TWO-FACED PROCESSES AND PSEUDORANDOM NUMBER GENERATORS

Boris Ryabko[1] *and Nadezhda Savina*[2]

[1]Institute of Computational Technologies of Siberian Branch of RAS,
Novosibirsk State University,
Novosibirsk, Russia, boris@ryabko.net
[2] Novosibirsk Humanitarian Institute, Novosibirsk, Russia, nnsavina@mail.ru

ABSTRACT

We describe binary-alphabet random processes whose Shannon entropy is less than 1 bit (per letter), but the frequency of occurrence of any word $u \in \{0,1\}^*$ goes to $2^{-|u|}$. It gives a possibility to construct pseudorandom number generators which have proven properties. In turn, this possibility is important for applications such as those in cryptography.

We describe analogical processes for any finite alphabet and carried out some experiments in which low-entropy sequences are transformed into two-faced sequences.