Switching Networks for Generating Random Permutations

Artur Czumaj
New Jersey Institute of Technology

Przemka Kanarek, and Krzysztof Loryś
University of Wrocław

Mirosław Kutyłowski
Wrocław University of Technology and AMU Poznań

Abstract

A switching network may be used for generating random permutations. After setting the values of switches, the network performs a fixed permutation of the input data. If the switches are set at random, then in some sense the switching network performs a random permutation. Our goal is to design architectures, for which the probability distribution on the set of permutations defined by the switching network is almost uniform.

We present a construction of a switching network with n inputs with a depth polynomial in $\log n$ so that the variation distance between the uniform distribution on the set of all permutations and the probability distribution defined by the network is $O(\frac{1}{n})$.

Our construction is based on path coupling method for showing rapid mixing property of stochastic processes. It is a convincing evidence for elegance and power of this technique.

As a surprising corollary of our construction we get an EREW PRAM algorithm for generating random permutations with runtime $\Theta(\log \log n)$. This is unexpected since some "easier" problems like establishing one value out of two requires $\Omega(\log n)$ steps.