The Source Coding Side of Secrecy

Paul Cuff – Princeton University

I. INTRODUCTION

Here we discuss achievability schemes and analysis techniques useful for source coding in adversarial settings. First we mention the equivalence between defining a “valid” joint distribution over all signals in a communication system and defining the behavior of the encoders and decoders. Then we show how to construct a joint distribution in reverse of the operation direction of the encoder, resulting in a communication system that is easy to analyze from the point of view of an optimal adversary. This relates to the work in [1] and [2].

II. CODING DEFINED BY A JOINT DISTRIBUTION

Questions of interest in information theory are usually defined in an operational context, involving encoders, decoders, messages, error probabilities, and distortions. All of these questions could be translated into statement and inquiries involving only probably distributions and their properties. For example, consider the definition of the rate-distortion function.

The standard definition of the rate-distortion function asks for the lowest communication rate such that there exists encoding functions and decoding functions that satisfy certain properties concerning the range of the encoding function and the resulting average distortion. We can alternatively state an equivalent definition for the rate-distortion function as a question about existence of probability distributions that satisfy certain conditions, as follows.

Rate-distortion Function: Given a source distribution $Q(x^n)$ and a distortion function $d(\cdot, \cdot)$, what is the minimum rate $R$ such that for all $\epsilon > 0$ and $n$ sufficiently large there exists a joint distribution $p(x^n, m, z^n)$ such that the cardinality of $M$ is less than $2^n R$, $X^n - M - X^n$ form a Markov chain, $p(x^n) = Q(x^n)$, and $E_{n} \sum_{i=1}^{n} d(x_i, \hat{x}_i) < D + \epsilon$? Let this be the value of the rate-distortion function $R(D)$.

The above restatement of the rate-distortion function is trivial and not very helpful. However, in some problems, particularly those involving an adversary, we find this form of the problem statement to be revealing. For one thing, the operation of the encoders and decoders are implicitly specified in the joint distribution of the signals. For example, the encoder in the rate-distortion function statement above operates according to the induced conditional distribution $p(m|x^n)$. But by changing the emphasis from defining how the encoder and decoder behave to instead defining a joint distribution to satisfy the constraints of the problem, a reverse-encoding construction is easily conceived. That is, we might find it useful to construct the inverse of the encoder, $p(x^n|m)$, to have certain properties rather than design the actual working of the encoder explicitly.

III. REVERSE-CHANNEL ENCODER

In [1] we characterize the best lossless source code that makes use of limited secret key to cause maximal distortion to an eavesdropper. An asymptotically optimal construction for the encoder is derived using two key concepts, discussed in the following two paragraphs. The communication is split into two parts, one message which has the secret key applied to it as a one-time pad, and the other non-secure message which is the crux of the analysis. The eavesdropper obtains the non-secure message, and we must be able to analyze the lowest distortion the eavesdropper can achieve given the received message.

The first key concept for constructing an optimal encoder is to design the encoder in reverse. Let $M$ be the non-secure message obtained by the eavesdropper, and let $X^n$ be the source sequence. The eavesdropper’s minimum average distortion when a particular message $m$ is observed depends on the distribution $p(x^n|m)$, which is the inverse of the encoder. Consider the following design. Using the standard technique of random codebook construction, let $U$ be an auxiliary random variable correlated with $X$ and construct a codebook of i.i.d. $U^n$ sequences indexed by $M$. Let $X^n$ be conditionally distributed as the output of a memoryless channel $\sim p(x|u)$ when the input to the channel is $U^n(M)$. The memoryless nature of this constructed conditional distribution $p(x^n|m)$ makes it trivial to characterize the minimum distortion incurred by the eavesdropper.

The last concept needed for the analysis is that of resolvability. In the construction above, if $M$ is uniformly distributed over a set of size $2^{nR}$, with $R > I(X;U)$, then the resulting distribution $p(x^n)$ will be close to the i.i.d. source distribution $Q(x^n)$ in total variation. Consequently, the constructed joint distribution is close in total variation to a valid joint distribution. We close this gap with some lemmas about total variation distance.

REFERENCES