CCIT Report #580 March 2006

Information Rates Subjected to State Masking

Neri Merhav and Shlomo Shamai (Shitz)
EE Dept., Technion – I.I.T., Haifa 32000, Israel
Email: [merhav,sshlomo]@ee.technion.ac.il

***Abstract*— We consider the problem of rate–R channel coding with causal/non–causal side information at the transmitter, under an additional requirement of minimizing the amount of information that can be learned from the channel output about the state sequence, which is defined in terms of the equivocation E (i.e., the mutual information between the state sequence and the channel output sequence). A single–letter characterization is provided for the achievable region of pairs $\{(R, E)\}$. Explicit results for the Gaussian case (Costa's dirty–paper channel) are derived in full detail.**

I. Introduction

The problem of information transfer via state–dependent channels is classical (see [9] for a partial review). One of the most interesting models is the case where the channel states are available at the transmitter either causally or non–causally. This framework has been fully characterized for i.i.d. states in famous studies by Shannon [14] and by Gel'fand and Pinsker (G–P) [7], repectively. These models, and in particular the G–P setting, have gained much interest in the last few years, mainly due to the wide scope application areas, such as watermarking, [3], [10], [12], [15], [11], multi–input–multi–output (MIMO) broadcast channels, [1], [2], network [8] and cooperative networks, [6], just to name a few applications.

One of the most interesting and well known examples the the G–P channel is the Gaussian setting where the states impact the channel additively. The surprising result by Costa [4] demonstrates that no loss in capacity is suffered no matter how strong that independent interfering state sequence is. Evidently, the many applications and the challenge here motivated much work in terms of actual coding strategies that come close to the optimum. These coding strategies (see, e.g., [21] and references therein), build on the insight of random binning which is the central mechanism in showing achievability in this problem [7], and can, in fact, be interpreted as practical binning strategies. In the Gaussian channel, nick–named ''dirty-paper" [4], efficient techniques based on modern codes were recently reported as well (see [16] and references therein). Source–channel coding aspects in the framework of state–dependent channel of this type are also considered [13], and the source–channel separation principle has been shown valid in various scenarios, in which the model itself is intimately related to the Wyner–Ziv (W–Z) source coding problem with side information at the decoder [20], and the G–P channel [7].

While in models addressed in [13], the source and channel states are assumed independent, this is not always the case. In some applications, the channel–state process is not inherently channel–related (like in fading), but may rather be an information–bearing signal on its own. The MIMO broadcast channel serves as a typical example, where a state sequence for one user is just the information–carrying sequence for another, and all produced at the same transmitter who addresses both users simultaneously [1]. In fact, these are exactly the cases where the justification to the non–causality is self–evident, as the transmitter controls the state sequence. The state sequence is often modelled as i.i.d. whether it is a specific codeword of a good codebook operating on a memoryless channel, which essentially mimics an i.i.d., or it is i.i.d., and it represents raw data, as say a systematic part of the information [13]. Furthermore, the state sequence may model also analogue information which is conveyed over the same channel with an overlayed digital part. This sort of applications gave rise to an interesting problem addressed by Sutivong *et. al.* [17], [18], where the role of the transmitter is two–fold: to transmit independent reliable information on the one hand, and to boost the quality of the state estimator at the receiver, which adopts a prescribed distortion measure, on the other. A coding scheme has been suggested in [18], which combines W–Z coding, based on the side information about the state available at the receiver side, and G–P coding which is used to convey the independent reliable rate, as well as the W–Z coded information. In the Gaussian case, it has been verified that this achievable tradeoff is in fact optimal [19]. In this specific case, a simple technique where the transmitter optimally power–shares between pure information transmission via the Costa strategy and simple state amplification achieves the optimal tradeoff.

In this paper, we focus on another aspect of the problem. The state sequence is referred to as undesired information that leaks to the receiver. It indeed could model a leakage in the system of, say, secret analogue (sampled) information, or stand for a codeword which is not intended to that receiver and is therefore to be concealed from the receiver side. Thus, the goal of the transmitter now is to try and mask this undesired information as much as possible on the one hand, and to transmit reliable independent data rate on the other. The amount of information that the receiver retrieves about the state sequence is measured by the blockwise mutual information (equivocation), as is customary in measuring the security of the cipher systems, in the literature of the Shannon theory. This measure guarantees that even if there is coding involved, only a small value of the associated mutual information limits the reliable information that the non–intended receiver can retrieve about the state sequence.

We characterize the tradeoff between the reliably transmit-