Niederreiter, Harald

Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences. (English) Zbl 0641.65005

General algebra, Proc. Conf., Salzburg/Austria 1986, Contrib. Gen. Algebra 5, 221-233 (1987).

[For the entire collection see Zbl 0626.00009.]

Relationships between continued fraction expansions for formal power series and various theoretical investigations on pseudorandom sequences are discussed. Two types of pseudorandom sequences are considered: (i) sequences of uniform pseudorandom numbers generated by the digital multistep (or Tausworthe) method; (ii) keystream sequences in the binary field F_2 for cryptographic applications. The discussion of (i) is based on earlier results of the author, in particular those in Monatsh. Math. 103, 269-288 (1987; Zbl 0624.12011). Consequences for the calculation of optimal parameters in the digital multistep method were studied by *G. L. Mullen* and the author [Computing 39, 155-163 (1987)]. Concerning (ii), connections between the linear complexity profile of a keystream sequence and the continued fraction expansion of its generating function are established. This yields a new proof of the characterization of binary sequences with perfect linear complexity profile. Considerable refinements of the results on linear complexity profile have been obtained more recently by the author [Advances in Cryptology - EUROCRYPT '87, Lecture Notes in Computer Science 304, 37-51 (1988)].

Reviewer: H.Niederreiter

MSC:

65C10 Random number generation in numerical analysis
30B70 Continued fractions; complex-analytic aspects
13F25 Formal power series rings
94A99 Communication, information

Keywords:

Tausworthe method; continued fraction expansions; formal power series; pseudorandom sequences; uniform pseudorandom numbers; keystream sequences; digital multistep method; linear complexity profile