Xing, Chaoping

Multisequences with almost perfect linear complexity profile and function fields over finite fields. (English) Zbl 1026.94006

J. Complexity 16, No. 4, 661-675 (2000).

Let $A = \{a_1, a_2, \cdots, a_m\}$ be a multisequence over the finite field $\mathbb{F}_q$ where $a_i = \{a_{i1}, a_{i2}, \cdots\}$ is an infinite sequence, and let $\{l_n(A)\}_{n=1}^{\infty}$ be the linear complexity profile of A. If $l_n(A) \geq \lceil \frac{m(n+1)-d}{m+1} \rceil$ for all n, A is called d-perfect for a positive integer d. A is called perfect if A is m-perfect. It is proved in this paper that A is perfect if and only if $l_n(A) = \lceil \frac{mn}{m+1} \rceil$. A construction of d-perfect multisequences is given in this paper by using a function field over a finite field. Let $\mathbf{F}$ be a global function field with the full constant field $\mathbb{F}_q$. For a place $\mathbb{Q}$ of degree m of $\mathbf{F}$, let $\mathbf{F}_{\mathbb{Q}} = \mathcal{O}_{\mathbb{Q}}/\mathcal{P}_{\mathbb{Q}}$ be the residue field of $\mathbb{Q}$, where $\mathcal{O}_{\mathbb{Q}}$, $\mathcal{P}_{\mathbb{Q}}$ are the integral ring and maximal ideal at $\mathbb{Q}$ respectively. Assume that t is a local parameter of $\mathbb{Q}$ with $\deg(t)_{\infty} = m + 1$. Choose m elements $x_1, x_2, \cdots, x_m \in \mathcal{O}_{\mathbb{Q}}$ such that $x_1(\mathbb{Q}), x_2(\mathbb{Q}), \cdots, x_m(\mathbb{Q})$ form an $\mathbb{F}_q$-basis of $\mathbf{F}_{\mathbb{Q}}$. For an element $y \in \mathcal{O}_{\mathbb{Q}}$, it can be expressed by a formal series

$$y = \sum_{j=0}^{\infty} \left(\sum_{i=1}^{m} a_{ij} x_i \right) t^j.$$

Put $a_i(y) = (a_{i1}, a_{i2}, \cdots)$ $(1 \leq i \leq m)$. Then it is proved that $A = (a_1, a_2, \cdots, a_m)$ is d-perfect where $d = \deg((y)_{\infty} \vee (x_1)_{\infty} \vee \cdots \vee (x_m)_{\infty})$. Some examples of this construction are given in the paper.

Reviewer: Pei Dingyi (Beijing)

MSC:

94A55 Shift register sequences and sequences over finite alphabets in information and communication theory
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
94A60 Cryptography

Keywords:

multi-sequences; linear complexity profile; perfect sequences; function field

Full Text: DOI

References:

[1] Kohel, D.R.; Ling, S.; Xing, C.P., Explicit sequence expansions, (), 308-317 · Zbl 1005.11064

[2] Niederreiter, H., Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to general algebra 5 (proc. Salzburg conf., 1986), (1987), Teubner Stuttgart, p. 221-233

[3] Niederreiter, H., Sequences with almost perfect linear complexity profile, (), 37-51

[4] Niederreiter, H.; Vielhaber, M., Linear complexity profiles: Hausdorff dimensions for almost perfect profiles and measures for general profiles, J. complexity, 13, 353-383, (1997) · Zbl 0934.94013

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

[6] Rueppel, R.A., Stream ciphers, (), 65-134

[7] Stichtenoth, H., Algebraic function fields and codes, (1993), Springer-Verlag Berlin · Zbl 0816.14011

[8] Xing, C.P.; 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.P.; Niederreiter, H.; Lam, K.Y.; Ding, C.S., Constructions of sequences with almost perfect linear complexity profile from curves over finite fields, Finite fields appl., 5, 301-313, (1999) · Zbl 0943.94005