FORMAL VERIFICATION OF SHANNON'S THEOREMS

REYNALD AFFELDT*, MANABU HAGIWARA, JONAS SENIZERGUES

The most fundamental results of information theory are Shannon's theorems. These theorems express the bounds for reliable data compression and transmission over a noisy channel. Their proofs are non-trivial but 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 (the so-called "unconditional security"). In this presentation, 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).