Dai, Zongduo; **Feng, Xiutao**

Classification and counting on multi-continued fractions and its application to multi-sequences. (English) Zbl 1142.40001

Sci. China, Ser. F. 50, No. 3, 351-358 (2007).

Summary: In the light of multi-continued fraction theories, we make a classification and counting for multi-strict continued fractions, which are corresponding to multi-sequences of multiplicity m and length n. Based on the above counting, we develop an iterative formula for computing fast the linear complexity distribution of multi-sequences. As an application, we obtain the linear complexity distributions and expectations of multi-sequences of any given length n and multiplicity m less than 12 by a personal computer. But only results of $m = 3$ and 4 are given in this paper.

MSC:

40A15 Convergence and divergence of continued fractions
40B05 Multiple sequences and series (should also be assigned at least one other classification number in this section)
94A55 Shift register sequences and sequences over finite alphabets in information and communication theory

Keywords:

multi-strict continued fractions; multi-sequences; linear complexity distribution

Full Text: DOI

References:

[1] Rueppel R A. Analysis and Design of Stream Cipher. Berlin: Springer-Verlag, 1986 · Zbl 0618.94001

[2] Feng X T, Dai Z D. Expected value of the linear complexity of two-dimensional binary sequences. SETA 2004, LNCS 3486, 2005, 113–128 · Zbl 1145.94416

[3] Wang L P, Niederreiter H. Enumeration results on the joint linear complexity profile of multi-sequences, finite fields and their application. doi: 10.1016/j.ffa.2005.03.005

[4] Niederreiter H, Wang L P. Proof of a conjecture on the joint linear complexity profile of multi-sequences. INDOCRYPT2005, LNCS3797, 2005, 13–22 · Zbl 1153.94338

[5] Dai Z D, Wang K P, Ye D F. m-Continued fraction expansions of multi-Laurent series. Adv Math (in Chinese), 2004, 33(2): 246–248

[6] Dai Z D, Wang K P, Ye D F. Multidimensional continued fraction and rational approximation. http://arxiv.org/abs/math.NT/0401141

[7] Dai Z D, Feng X T, Yang J H. Multi-continued fraction algorithm and generalized B-M algorithm over F 2. SETA 2004, LNCS 3486, 2005, 339–354 · Zbl 1145.94413

[8] Dai Z D, Wang K P, Ye D F. Multi-continued fraction algorithm on multi-formal Laurent Series. Acta Arith, 2006, 1–21 · Zbl 1146.11036

[9] Wan Z X. Geometry of Classical Group over Finite Fields. 2nd ed. Beijing: Science Press, 2002