1 \), we know there exists a function \( f \) such that

\[ D(p_1, p_5, \ldots, p_n) = A p_1 \ln p_1 + f(p_5, \ldots, p_n). \tag{58} \]

Since \( D \) is symmetric, we further know that

\[ D(p_4, \ldots, p_n) = \sum_{i \geq 4} A p_i \ln p_i. \tag{59} \]

To sum up, we have

\[ G(P) = A \sum_{i=1}^{n} p_i \ln p_i. \tag{60} \]

To guarantee that \( G(P) \) is convex, we need \( A > 0 \). Plugging (60) into Lemma 2, the proof is complete.

B. The Case \( n = 2 \)

Under the Data Processing Axiom, Lemma 2 implies the corresponding representation. On the other hand, for an arbitrary convex function \( G \), the Savage representation of proper scoring rules [7] gives the construction of the corresponding loss function \( \ell. \) Indeed, the Savage representation asserts, for a convex function \( G \), we can define a loss function \( \ell_G(x, Q) : \mathcal{X} \times \Gamma_n \to \mathbb{R} \) by

\[ \ell_G(x, Q) \triangleq \langle G'(Q), Q \rangle - G(Q) - G'_s(Q), \tag{61} \]

where \( G'(Q) \) denotes a sub-gradient of \( G(Q) \) at \( Q \), and \( G'_s(Q) \) is the component of \( G'(Q) \) corresponding to \( Q(x) \) (see, e.g., [7] for details). The loss function \( \ell_G(x, Q) \) also satisfies

\[ P \in \arg \inf_{Q \in \Gamma_n} \mathbb{E}_{P}[\ell_G(X, Q)]. \tag{62} \]

Substituting loss function \( \ell_G(x, Q) \) into (2) defines a valid \( C(\ell, P_{XY}) \). The proof is completed via noting that the only non-trivial statistically sufficient transform on a binary alphabet is permutation transform, and the function \( G \) is assumed to be invariant to permutations.

APPENDIX

PROOF OF LEMMAS

A. Proof of Lemma 1

It follows from (3) that if we define

\[ V(P) = - \inf_{i \in \mathcal{X}} \mathbb{E}_{P}[\ell(X, \hat{x})], \tag{63} \]

then \( V(P) \) cannot take values in \([\infty, -\infty]\).

Since \( \mathbb{E}_{P}[\ell(X, \hat{x})] \) is linear in \( P \), and \( V(P) \) is the pointwise supremum over a family of linear functions of \( P \), we know \( V(P) \) is convex and lower semi-continuous on \( \Gamma_n \).

Since \( \Gamma_n \) is a compact set, we know that the lower semi-continuous function \( V(P) \) attains its minimum on \( \Gamma_n \).

At the same time, since \( \Gamma_n \) is a polytope, we know \( \forall P = (p_1, p_2, \ldots, p_n) \in \Gamma_n \), we have \( P = \sum_{i=1}^{n} p_i \delta_i \), where \( \delta_i = (0, 0, \ldots, 1, 0, \ldots, 0) \) is a distribution that puts mass one at symbol \( i \).
Since $V(P)$ is convex, we have

$$V(P) = V\left(\sum_{i=1}^{n} p_i \delta_i\right) \leq \sum_{i=1}^{n} p_i V(\delta_i) \leq \max\{V(\delta_i), 1 \leq i \leq n\}. \tag{64}$$

That is to say, the function $V(P)$ attains its maximum at one of the boundary points $\delta_i$. Thus, we know that $V(P)$ is bounded.

Now we proceed to show that

$$\inf_{\hat{X}(Y)} \mathbb{E}_P[\ell(X, \hat{X}(Y))] = -\sum_{y} P_Y(y) V(P_{X|Y=y}). \tag{65}$$

First, for any estimator $\hat{X}(Y)$, by the law of iterated expectation, we have

$$\mathbb{E}_P[\ell(X, \hat{X}(Y))] = \mathbb{E}_P[\mathbb{E}_P[\ell(X, \hat{X}(Y))|Y]] \geq \mathbb{E}_P[-V(P_{X|Y=y})] \geq -\sum_{y} P_Y(y) V(P_{X|Y=y}). \tag{66}$$

Hence,

$$\inf_{\hat{X}(Y)} \mathbb{E}_P[\ell(X, \hat{X}(Y))] \geq -\sum_{y} P_Y(y) V(P_{X|Y=y}). \tag{67}$$

Second, by the definition of infimum, for any $\epsilon > 0$, there exists an estimator $\hat{x}_\epsilon(y) \in \hat{X}$ such that

$$-V(P_{X|Y=y}) > \sum_{x \in X} P_X|Y=y(x)\ell(x, \hat{x}_\epsilon(y)) - \epsilon. \tag{68}$$

