Computer Science > Information Theory

Assisted Common Information with an Application to Secure Two-Party Sampling

Vinod M. Prabhakaran, Manoj M. Prabhakaran

(Submitted on 6 Jun 2012)

In this paper we generalize the notion of common information of two dependent variables introduced by G\'acs & K\"orner. They defined common information as the largest entropy rate of a common random variable two parties observing one of the sources each can agree upon. It is well-known that their common information captures only a limited form of dependence between the random variables and is zero in most cases of interest. Our generalization, which we call the Assisted Common Information system, takes into account almost-common information ignored by G\'acs-K\"orner common information. In the assisted common information system, a genie assists the parties in agreeing on a more substantial common random variable; we characterize the trade-off between the amount of communication from the genie and the quality of the common random variable produced using a rate region we call the region of tension.

We show that this region has an application in deriving upperbounds on the efficiency of secure two-party sampling, which is a special case of secure multi-party computation, a central problem in modern cryptography. Two parties desire to produce samples of a pair of jointly distributed random variables such that neither party learns more about the other's output than what its own output reveals. They have access to a set up - correlated random variables whose distribution is different from the desired distribution - and noiseless communication. We present an upperbound on how efficiently a given set up can be used to produce samples from a desired distribution by showing a monotonicity property for the region of tension: a protocol between two parties can only lower the tension between their views. Then, by calculating the bounds on the region of tension of various pairs of correlated random variables, we derive state-of-the-art bounds on the efficiency of secure two-party sampling.

Subjects: **Information Theory (cs.IT)**; Cryptography and Security (cs.CR)
Cite as: **arXiv:1206.1282 [cs.IT]**
(or **arXiv:1206.1282v1 [cs.IT]** for this version)

Submission history

From: Manoj Prabhakaran [view email]
[v1] Wed, 6 Jun 2012 17:25:57 GMT (332kb,D)

Which authors of this paper are endorsers?