A Metric Between Probability Distributions on Finite Sets of Different Cardinalities

M. Vidyasagar, Fellow IEEE

Abstract—With increasing use of digital control it is natural to view control inputs and outputs as stochastic processes assuming values over finite alphabets rather than in a Euclidean space. As control over networks becomes increasingly common, data compression by reducing the size of the input and output alphabets without losing the fidelity of representation becomes relevant. This requires us to define a notion of distance between two stochastic processes assuming values in distinct sets, possibly of different cardinalities. If the two processes are i.i.d., then the problem becomes one of defining a metric between two probability distributions over distinct finite sets of possibly different cardinalities. This is the problem addressed in the present paper. A metric is defined in terms of a joint distribution on the product of the two sets, which has the two given distributions as its marginals, and has minimum entropy. Computing the metric exactly turns out to be NP-hard. Therefore an efficient greedy algorithm is presented for finding an upper bound on the distance.

I. INTRODUCTION

Suppose we view a control system as an input-output map where the input signal is a sequence \( \{u_t\} \) assuming values in some finite set \( U \), while the output signal is a sequence \( \{y_t\} \) assuming values in another finite set \( Y \). In this setting, the problem of order reduction is quite different in nature from the traditional order reduction problem, where the emphasis is on reducing the dimension of the (Euclidean) state space. If the system has some element of randomness in it, we should view \( \{u_t, y_t\} \) as a stochastic process assuming values in the set \( U \times Y \).\(^1\) For the purposes of controller design, it would be worthwhile to know whether the finely quantized inputs and outputs can be replaced by a coarser quantization without losing too much accuracy in the representation. Such considerations become particularly germane in the problem of control over networks, whereby the plant and controller may be connected only through a noisy channel. This type of order reduction would require approximating the original stochastic process by another one assuming values in a set of smaller cardinality \( U' \times Y' \). The approximation can be quantified by defining a metric distance between two stochastic processes assuming values in distinct sets (of different cardinalities). So far as the author is aware, no such metric is available in the literature. The closest the author has been able to find is a paper by Ornstein [15] in the inaugural issue of the Annals of Probability, in which he defines a metric distance between two stochastic processes assuming values in a common finite set.

Our analysis is based on information theory. The use of information-theoretic methods in the controls community has a long history, going back at least to [16] if not much earlier. In this paper, we define a metric distance between two distributions on distinct finite sets by maximizing their mutual information. It turns out that actually computing the metric distance between two probability distributions is an NP-hard problem as it can be reduced to a nonstandard bin-packing problem. Therefore we develop efficient greedy algorithm. Specifically, we can compute an upper bound on the distance in \( O((n + m^2) \log m) \) operations where \( n \) and \( m \) are the cardinalities of the two sets with \( n \geq m \).

II. THE VARIATION OF INFORMATION METRIC

A. Concepts from Information Theory

Throughout the paper, we shall use the symbols \( \mathbb{A}, \mathbb{B}, \mathbb{C} \) for finite sets of cardinality \( n, m, l \) respectively. The symbols \( X, Y, Z \) denote random variables assuming values in \( \mathbb{A}, \mathbb{B}, \mathbb{C} \) respectively. The symbols \( \phi, \psi, \xi \) denote probability distributions on the sets \( \mathbb{A}, \mathbb{B}, \mathbb{C} \) respectively. Though the elements of these sets could be any abstract entities, to avoid notational clutter we shall write \( \mathbb{A} = \{1, \ldots, n\} \) instead of the more precise \( \mathbb{A} = \{a_1, \ldots, a_n\} \). Let \( e \) denote the column vector of all one’s, and the subscript denote its dimension. Thus \( e_n \) is a column vector of \( n \) one’s. A matrix \( P \in [0, 1]^{m \times n} \) is said to be stochastic if \( Pe_n = e_m \), that is, for each row, the sum of all columns equals one. The set of \( m \times n \) stochastic matrices is denoted by \( \mathbb{S}_{m \times n} \). If we take the degenerate case of \( m = 1 \), then the symbol \( \mathbb{S}_n = \mathbb{S}_{1 \times n} \) denotes the set of nonnegative (row) vectors that add up to one. Clearly \( \mathbb{S}_n \) can be identified with the set \( \mathcal{M}(\mathbb{A}) \) of all probability distributions on \( \mathbb{A} \).

