Common Randomness in Information Theory and Cryptography
Part II: CR capacity

Rudolf Ahlswede
Universität Bielefeld
Fakultät für Mathematik
Postfach 100131
33501 Bielefeld
Germany

Imre Csiszár *
Mathematical Institute of the
Hungarian Academy of Sciences
P.O. Box 127
H-1364 Budapest
Hungary

Abstract

The CR capacity of a two-teminal model is defined as the maximum rate of common randomness that the terminals can generate using resources specified by the given model. We determine CR capacity for several models, including those whose statistics depend on unknown parameters. The CR capacity is shown to be achievable robustly, by common randomness of nearly uniform distribution no matter what the unknown parameters are. Our CR capacity results are relevant for the problem of identification capacity, and also yield a new result on the regular (transmission) capacity of arbitrarily varying channels with feedback.

Key words: common randomness, identification capacity, correlated sources, arbitrarily varying channel, feedback, randomization.

*I. Csiszár was partially supported by the Hungarian National Foundation for Scientific Research, Grant T16386.

1 Introduction

Suppose two terminals, called Terminal $\mathcal{X}$ and Terminal $\mathcal{Y}$, have resources such as access to side information and communication links that allow them to observe and (perhaps cooperatively) generate certain random variables (RV's). The permissible rules for this are specified by the particular model, but it is always assumed that the terminals have unrestricted computational power, thus the RV's that can be generated and observed at a terminal at a given time include, as a minimum, all functions of the RV's previously observed there. Common randomness (CR) of $\mathcal{X}$ and $\mathcal{Y}$ means, intuitively, a RV generated by them and observable to both, perhaps with a small probability of error.

A RV generated by a terminal is not necessarily observable there, e.g., when Terminal $\mathcal{X}$ inputs a RV X into a noisy channel to Terminal $\mathcal{Y}$, he thereby generates an output Y observable only at $\mathcal{Y}$. If Terminal $\mathcal{X}$ suitably encodes the RV X he wants to transmit, enabling $\mathcal{Y}$ to decode, then this X will represent CR. If noiseless feedback from $\mathcal{Y}$ to $\mathcal{X}$ is available then the output Y will always represent CR.

In Part 1 [7] we were interested in CR under an additional secrecy constraint, with the motivation that the generated CR will be used as an encryption key. In this paper we do not require secrecy, and just study the maximum amount of CR afforded by a given model, the amount measured by entropy. The most convenient form of CR is uniform common randomness (UCR), i.e., CR represented by a uniformly (or nearly uniformly) distributed RV. For the type of models we will consider, the maximum attainable amount of CR and UCR will be asymptotically the same.

As a very simple example, suppose that there is a DMC from Terminal $\mathcal{X}$ to Terminal $\mathcal{Y}$, Terminal $\mathcal{X}$ can randomize (= can generate RV's with arbitrary distributions), and can input into the DMC any random sequence X^n he has generated (of given "large" length n). Terminal $\mathcal{Y}$ can observe the output Y^n but the terminals have no other resources. It is intuitively clear that in this case $\mathcal{X}$ has to chose X^n to be uniformly distributed on the $\approx \exp(nC)$ codewords of an optimum code; then $\mathcal{Y}$ can decode, and the achieved $\approx nC$ amount of CR is best possible. If noiseless feedback is available, it is better for $\mathcal{X}$ to send independent repetitions of a RV X that produces maximum output entropy $H(Y)$. As now $\mathcal{X}$ can observe Y^n, in this way CR of amount $nH(Y)$ results, clearly the largest possible. Notice that here, too, the optimum could (almost) be attained by a nearly uniform RV, obtained by applying a compression code to Y^n.

As a combinatorial example, let $\mathcal{G}$ be a bipartite graph with vertex sets $\mathcal{X}$ and $\mathcal{Y}$ (we continue the practice of Part 1 that the symbols of the terminals also denote sets assigned to them). Nature selects an edge $(x, y) \in \mathcal{G}$ at random, Terminal $\mathcal{X}$ observes x, Terminal $\mathcal{Y}$ observes y. The terminals can communicate over a noiseless channel, but at most b binary digits may be transmitted, in any number of rounds. No other resources are available (above the minimum described in the first paragraph), in particular, neither terminal can randomize. Then, clearly, $\log|\mathcal{G}|$ is an upper bound to CR, which can be attained iff the communication complexity $C_\infty(\mathcal{H}, P_\mathcal{V}, P_\mathcal{E})$ does not exceed b (with the notation of [17]); here $\mathcal{H}$ denotes the hypergraph with vertex set $\mathcal{V} = \mathcal{X}$ and edge set $\mathcal{E}$ consisting of the sets $\{x : (x, y) \in \mathcal{G}\}$, $y \in \mathcal{Y}$. It may be an interesting study in communication complexity