GENERALIZING FANO'S INEQUALITY

Te Sun Han
Dept. Information Systems
Senshu University
Kawasaki 214, Japan

Sergio Verdú
Dept. Electrical Eng.
Princeton University
Princeton, NJ 08544

One of the most useful results in the Shannon theory is the lower bound on mutual information due to Fano

Theorem 1. Suppose that X and Y are random variables that satisfy:

a) X and Y take values on the same finite set with cardinality M

b) either X or Y is equiprobable.

Then,

$$I(X;Y) \geq P[X=Y] \log M - h(P[X=Y]) \tag{1}$$

where h is the binary entropy function.

The purpose of this paper is to give a more general version of the lower bound in Theorem 1 by dropping its assumptions.

The restriction that X and Y take values on the same set is made throughout for convenience in expressing the results. It is easy to see from the mutual information data processing theorem that it can be lifted by replacing $P[X=Y]$ by $P[X=\phi(Y)]$ where ϕ is an arbitrary function mapping the space of Y to the space of X. The assumption that at least one of the random variables is equiprobable is a nontrivial restriction, which we want to eliminate.

The power of Theorem 1 stems from its ability to lower bound the mutual information between two random variables in terms of a single parameter computable from their joint distribution: the probability that the random variables take the same value. Since it is possible to construct independent (nonequiprobable) random variables (X,Y) for any arbitrarily specified $P[X=Y]$, it is apparent that dropping assumption b) of Theorem 1 will require a lower bound that depends on the distribution of X and Y not only through $P[X=Y]$, but through some other, hopefully simple, quantity.

Consider the following result.

Theorem 2. Define the binary divergence function $d(x\|y)$ as the divergence between the two-mass distributions $(x, 1-x)$ and $(y, 1-y)$. If X and Y take values on the same set, then

$$I(X;Y) \geq d(P[X=Y] \,\|\, P[X=\bar{Y}]), \tag{2}$$

where $\bar{Y}$ is independent of X and has the same distribution as Y. Furthermore, equality holds in (2) if and only if

$$P_{XY}(x,y) = \begin{cases} \alpha P_X(x)P_Y(y) & x = y \\ \beta P_X(x)P_Y(y) & x \neq y \end{cases} \tag{3}$$

This work was supported in part by the Office of Naval Research under Grant N00014-90-J-1734.

Note that

$$P[X=\bar{Y}] = \sum_{\omega\in\Omega} P_X(\omega)P_Y(\omega) \tag{4}$$

i.e., the inner product between the marginals of X and Y which, in many cases is easy to obtain from the description of X and Y.

Condition (3) implies that the marginals are either nonoverlapping or both equiprobable.

We will now loosen (2) by applying the following lower bound on binary divergence

$$d(x\|y) \geq x \log \frac{1}{y} - h(x) \tag{10}$$

to Theorem 2, resulting in the following generalization of Theorem 1:

Theorem 3. If X and Y take values on the same set, then

$$I(X;Y) \geq P[X=Y] \log \frac{1}{P[X=\bar{Y}]} - h(P[X=Y]) \tag{11}$$

$$\geq P[X=Y] \log \frac{1}{\max_{\omega\in\Omega} P_X(\omega)} - h(P[X=Y]) \tag{12}$$

where by symmetry we can replace $\max_{\omega\in\Omega} P_X(\omega)$ by $\max_{\omega\in\Omega} P_Y(\omega)$.

It is tempting to strengthen the lower bound in Theorem 3 with

$$I(X;Y) \geq P[X=Y]\, H(X) - h(P[X=Y]). \tag{!?}$$

However, counterexamples to (!?) can be found. It is possible to modify the incorrect bound (!?) in terms of entropy and obtain the following result.

Theorem 4. Assume that X and Y take values on the same set and denote

$$p = \inf_{\omega\in\Omega} P[X=Y \mid X=\omega] = \inf_{\omega\in\Omega} P_{Y|X}(\omega|\omega) \tag{13}$$

Then,

$$I(X;Y) \geq p\, H(X) - h(P[X=Y]) \tag{14}$$

If, in addition, $p > 1 - \frac{1}{e}$, then

$$I(X;Y) \geq p\, H(X) - h(p). \tag{15}$$