Suppose \( X, Y \) are random variables assuming values in \( \mathbb{A}, \mathbb{B} \) respectively, and let \( \mathbf{\Theta} \in \mathcal{M}(\mathbb{A} \times \mathbb{B}) \) denote their joint distribution. For each index \( i \) between 1 and \( n \), let \( p_i \) denote the conditional distribution of \( Y \) given that \( X = i \). That is,

\[
p_{ij} = \frac{\theta_{ij}}{\sum_{j'=1}^{m} \theta_{ij'}}.
\]

Note that the matrix \( P = [p_{ij}] \) belongs to \( \mathbb{S}_{n \times m} \), and the \( i \)-th row of \( P \), denoted by \( p_i \), belongs to \( \mathbb{S}_m \) for each \( i \). If we represent the joint distribution of \( X \) and \( Y \) by an \( n \times m \) matrix \( \Theta = [\theta_{ij}] \) where \( \theta_{ij} = \Pr\{X = i \& Y = j\} \), then we...
can write

\[ P = [\text{Diag}(\phi)]^{-1}\Theta, \quad (1) \]

where \( \text{Diag}(\phi) \) represents the \( n \times n \) diagonal matrix with \( \phi_1, \ldots, \phi_n \) as the diagonal elements. Suppose we now define \( Q \in S_{m \times n} \) by

\[ q_{ij} = \Pr\{X = i|Y = j\}. \]

Then it is easy to see that the following identities hold:

\[ \Theta = \text{Diag}(\phi)P = Q^T\text{Diag}(\psi), \quad (2) \]

\[ Q = [\text{Diag}(\psi)]^{-1}P^T\text{Diag}(\phi). \quad (3) \]

Now we introduce various concepts from information theory. All the concepts introduced below are discussed in [6, Chapter 2]. The function \( h : [0,1] \rightarrow \mathbb{R}_+ \) is defined by \( h(r) = -r\log r \), with the standard convention that \( h(0) = 0 \). Note that \( h \) is continuously differentiable except at \( r = 0 \), and that \( h'(r) = -(1 + \log r) \). The symbol \( H \) denotes the Shannon entropy of a probability distribution. Thus if \( \phi \in S_n \), then

\[ H(\phi) = -\sum_{i=1}^n \phi_i \log \phi_i = \sum_{i=1}^n h(\phi_i). \]

We define the conditional entropy of \( Y \) given \( X \) as

\[ H(Y|X) = \sum_{i=1}^n \phi_i H(p_{i1}) = \sum_{i=1}^n \phi_i \sum_{j=1}^m h(p_{ij}) \]

\[ = -\sum_{i=1}^n \phi_i \sum_{j=1}^m p_{ij} \log p_{ij}, \]

where \( p_{ij} \) denotes the \( i \)-th row of the matrix \( P \). With this definition the identities

\[ H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) \quad (4) \]

hold. The mutual information between \( X \) and \( Y \) is defined as

\[ I(X,Y) = H(X) + H(Y) - H(X,Y) \]

\[ = H(Y) - H(Y|X) = H(X) - H(X|Y). \]

B. Setting Up the Problem

Suppose \( X, Y \) are random variables assuming values in the sets \( \mathcal{A}, \mathcal{B} \), respectively, with distributions \( \phi, \psi \) respectively. We ask: What is the maximum possible mutual information between \( X \) and \( Y \)? Clearly this is equivalent to asking the question: What is a (or the) distribution \( \Theta \) on \( \mathcal{A} \times \mathcal{B} \) that has minimum entropy, while satisfying the boundary conditions \( \Theta_{\mathcal{A}} = \phi, \Theta_{\mathcal{B}} = \psi \)?

Definition 1: Given sets \( \mathcal{A}, \mathcal{B} \) with \( |\mathcal{A}| = n, |\mathcal{B}| = m \), and given \( \phi \in S_n, \psi \in S_m \), define

\[ W(\phi, \psi) := \min_{\Theta \in M(\mathcal{A} \times \mathcal{B})} \{ H(\Theta) : \Theta_{\mathcal{A}} = \phi, \Theta_{\mathcal{B}} = \psi \}, \quad (5) \]

\[ V(\phi, \psi) := W(\phi, \psi) - H(\phi). \quad (6) \]

It is obvious that

\[ W(\psi, \phi) = W(\phi, \psi), V(\psi, \phi) = V(\phi, \psi) + H(\phi) - H(\psi), \quad (7) \]

where the second identity follows from (4).

