Feng, Xiutao; **Wang, Quanlong**; **Dai, Zongduo**
Multi-sequences with d-perfect property. (English) Zbl 1075.68024
J. Complexity 21, No. 2, 230-242 (2005).

Summary: Sequences with almost perfect linear complexity profile are defined by *H. Niederreiter* [in: Proceedings of the Salzburg Conference 1986, Teubner, Stuttgart, Contrib. Gen. Algebra 5, 221–233 (1987; Zbl 0641.65005)]. *C. Xing* and *K. T. Lam* [IEEE Trans. Inf. Theory 45, 1267–1270 (1999; Zbl 0943.94008)] and *C. Xing* [J. Complexity 16, 661–675 (2000; Zbl 1026.94006)] extended this concept from the case of single sequences to the case of multi-sequences and further proposed the concept of d-perfect multi-sequences. In this paper, based on the technique of m-continued fractions due to Dai et al., we investigate the property of d-perfect multi-sequences and obtain a sufficient and necessary condition for d-perfect multi-sequences. We show that d-perfect multi-sequences are not always strongly d-perfect. In particular, we give an example to disprove the conjecture, posed by Xing (2000), on d-perfect multi-sequences.

MSC:

68P25 Data encryption (aspects in computer science)

Keywords:

Multi-sequences; Linear complexity profile; d-perfect; m-continued fraction

Full Text: DOI

References:

[1] Dai, Z.; Wang, K.; Ye, D., \textit{m}-continued fraction expansions of multi-Laurent series, Adv. math. (China), 33, 246-248, (2004)

[2] Z. Dai, K. Wang, D. Ye, Multidimensional Continued Fraction and Rational Approximation, http://arxiv.org/abs/math.NT/0401141.

[3] Lidl, R.; Niederreiter, H., Introduction to finite fields and their applications, (1986), Cambridge University Press Cambridge · Zbl 0629.12016

[4] H. Niederreiter, Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to General Algebra, Proceedings of the Salzburg Conference 1986, Vol. 5, Teubner, Stuttgart, 1987, pp. 221-233.

[5] H. Niederreiter, Sequences with almost perfect linear complexity profile, Advances in Cryptology-EUROCRYPT' 87, Lecture Notes in Computer Science, Vol. 304, Springer, Berlin, 1988, pp. 37-51.

[6] Rueppel, R.A., Analysis and design of stream ciphers, (1986), Springer Berlin · Zbl 0654.68044

[7] Stark, H., An introduction to number theory, (1979), MIT Press Cambridge, MA

[8] Xing, C.; Lam, K.Y., Sequences with almost perfect linear complexity profiles and curves over finite fields, IEEE trans. inform. theory, 45, 1267-1270, (1999) · Zbl 0943.94008

[9] Xing, C., Multi-sequences with almost perfect linear complexity profile and function fields over finite fields, J. complexity, 16, 661-675, (2000) · Zbl 1026.94006