Peres, Yuval

Iterating von Neumann's procedure for extracting random bits. (English) Zbl 0754.60040

Ann. Stat. 20, No. 1, 590-597 (1992).

Let $\{X_i\}_{i=1,2,\ldots,n}$ be a sequence of independent random variables with $p = P(X_i = 0) \neq 1/2$ and $q = 1 - p = P(X_i = 1)$, where p is unknown. The X_i's are so-called random biased bits. Without assuming prior knowledge of p the first consideration is to extract from the X_i's as many as possible independent unbiased bits by the help of a simple procedure by von Neumann (1951). Given n biased bits, this procedure extracts approximately $np(1-p)$ unbiased bits.

The aim of this paper is to show that the number of unbiased bits produced by iterating this procedure is arbitrarily close to the entropy bound. The proof is based on a functional equation satisfied by the entropy function. In the last section an extension to exchangeable processes and a discussion on the relationship to the Keane-Smorodinsky finitary codes are given.

Reviewer: L.Paditz (Dresden)

MSC:

60G35 Signal detection and filtering (aspects of stochastic processes)
94A17 Measures of information, entropy
60G09 Exchangeability for stochastic processes

Keywords:

exchangeability; random biased bits; number of unbiased bits; exchangeable processes; Keane-Smorodinsky finitary codes

Full Text: DOI