C. The Variation of Information Metric

We begin by defining a metric between random variables, and then move on to distributions.

Definition 2: Given two random variables \( X, Y \), the variation of information between them is defined as

\[ v(X,Y) = H(X|Y) + H(Y|X). \quad (8) \]

This measure is introduced in [13], [14] where it is referred to as the ‘variation of information’ metric between random variables. So we retain the same nomenclature, though our metric is between probability distributions.

Theorem 1: The function \( v(\cdot, \cdot) \) satisfies the axioms of a pseudometric. Thus \( v \) has the properties that for all random variables \( X, Y, Z \), we have \( v(X,Y) \geq 0 \), \( v(X,Y) = v(Y,X) \), and \( v(X,Y) \leq v(X,Z) + v(Y,Z) \).

Proof: It is obvious that \( v(X,Y) \geq 0 \), and it follows from (8) that \( v(X,Y) = v(Y,X) \). To show that \( v(\cdot, \cdot) \) satisfies the triangle inequality, we make use of the easily-proved inequality

\[ H(X|Y) \leq H(X,Z|Y) = H(Z|Y) + H(X|Z) \leq H(Z|Y) + H(X|Z). \quad (9) \]

To prove the triangle inequality, invoke the one-sided triangle inequality (9) and observe that

\[ v(X,Y) = H(X|Y) + H(Y|X) \leq H(X,Z) + H(Z|Y) + H(Y|Z) + H(Z|X) = v(X,Z) + v(Y,Z). \]

This completes the proof.

Now we turn the above pseudometric between random variables into a pseudometric between probability distributions.

Definition 3: Given two probability distributions \( \phi \in S_n, \psi \in S_m \), the variation of information metric between them is defined as

\[ d(\phi, \psi) = V(\phi, \psi) + V(\psi, \phi). \quad (10) \]

Theorem 2: The function \( d \) defined in (10) is a pseudometric in that it is nonnegative, symmetric and satisfies the triangle inequality.

Proof: It is obvious that \( d \) is nonnegative and symmetric; so it only remains to prove the triangle inequality. To prove this, we first establish a small technical point. Suppose \( \eta \in M(\mathcal{A} \times \mathcal{C}), \zeta \in M(\mathcal{B} \times \mathcal{C}) \) and that \( \eta_{\mathcal{C}} = \zeta_{\mathcal{C}} = \xi \). Then it is always possible to find a distribution \( \nu \in M(\mathcal{A} \times \mathcal{B} \times \mathcal{C}) \) such that \( \nu_{\mathcal{A} \times \mathcal{C}} = \eta \) and \( \nu_{\mathcal{B} \times \mathcal{C}} = \zeta \). In words, the claim is that, given two joint distributions, one of \( X \) and \( Z \), and another of \( Y \) and \( Z \), both of them having the same marginal distribution for \( Z \), it is possible to find a joint distribution for all three variables \( X, Y, Z \) such that the marginal distributions of \( (X,Y) \) and of \( (Y,Z) \) match the two given joint distributions. To establish the claim, we construct \( \nu \) by making \( X \) and \( Y \) conditionally independent given \( Z \), or equivalently, by making \( X \rightarrow Z \rightarrow Y \) into a very short Markov chain. Accordingly, let

