CHANNEL RESOLVABILITY

TE SUN HAN

Dept. Information Systems
Senshu University
Kawasaki 214, Japan

SERGIO VERDÚ

Dept. Electrical Eng.
Princeton University
Princeton, NJ 08544, USA

ABSTRACT

In the field of simulations, we are frequently encountered with the problem of random number generation (RNG). Suppose that we are given a stochastic system (channel) and that the objective of the simulation is to generate a random number as the output of the system, so as to be distributed according to the output statistics corresponding to the given inputs statistics. In doing so, a *basic* random number generator such as coin tossings, dice rollings, and etc., is usually used to generate the input sample path whose end is labelled with one of the possible inputs to the system. The important question is then raised: how many random bits are required per input sample? If we were to reproduce the given output statistics with *exact* precision, an infinite number of random bits would be required in most practical cases (for example, consider the continuous input distribution). Our real objective here is, instead, to approximate the output statistics with *arbitrary* precision. Therefore, the required number of random bits depends not only on the input statistics, but also on the degree of approximation required for the output statistics. We require the variational-distance between the true output distribution and the approximated output distribution to vanish *asymptotically*. This leads us to introduce a new concept in the Shannon theory: the *resolvability* of a system (channel) as the minimum number of random bits per input sample required to achieve arbitrary accurate approximation of the output statistics regardless of the actual input statistics. Intuitively, we can anticipate that the resolvability of a system depend on how

"noisy" it is. A coarse approximation of the input statistics of which the generation requires rather few bits will be enough when the system is very noise, because, then, the output can not reflect any fine detail contained in the input statistics.

Although the problem of approximation of this kind does not involve any coding or any sort of decoding (reproduction of information), its analysis as well as the results turns to be very Shannon-theoretic in nature, and of an intermediate character between source coding and channel coding. For example, one of our main conclusions is that resolvability is equal to Shannon capacity for the class of channels which satisfy the *strong converse*.

In order to give the formal definition to the above notion of "number of random bits per input sample", we consider two measures: *worst-case* one and *average* one. The former is defined by using a new measure, *resolution*, of randomness for distributions, and the latter is defined by the usual randomness measure, i.e., *entropy*. The above *resolvability* is formulated in terms of resolution, whereas the *mean-resolvability* is in terms of entropy. With these definitions, we shall show the general characterization of resolvability as the supremum of the *limsup in probability of information spectra* over all the possible input distributions, which has a nice dualty to the general characterization of channel capacity as the supremum of the *liminf in probability of information spectra* over all the possible input distributions.

It will be revealed that the approximation of output statistics has some intrinsic connections with following major problems in the Shannon theory: fixed-length/variable length source coding, channel coding and identification via channel. In particular, along the line of output approximation, we can show the very general formula for the minimum achievable (fixed-length) source coding rate. Moreover, as a simple consequence of the achievability part of the resolvability theorem, it is demonstrated that identification capacity is equal to channel capacity as long as the channel has a finite-input alphabet and satisfies the strong converse, which is a generalization of the results of Ahlswede-Dueck and Han-Verdu. Most of the main conclusions on resolvability hold also when the variational-distance approximation criterion is replaced by the normalized divergence. In this framework, in particular, we can provide the formal proof to a folk-theorem: *the output distribution due to any good channel code must approximate the output distribution due to the capacity-achieving input*.