Identification under Random Processes *

Rudolf Ahlswede and Vladimir B. Balakirsky

*The work was supported in part by SFB-343, Universität Bielefeld, Germany

1 Introduction

Identification via channels was introduced in [1,2] as a problem of a reliable transmission of one of M messages to M receivers in such a way that each receiver decides whether it is his message, which was sent, or not. If a receiver misses his message then the decoding error of the first kind takes place, and if a receiver accepts a message which was sent for a different receiver, then the decoding error of the second kind takes place. An identification scheme should be constructed in such a way that the decoding error probabilities of the both kinds are small for all receivers.

A key idea of constructing good identification codes is an assignement of the probability distributions (PDs) to the messages instead of fixed codewords. Suppose we a given a discrete memoryless channel W having the input alphabet $\mathcal{X}$ and the output alphabet $\mathcal{Y}$, i.e., the probability to receive a vector $\mathbf{y} = (y^{(1)}, ..., y^{(n)}) \in \mathcal{Y}^n$, when a vector $\mathbf{x} = (x^{(1)}, ..., x^{(n)}) \in \mathcal{X}^n$ was transmitted, is defined as

$$W(\mathbf{y}|\mathbf{x}) = \prod_{t=1}^{n} W(y^{(t)}|x^{(t)}).$$

Definition 1 An $(n, M, \Lambda_1, \Lambda_2)$ ID code is a collection

$$\{ \ (Q_i(\cdot), \mathcal{D}_i), \ i = 1, ..., M \ \}$$

such that, for all $i, j = 1, ..., M$,

1) $Q_i(\cdot) = \{ \ Q_i(\mathbf{x}), \mathbf{x} \in \mathcal{X}^n \ \}$ is a PD;

2) $\mathcal{D}_j \subset Y^n$;

3) $\sum_{\mathbf{x}} Q_j(\mathbf{x}) \cdot W(\mathcal{D}_j|\mathbf{x}) \geq 1 - \Lambda_1$;

4) $\sum_{\mathbf{x}} Q_i(\mathbf{x}) \cdot W(\mathcal{D}_j|\mathbf{x}) \leq \Lambda_2$ if $i \neq j$.

The input distributions of an ID code can be realized if the sender has M collections of not necessarily distinct codewords. To send the i-th message, he selects one of the codewords of the i-th collection in accordance with the uniform distribution. Each receiver knows his collection and checks if the received vectors is likely to be generated by one of the codewords of this collection or not. The known results show that the number of messages that can be reliably transmitted using an ID code turns out to be doubly exponential in the blocklength n [1].

We will consider the system of information transmission given in Fig.1, where the sender and the receivers have an access to a public random process and get correlated binary sequences $\mathbf{x}^*$ and $\mathbf{y}^*$ of length k before the sender generates a codeword, depending of the message i, and transmits it over a memoryless channel W. The probability to receive a pair $(\mathbf{x}^*, \mathbf{y}^*)$ is defined as

$$P(\mathbf{x}^*, \mathbf{y}^*) \quad = \quad 2^{-k} p^{d_H(\mathbf{x}^*, \mathbf{y}^*)} (1-p)^{k - d_H(\mathbf{x}^*, \mathbf{y}^*)}, \tag{1.1}$$