\[ \nu_{ijk} = \frac{\eta_{ik} \zeta_{jk}}{\xi_k}. \]
It is routine to verify that \( \nu \) has the required properties, using the identities
\[
\xi_k = \sum_{i \in A} \eta_{ik} = \sum_{j \in B} \zeta_{jk}.
\]
Now we return to the proof that \( d \) satisfies the triangle inequality. Given three different probability distributions \( \phi \in \mathcal{M}(A), \psi \in \mathcal{M}(B), \xi \in \mathcal{M}(C) \), let us choose distributions \( \theta \in \mathcal{M}(A \times B), \eta \in \mathcal{M}(A \times C) \) and \( \zeta \in \mathcal{M}(B \times C) \) such that
\[
\theta_A = \phi, \theta_B = \psi, H(\theta) = W(\phi, \psi),
\]
\[
\eta_A = \phi, \eta_C = \xi, H(\eta) = W(\phi, \xi),
\]
\[
\zeta_B = \psi, \zeta_C = \xi, H(\zeta) = W(\psi, \xi).
\]
Now choose \( \nu \) to be any distribution on \( A \times B \times C \) such that
\[
\nu_{A \times C} = \eta, \nu_{B \times C} = \zeta.
\]
Let \( X, Y, Z \) be three random variables with the joint distribution \( \nu \). Then the triangle inequality for the quantity \( v \) shows that
\[
v(X, Y) \leq v(X, Z) + v(Y, Z).
\]
The manner in which \( \eta \) and \( \zeta \) were chosen shows that
\[
v(X, Z) = d(\phi, \xi), v(Y, Z) = d(\psi, \xi).
\]
However, an analogous statement about \( v(X, Y) \) may not be true. So we note instead that \( d(\phi, \psi) \) is the minimum of \( v(X, Y) \) whenever \( X \) and \( Y \) have distributions \( \phi, \xi \) respectively. Hence
\[
d(\phi, \psi) \leq v(X, Y) \leq v(X, Z) + v(Y, Z) = d(\phi, \xi) + d(\psi, \xi),
\]
which is the desired conclusion.

III. COMPUTING THE METRIC

A. Problem Formulation and Elementary Properties

Now that we have defined the metric, the next step is to compute it. Note that if we compute \( V(\phi, \psi) \), then \( V(\psi, \phi) \) is automatically determined by (7). Also, minimizing the conditional entropy maximizes the mutual information, so we refer to this approach as MMI. For reasons that will become later, we assume that \( n \geq m \). Clearly there is no loss of generality in doing this. The next step is to reparametrize the problem, by changing the variable of optimization from the joint distribution \( \theta \in \mathbb{S}_{mn} \) to the matrix of conditional probabilities \( P \in \mathbb{S}_{n \times m} \). Thus the boundary conditions \( \theta_A = \phi, \theta_B = \psi \) get replaced by \( \phi P = \psi \). Also, it is clear that, for a particular choice of \( P \), the conditional entropy \( H(Y|X) \) is given by
\[
J_{\phi}(P) = \sum_{i=1}^{n} \phi_i H(p_i), \quad \text{for} \quad 0 \leq \phi, \psi \leq 1,
\]
where \( p_i \) is the \( i \)-th row of \( P \). Moreover, it follows from (4) that if \( P \) and \( Q \) are related by (2), then
\[
J_{\psi}(Q) = J_{\phi}(P) + H(\phi) - H(\psi).
\]
Finally, it is easy to see that, given \( \phi \in \mathbb{S}_n, \psi \in \mathbb{S}_m \), the quantity \( V \) defined in (6) can also be defined equivalently as
\[
V(\phi, \psi) = \min_{P \in \mathbb{S}_{n \times m}} \{ J_{\phi}(P) \}.
\]

B. A Principle of Optimality

We now state a ‘principle of optimality’ for this problem. Suppose \( \phi \in \mathbb{S}_n, \psi \in \mathbb{S}_m \) are specified, and that \( \phi_i > 0 \) for all \( i \). Suppose \( A = \{1, \ldots, n\} \), and let \( A' \) be a nonempty proper subset of \( A \). For notational convenience, suppose \( A' = \{1, \ldots, k\} \) where \( k < n \). For \( \phi \in \mathbb{S}_n, P \in \mathbb{S}_{n \times m} \), define
\[
\phi' := [\phi_1 \ldots \phi_k], P' := \begin{bmatrix} P_1 \\ \vdots \\ P_k \end{bmatrix},
\]
and note that \( P' \in \mathbb{S}_{k \times m} \), though in general \( \phi' \) need not belong to \( \mathbb{S}_k \). After this elaborate build-up we can now state the principle of optimality.

Theorem 4: With all notation as above, suppose \( \phi_i > 0 \ \forall i \), and suppose that \( P^* \) minimizes \( J_{\phi}(P) \) subject to the constraint that \( \phi P = \psi \). Define \( c = \phi' e_k > 0 \), and \( \psi' = \sum_{i=1}^{k} \phi_i p_i^* = \phi' (P^*)' \). Observe that \( (1/c) \phi' \not\in \mathbb{S}_k, (1/c) \psi' \not\in \mathbb{S}_m \). Then \( (P^*)' \) minimizes \( J_{\phi}(P') \) over \( \mathbb{S}_{k \times m} \) subject to the constraint that \( (1/c) \phi' P' = (1/c) \psi' \).

