J Autom Reasoning
DOI 10.1007/s10817-013-9298-1

Formalization of Shannon's Theorems

Reynald Affeldt · Manabu Hagiwara · Jonas Sénizergues

Received: 1 May 2013 / Accepted: 27 November 2013

Abstract The most fundamental results of information theory are Shannon's theorems. These theorems express the bounds for (1) reliable data compression and (2) data transmission over a noisy channel. Their proofs are non-trivial but are rarely detailed, even in the introductory literature. This lack of formal foundations is all the more unfortunate that crucial results in computer security rely solely on information theory: this is the so-called "unconditional security". In this article, we report on the formalization of a library for information theory in the SSReflect extension of the Coq proof-assistant. In particular, we produce the first formal proofs of the source coding theorem, that introduces the entropy as the bound for lossless compression, and of the channel coding theorem, that introduces the capacity as the bound for reliable communication over a noisy channel.

Keywords Information theory · Shannon's theorems · Noisy-channel coding theorem · Coq · SSReflect

This article is a revised and extended version of a conference paper [1].

This work was essentially carried out when the second and third author were affiliated with Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Japan.

R. Affeldt (✉)
Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Tsukuba, Ibaraki, Japan
e-mail: reynald.affeldt@aist.go.jp

M. Hagiwara
Department of Mathematics and Informatics, Faculty of Science, Chiba University, Chiba, Japan

J. Sénizergues
École Normale Supérieure de Cachan, Cachan, France

Published online: 11 December 2013