NEW DIRECTIONS IN THE THEORY OF IDENTIFICATION VIA CHANNELS

RUDOLF AHLSWEDE [1] AND ZHEN ZHANG [2]

1.
Universität Bielefeld
Fakultät für Mathematik
Postfach 100131
33501 Bielefeld
Germany

2.
Communication Sciences Institute
University of Southern California
Los Angeles, CA 90089–2565
Research supported in part by
NSF Grant NCR–920 5265 and
SFB 343, Diskrete Strukturen
in der Mathematik, Bielefeld

Abstract

We study two problems in the theory of identification via channels. The first problem concerns the identification via channels with noisy feedback. Whereas for Shannon's transmission problem the capacity of a discrete memoryless channel does not change with feedback, we know from [3] and [4] that the identification capacity is affected by feedback. We study its dependence on the feedback channel. We prove both, a direct and a converse, coding theorem. Although a gap exists between the upper and lower bounds provided by these two theorems, the results of [3] and [4], namely the result for channels without feedback and the result for channels with complete feedback, are all special cases of these two new theorems, because in these cases the bounds coincide.

The second problem is the identification via wiretap channels. A secrecy identification capacity is defined for the wiretap channel in analogy to the definition of [1]. A "Dichotomy Theorem" is proved which says here that the second order secrecy identification capacity is the same as Shannon's capacity for the main channel as long as the secrecy transmission capacity of the wiretap channel is not zero, and zero otherwise.

Equivalently we can say that the identification capacity is not lowered by the presence of a wiretapper as long as one bit can be transmitted (or identified) correctly with arbitrarily small error probability. This is in strong contrast to the case of transmission.

Key Words. Cryptography, Identification, Channel Capacity, Wiretap Channel, Noisy Feedback.