Proof: Note that \( (P')' \) is also a stochastic matrix in that \( (P')' e_m = e_k \). Hence
\[
\psi' e_m = \phi' (P')' e_m = \phi' e_k = c > 0,
\]
because every component of \( \phi' \) is positive. Hence \( \psi' \) is certainly not the zero vector, even though some components of \( \psi' \) could be zero. Thus \( (1/c) \phi' \not\in \mathbb{S}_k, (1/c) \psi' \not\in \mathbb{S}_m \), and the minimization problem under study is similar to the larger problem. To prove the claim, suppose by way of contradiction that there exists another matrix \( Q' \in \mathbb{S}_{k \times m} \) that satisfies \( \phi' Q' = \psi' \) such that
\[
J_{\phi'}(Q') = \sum_{i=1}^{k} \phi_i H(q_i) < J_{\phi'}((P^*)') = \sum_{i=1}^{k} \phi_i H(p_i).
\]
Define in an analogous fashion
\[(P^*)'' = \begin{bmatrix}
p_k+1 \\
\vdots \\
p_n 
\end{bmatrix}, Q = \begin{bmatrix}
Q' \\
(P^*)'
\end{bmatrix},
\]
and note that, since \(P^*\) is feasible for the original problem, we have that
\[
\sum_{i=k+1}^n \phi_i p_i^* = \phi P^* - \phi'(P^*)' = \psi - \psi'.
\]
Now
\[
J_\phi(Q) = \sum_{i=1}^k \phi_i H(q_i) + \sum_{i=k+1}^n \phi_i H(p_i^*) \\
< \sum_{i=1}^k \phi_i H(p_i^*) + \sum_{i=k+1}^n \phi_i H(p_i^*) = J_\phi(P^*),
\]
while
\[
\phi Q = \phi' Q' + \sum_{i=k+1}^n \phi_i p_i^* = \psi' + \psi - \psi' = \psi.
\]
Hence \(Q\) is feasible for the original problem and has a lower objective function, which is a contradiction. Hence \((P^*)'\) is a minimizer of the reduced-size problem. ■

IV. Solution to the MMI Problem in the \(n \times 2\) Case

A. The \(2 \times 2\) Case

In this subsection we give an explicit closed-form expression for \(V(\phi, \psi)\) when \(n = m = 2\) and \(\phi, \psi \in S_2\). Without loss of generality, assume that \(\phi \neq \psi\) because \(V(\phi, \psi) = 0\) if \(\phi = \psi\). Also, again without loss of generality, rearrange the elements of \(\phi, \psi\) such that both vectors are in strictly increasing order.\(^2\) Then we can distinguish between two cases, namely (a) \(0 < \psi_1 < \phi_1 < \phi_2 < \psi_2\), and (b) \(0 < \phi_1 < \psi_1 < \phi_2 < \psi_2\).

**Theorem 5:** Suppose \(n = m = 2\) and \(\phi, \psi \in S_2\). Suppose further that we have either case (a) or case (b) above. If \(0 < \psi_1 < \phi_1 < \phi_2 < \psi_2\), then
\[
V(\phi, \psi) = -\psi_1 \log(\psi_1/\phi_1) \\
- (\phi_1 - \psi_1) \log(1 - \psi_1/\phi_1).
\] (19)
If \(0 < \phi_1 < \psi_1 < \psi_2 < \phi_2\) then
\[
V(\phi, \psi) = -(\phi_2 - \psi_2) \log(1 - \psi_2/\phi_2) \\
- \psi_2 \log(\psi_2/\phi_2).
\] (20)
**Proof:** From Theorem 3, we know that any optimal choice of \(P \in S_{2 \times 2}\) must be an extreme point of the feasible region. Thus at least one component of \(P\) must be zero. The constraints that \(P\) is stochastic and that \(\phi P = \psi\) lead to the following four possible extreme points of the feasible region.
\[
P_{11} = \begin{bmatrix}
\psi_1/\phi_2 & 1 \\
1 - \psi_1/\phi_2 & 0
\end{bmatrix}, P_{12} = \begin{bmatrix}
1 - \psi_1/\phi_2 & \psi_1/\phi_2 \\
\psi_1/\phi_2 & 0
\end{bmatrix},
\]
\[
P_{21} = \begin{bmatrix}
\psi_1/\phi_1 & 0 \\
1 - \psi_1/\phi_1 & 1
\end{bmatrix}, P_{22} = \begin{bmatrix}
1 - \psi_1/\phi_1 & \psi_1/\phi_1 \\
\psi_1/\phi_1 & 0
\end{bmatrix}.
\]
Moreover, since \(\psi_2 > \phi_2\) and \(\psi_2 > \phi_1\), it follows that \(P_{12}\) and \(P_{22}\) are infeasible, and the only possibilities are \(P_{11}\) and \(P_{21}\). So all we need to do is to compute \(J_\phi(P_{11}), J_\phi(P_{21})\), and pick the one that is smaller. This is an exercise in calculus and is omitted. The other case follows by symmetry. ■

