Pseudorandomness of binary threshold sequences derived from multiplicative inverse

László Mérai

Department of Computer Algebra, Eötvös Loránd University, Budapest, Hungary

merai@cs.elte.hu

Let p be a prime and $c_1, c_2, \ldots, c_h \in \mathbb{Z}_p$ be fixed elements. For initial values $x_1, \ldots, x_h \in \mathbb{Z}_p$ consider the sequence (x_n) defined by the linear recursion

$$x_n = c_1 x_{n-1} + \ldots + c_h x_{n-h}, \quad n > h.$$

The aim of the talk is to study the pseudorandom properties of the following finite binary sequence $E_T = \{e_1, e_2, \ldots, e_T\} \in \{1, -1\}^T$ built from the linear recursive sequence (x_n) by the rule

$$e_n = \begin{cases} 1 & \text{if } p \nmid f(x_n) \text{ and } 0 < f^{-1}(x_n) < p/2 \\ -1 & \text{otherwise,} \end{cases}$$

where $f^{-1}(x_n)$ is the multiplicative inverse of $f(x_n)$ modulo p.