

Year: 2011

Vol.: 79

Fasc.: 3-4

Title: Measures of pseudorandomness of families of binary lattices, I (Definitions, a construction using quadratic characters)

Author(s): Katalin Gyarmati , Christian Mauduit and András Sárközy

In the last 15 years a new constructive theory of pseudorandomness of binary sequences has been developed. Later this theory was extended to n dimensions, i.e., to the study of pseudorandomness of binary lattices. In the applications it is not enough to consider single binary sequences, one also needs information on the structure of large families of binary sequences with strong pseudorandom properties. Thus the related notions of family complexity, collision and avalanche effect have been introduced. In this paper our goal is to extend these definitions to binary lattices, and we will present constructions of large families of binary lattices with strong pseudorandom properties such that these families also possess a nice structure.

Address:

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
Pázmány Péter sétány 1/C
H-1117 Budapest
Hungary

Address:

Christian Mauduit
Institut de Mathématiques de Luminy
CNRS, UMR 6206
163 avenue de Luminy, Case 907
F-13288 Marseille Cedex 9
France

Address:

András Sárközy
Eötvös Loránd University
Department of Algebra and Number Theory
Pázmány Péter sétány 1/C
H-1117 Budapest
Hungary