Analysis of Peres' algorithm and its streaming versions for random number generation

林昭京*、姚怡慶
中央研究院統計科學研究所

Abstract

von Neumann (1951) introduced a simple algorithm for generating independent and unbiased random bits by tossing a coin of unknown bias p. While his algorithm fails to attain the entropy bound, Peres (1992) showed that the entropy bound can be attained asymptotically by iterating von Neumann's algorithm. Specifically, Peres showed that $\lim_{n\to\infty} \frac{1}{n} b(n,p) = h(p)$ uniformly in $p \in (0,1)$, where $b(n,p)$ denotes the expected number of unbiased output bits generated when Peres' algorithm is applied to an input sequence $(X_1, \ldots, X_n)$ with X_i being the outcome of the ith coin toss, and $h(p) = -p\log p - (1-p)\log(1-p)$ (the Shannon entropy of each X_i). We consider the (second-order) behavior of $nh(p) - b(n,p)$ as $n \to \infty$. For $p = \frac{1}{2}$, it is shown that $\lim_{n\to\infty} \log[n - b(n, \frac{1}{2})]/\log n = \log[\frac{1+\sqrt{5}}{2}]$. Some open problems on the asymptotic behavior of $nh(p) - b(n,p)$ are briefly discussed. The original Peres' algorithm is not streaming in the sense that some of the output bits generated from $(X_1, \ldots, X_n)$ (the first n coin tosses) may be placed after the output bits induced by X_{n+1}. We introduce a binary tree representation of Peres' algorithm, based on which we further introduce a class of streaming versions of Peres' algorithm in terms of orderings of the nodes of the binary tree. We show by example that in general a streaming version of Peres' algorithm fails to generate unbiased output bits. However, based on a special node ordering, the corresponding streaming version of Peres' algorithm is shown to be unbiased.

Keywords: entropy, analysis of algorithms, Elias' extractor, Peres' extractor, von Neumann's extractor, superadditivity, streaming algorithm, status tree.