B. The \(n \times 2\) Case

We begin with a notion that is encountered again several times in the paper.

**Definition 4:** Given \(\phi \in S_n, \psi \in S_m\) with \(n > m, \psi\) is said to be an aggregation of \(\phi\) if there exists a partition of \(N\) into \(m\) sets \(I_1, \ldots, I_m\) such that \(\sum_{i \in I_2} \phi_i = \psi_j\) for \(j = 1, \ldots, m\).

Next we introduce the bin-packing problem with overstuffing and variable bin capacities as follows: Given \(\phi \in S_n, \psi \in S_m\), find a partition of \(N\) into \(m\) sets \(I_1, \ldots, I_m\) such that the total mismatch
\[
MI = \sum_{j \in B} |\psi_j - \sum_{i \in I_j} \phi_i|
\]
is as small as possible. Unfortunately, this problem is also NP-hard [7]. Even determining whether a given \(\psi\) is an aggregation of a given \(\phi\) or not is also NP-hard. The bin packing with overstuffing is discussed in [7], [3], [4] among other papers.

With this background, we now present a partial solution to the problem of computing \(V(\phi, \psi)\) when \(m = 2\) in terms of the bin-packing problem with overstuffing with two bins. If \(\psi\) is an aggregation of \(\phi\), then obviously \(V(\phi, \psi) = 0\). Otherwise, let \(\psi_1, \psi_2\) denote the capacity of the two bins, and let \(\phi_1, \ldots, \phi_n\) denote the list to be packed. Without loss of generality, assume that the \(\phi_i\) are in decreasing order of magnitude. Let \(N_1, N_2\) denote an optimal partition of \(N = \{1, \ldots, n\}\) and let \(c\) denote the minimum unutilized capacity. Again, without loss of generality, assume that bin 1 is underutilized and that bin 2 is overstuffed. This means that
\[
\psi_2 - \sum_{i \in N_2} \phi_i = -\psi_1 + \sum_{i \in N_1} \phi_i = c.
\] (21)

**Theorem 6:** Suppose \(\psi\) is not an aggregation of \(\phi\), and solve the bin-packing problem as above. If \(n \in N_2\), then an optimal choice of \(P\) that minimizes \(J_\phi(P)\) subject to \(\phi P = \psi\) is given by
\[
p_i = [1 \ 0] \forall i \in N_1, p_i = [0 \ 1] \forall i \in N_2 \setminus \{n\},
\]
\[
p_n = [c/\phi_n \ (\phi_n - c)/\phi_n].
\] (22)
Moreover

\[ V(\phi, \psi) = \phi_n H(p_n) = f_c(\phi_n), \]

where the function \( f \) is defined as

\[ f_u(\phi) := \phi [h(u/\phi) + h(1 - (u/\phi))]. \tag{23} \]

**Proof:** From the principle of optimality, we know that if a matrix \( P \) is optimal for the \( n \times 2 \) problem, then every \( 2 \times 2 \) submatrix is optimal for its respective problem, and thus has at most one strictly positive row, while the rest are either \([1 \ 0]\) or \([0 \ 1]\). Accordingly, define \( P \) as above, and let \( R \) be another matrix that has exactly one strictly positive row such that \( \phi R = \psi \). All we need to do is to show that \( J_\phi(R) \geq J_\phi(P) \). For this purpose, suppose the \( k \)-th row of \( R \) is strictly positive, and define

\[ I_1 = \{ i : r_i = [1 \ 0] \}, I_2 = \{ i : r_i = [0 \ 1] \}, \]