Now define an estimator $\hat{X}(Y) = \hat{x}_\epsilon(Y)$. We have

$$\mathbb{E}_P[\ell(X, \hat{X}(Y))] = \mathbb{E}_P[\mathbb{E}_P[\ell(X, \hat{x}_\epsilon(Y))|Y]] \geq \mathbb{E}_P[-V(P_{X|Y=y}) + \epsilon] \geq -\sum_{y} P_Y(y) V(P_{X|Y=y}) + \epsilon. \tag{69}$$

By the arbitrariness of $\epsilon$ we have

$$\inf_{\hat{X}(Y)} \mathbb{E}_P[\ell(X, \hat{X}(Y))] \leq -\sum_{y} P_Y(y) V(P_{X|Y=y}). \tag{70}$$

Combining it with (69), we know that (65) holds. The claim follows from plugging (63) and (65) into the definition of $C(\ell, P_{XY})$.

B. Proof of Lemma 2

By Lemma 1, we know there exists a convex function $V : \Gamma_n \to \mathbb{R}$, such that

$$C(\ell, P_{XY}) = \left(\sum_{y} P_Y(y) V(P_{X|Y=y})\right) - V(P_X). \tag{71}$$

Let $\delta_i \triangleq (0, 0, \ldots, 1, \ldots, 0)$ be a distribution in $\Gamma_n$ that puts mass one on the $i$-th symbol of $X$. Define $a_i \triangleq V(\delta_i)$. We know that $a_i \in \mathbb{R}, \forall i = 1, 2, \ldots, n$.

Define the convex function $G : \Gamma_n \to \mathbb{R}$ as

$$G(P) = V(P) - \sum_{i=1}^{n} a_i p_i. \tag{72}$$

Now it is easy to verify that $G(\delta_i) = 0, \forall i = 1, 2, \ldots, n$.

After some algebra we can show that

$$C(\ell, P_{XY}) = \left(\sum_{y} P_Y(y) G(P_{X|Y=y})\right) - G(P_X). \tag{73}$$

Taking $Y \in \mathcal{X}$, and $P_Y = (p_1, p_2, \ldots, p_n)$ to be an arbitrary probability distribution. Setting $P_{X|Y=y} = \delta_y$, then we have

$$C(\ell, P_{XY}) = -G(P_X) = -G((p_1, p_2, \ldots, p_n)). \tag{74}$$

Define $T = \pi(X)$ to be a permutation of $X$, which is sufficient for $Y$. The Data Processing Axiom implies that

$$C(\ell, P_{XY}) = C(\ell, P_{TY}), \tag{75}$$

By construction, we have

$$C(\ell, P_{XY}) = -G((p_1, p_2, \ldots, p_n)), \tag{76}$$

$$C(\ell, P_{TY}) = -G((p_{\pi^{-1}(1)}, p_{\pi^{-1}(2)}, \ldots, p_{\pi^{-1}(n)})), \tag{77}$$

which implies that the function $G$ is invariant to permutations. We take $\epsilon = -(a_1, a_2, \ldots, a_n)$ to finish the proof.

ACKNOWLEDGMENT

The authors would like to thank the Associate Editor, two anonymous reviewers, and Yanjun Han, whose comments have significantly improved the presentation of the paper.

REFERENCES


Kartik Venkat (S’12) is a Ph.D. candidate in the Department of Electrical Engineering at Stanford University. His research interests include statistical inference, information theory, machine learning, and their applications in genomics, wireless networks, neuroscience, and quantitative finance. Kartik received a Bachelors degree in Electrical Engineering from the Indian Institute of Technology, Kanpur in 2010, and a Master’s degree in Electrical Engineering from Stanford University in 2012. His honors include a Stanford Graduate Fellowship for Engineering and Sciences, the Numerical Technologies Founders Prize, and a Jack Keil Wolf ISIT Student Paper Award at the 2012 International Symposium on Information Theory.

Tsachy Weissman (S’99–M’02–SM’07–F’13) graduated summa cum laude with a B.Sc. in electrical engineering from the Technion in 1997, and earned his Ph.D. at the same place in 2001. He then worked at Hewlett Packard Laboratories with the information theory group until 2003, when he joined Stanford University, where he is currently Professor of Electrical Engineering and incumbent of the STMicroelectronics chair in the School of Engineering. He has spent leaves at the Technion, and at ETH Zurich.

Tsachy’s research is focused on information theory, compression, communication, statistical signal processing, the interplay between them, and their applications. He is recipient of several best paper awards, and prizes for excellence in research and teaching. He served on the editorial board of the IEEE Transactions on Information Theory from Sept. 2010 to Aug. 2013, and currently serves on the editorial board of Foundations and Trends in Communications and Information Theory. He is Founding Director of the Stanford Compression Forum.