while \( r_k \) is strictly positive. Then \( \phi R = \psi \) implies that

\[ u_1 := \psi_1 - \sum_{i \in I_1} \phi_i > 0, \quad u_2 := \psi_2 - \sum_{i \in I_2} \phi_i > 0, \quad u_1 + u_2 = \phi_k, \]

\[ r_k = \begin{bmatrix} u_1/\phi_k & u_2/\phi_k \end{bmatrix}, \]

\[ J_\phi(R) = \phi_k H(r_k) = f_u(\phi_k), \]

where the function \( f \) is defined in (23), and we use the fact that \( u_2 = \phi_k - u_1 \). The fact that \( c \) is the optimal unutilized capacity implies that \( c \leq \min\{u_1, u_2\} \), so that \( c \leq \min\{u_1, u_2\} \leq \max\{u_1, u_2\} \leq \phi_k - c \). In turn this implies that

\[ H(r_k) = H(\begin{bmatrix} u_1/\phi_k & u_2/\phi_k \end{bmatrix}) \geq H(\begin{bmatrix} c/\phi_k & (\phi_k - c)/\phi_k \end{bmatrix}). \]

So we now conclude that

\[ J_\phi(R) = \phi_k H(r_k) \geq \phi_k H(\begin{bmatrix} c/\phi_k & (\phi_k - c)/\phi_k \end{bmatrix}) = f_c(\phi_k) \geq f_c(\phi_n) = J_\phi(P) \]

because \( \phi_n \leq \phi_k \) and \( f_c(\cdot) \) is a strictly increasing function.

\[ \blacksquare \]

**V. Solution to the MMI Problem in the \( n \times m \) Case**

**A. Greedy Algorithm for the MMI Problem**

In general, determining whether \( \psi \) is an aggregation of \( \phi \), or finding the optimal bin allocations allowing overstuffing, are both NP-hard problems [3], [4]. It follows that computing \( V(\phi, \psi) \), or equivalently, computing the maximum mutual information, is also NP-hard when \( m = 2 \). It is therefore plausible that the problem of computing \( V(\phi, \psi) \) continues to be NP-hard if \( 3 \leq m \leq n \). But we do not explore this issue further. Instead, we borrow a standard greedy algorithm for bin-packing with overstuffing from the computer science literature [21], known as ‘best fit,’ and adapt it to the current situation. We begin by arranging the elements of \( \psi \) in descending order. In general it is not necessary to sort the elements of \( \phi \).

Given \( \phi \in S_n, \psi \in S_m \) with \( m < n \), proceed as follows:

1) Set \( s = 1 \), where \( s \) is the round counter. Define \( n_s = n, m_s = m, \phi_s = \phi, \psi_s = \psi \).

2) Place each element of \( \phi \) in the bin with the largest unused capacity. If a particular component \( (\phi_s)_i \) does not fit into any bin, assign the index \( i \) to an overflow index set \( K_s \).

3) When all elements of \( \phi_s \) have been processed, let \( I_1^{(s)}, \ldots, I_m^{(s)} \) be the indices from \( \{1, \ldots, n_s\} \) that have been assigned to the various bins, and let \( K_s \) denote the set of indices that cannot be assigned to any bin. If \( |K_s| > 1 \) go to Step 4; otherwise go to Step 5.

4) Define \( \alpha_1^{(s)}, \ldots, \alpha_m^{(s)} \) to be the unutilized capacities of the \( m_s \) bins, and define \( \alpha^{(s)} = [\alpha_1^{(s)}, \ldots, \alpha_m^{(s)}] \). Then the total unutilized capacity \( c_s := \alpha^{(s)} e_{m_s} \) satisfies

\[ c_s = \sum_{j=1}^{m_s} \alpha_j^{(s)} = \sum_{i \in K_s} (\phi_s)_i. \tag{24} \]

Since each \( (\phi_s)_i, i \in K_s \) does not fit into any bin, it is clear that \( (\phi_s)_i > \alpha_j^{(s)}, \forall i, j \). In turn this implies that \( |K_s| < m_s \). Next, set \( n_{s+1} = m_s, m_{s+1} = |K_s| \), and define

\[ \phi_{s+1} = 1/c_s (\phi_s) \in S_{m_{s+1}}, \psi_{s+1} = 1/c_s [(\phi_s)_i] \in S_{m_{s+1}}. \]

Increment the counter and go to Step 2.

5) When this step is reached, \( |K_s| \) is either zero or one. If \( |K_s| = 0 \), then it means that \( \psi \) is a perfect aggregation of \( \phi \). So define \( V_s = 0 \) and proceed as below. If \( |K_s| = 1 \), then only one element of \( \phi_s \), call it \( (\phi_s)_k \), cannot be packed into any bin, and this component must equal \( c_s \). So let

\[ v_s = 1/c_s \alpha^{(s)} \in S_{m_s}, V_s = c_s H(v_s), \]

\[ U_s = V_s + H(\phi_s) - H(\psi_s). \]

Define \( P_s \in S_{n_s \times m_s} \) by

\[ p_i = b_j \text{ if } i \in I_j^{(s)} \]

where \( b_j \) is the \( j \)-th unit vector with \( m_s \) components. Then \( V_s \) is the minimum value of \( J_{\phi_s} (\cdot) \), and \( P_s \) achieves that minimum. Next, define \( Q_s \in S_{m_s \times n_s} \) by

\[ Q_s = [\text{diag}(\psi_s)]^{-1} P_s^T \text{Diag}(\phi_s). \]

Then it follows from (16) that \( Q_s \) minimizes \( J_{\phi_s} (\cdot) \), and that \( U_s \) is the value of that minimum.

6) In this step, we invert all of the above steps by transposing \( Q_{s+1} \), applying the transformation in (2), and embedding the resulting matrix into \( P_s \). We also correct the cost function using (16). Decrement the counter \( s \) and recall that \( m_s = n_{s+1} \). Recall the unutilized capacity \( c_s \) defined in (24) which has been found during the forward iteration, and define

\[ V_s = c_s U_{s+1}, U_s = V_s + H(\phi_s) - H(\psi_s). \]

714
Define $P_s \in \mathbb{S}_{n_s \times m_s}$ by

$$p_i = b_j \text{ if } i \in I(s)$$

$$p_i = \text{i-th row of } Q_{s+1}.$$ 

If $s = 1$, halt; otherwise repeat the step.

B. Computational Complexity

The computational complexity of algorithm is easy to bound. The first step is to sort the elements of $\psi$, which has complexity $O(m^2)$ if we insist on an exact answer or $O(m \log m)$ if we use a randomized algorithm like quick sort. We use the latter bound here. In each step of the best fit algorithm, the bin in which the current element of $\phi$ has been placed has maximum capacity before placing, but necessarily after placing. So it needs to moved into the right place. Since the rest of the bins are still in descending order of capacity, this can be achieved in $O(\log m)$ steps using a bisection search. And this has to be done $n$ times. So once $\psi$ is sorted, one run of the best fit algorithm has complexity $O(n \log m)$, which dominates the complexity $O(m \log m)$ of sorting $\psi$, since $m \leq n$. Since the size of the problem decreases at each round, at worst we may have to run the best fit algorithm $m - 1$ times. Moreover, after the first round, the size of the problem is not any larger than $m \times (m - 1)$. So the overall complexity of the greedy algorithm is no worse than $O(n \log m) + mO(m \log m) = O((n+m^2) \log m)$. The fact that the complexity is only linear in $n$ is heartening.

In [18], the application of the greedy algorithm is illustrated on a large $40 \times 10$ example that needs to go through three rounds.

VI. Conclusions

In this paper we have studied the problem of defining a metric distance between two probability distributions over distinct finite sets of possibly different cardinalities. Along the way, we have formulated the problem of constructing a joint distribution on the product of the two sets, which has the two given distributions as its marginals, in such a way that the joint distribution has minimum entropy. While the problem of maximizing mutual information is occasionally discussed in the literature, this specific problem does not appear to have been studied earlier. This problem turns out to be NP-hard, so we reformulated the problem as a bin-packing problem with overstuffing, and adapt the best fit algorithm for bin-packing, leading to an upper bound on the distance between the two given distributions. The complexity of this algorithm is $O((n+m^2) \log m)$, where $n$ is the larger of the two cardinalities and $m$ is the smaller.

Applications of the metric to the problem of order reduction are presented in a companion paper [19]. A full length version that combines both papers and is under review for journal publication can be found at [18].

REFERENCES