Finite Fields and Their Applications 33 (2015) 175–186

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the complexity of a family of Legendre sequences with irreducible polynomials ☆

Katalin Gyarmati

Eötvös Loránd University, Department of Algebra and Number Theory, Budapest, Pázmány Péter st. 1/C, H1117, Hungary

ARTICLE INFO

Article history:
Received 17 July 2014
Received in revised form 30 October 2014
Accepted 2 November 2014
Available online 13 January 2015
Communicated by D. Panario

MSC:
primary 11K45
secondary 12E05

Keywords:
Pseudorandom
f-complexity
Irreducible polynomials

ABSTRACT

Ahlswede, Khachatrian, Mauduit and Sárközy [1] introduced the f-complexity measure ("f" for family) in order to study pseudorandom properties of large families of binary sequences. So far several families have been studied by this measure. In the present paper I considerably improve on my earlier result in [8], where the f-complexity measure of a family based on the Legendre symbol and polynomials over $\mathbb{F}_p$ is studied. This paper also extends the earlier results to a family restricted on irreducible polynomials.

1. Introduction

Finite pseudorandom binary sequences play a crucial role in cryptography, in particular they are used as *key* in the well-known and frequently used Vernam-cipher. Thus it is an important problem to decide whether a given binary sequence can be considered as a pseudorandom sequence or not. The classical approach to characterize

☆ Research partially supported by Hungarian National Foundation for Scientific Research, grant Nos. K100291 and NK104183, and the János Bolyai Research Fellowship.

E-mail address: gykati@cs.elte.hu.

http://dx.doi.org/10.1016/j.ffa.2014.11.004
1071-5797/

pseudorandomness is to use computational complexity. However this approach has certain weak points thus in 1997 Mauduit and Sárközy [15] introduced another quantitative and constructive approach towards pseudorandomness, and they introduced certain measures (called well-distribution and correlation measure of order ℓ) of pseudorandomness. See [15] for details. Since then many constructions have been given for finite binary sequences possessing strong pseudorandom properties in terms of these measures.

Moreover in the most applications one needs large families of sequences of this type. Goubin, Mauduit and Sárközy [6] succeeded in constructing large families of pseudorandom binary sequences with proved strong pseudorandom properties. The construction studied by them was the following:

Construction 1.1. *Let $K \geq 1$ be an integer and p be a prime number. If $f \in \mathbb{F}_p[x]$ is a polynomial with degree $1 \leq k \leq K$ and no multiple zeros in $\overline{\mathbb{F}}_p$, then define the binary sequence $E_p(f) = E_p = (e_1, \dots, e_p)$ by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1, \\ +1 & \text{for } p \mid f(n). \end{cases} \tag{1.1}$$

Let $\mathcal{F}(K, p)$ denote the set of all sequences obtained in this way.

Indeed, first Hoffstein and Lieman [12] proposed the use of polynomials f in (1.1) such that they are squarefree and neither even, nor odd, but they did not prove anything on the pseudorandom properties of the corresponding sequence $E_p(f)$. Goubin, Mauduit and Sárközy proved that under certain not too restrictive conditions on the polynomial f, the sequences constructed in this way have strong pseudorandom properties. Since then many other families have been constructed, but still this seems to be the most satisfactory construction.

Clearly for a polynomial $f \in \mathbb{F}_p[x]$ and an element $a \in \mathbb{F}_p^*$ the sequences $E_p(f)$ and $E_p(a^2 f)$ are the same. By this and the results of Tóth [17, Theorem 1] the size of $\mathcal{F}(K, p)$ equals twice of the number of monic squarefree polynomials of degree $\leq K$ for $K \leq \frac{p^{1/2}}{2}$. This number was estimated first by Carlitz [4] and as a conclusion we get $|\mathcal{F}(K, p)| = 2p^K$ for $K \leq \frac{p^{1/2}}{2}$. In general we have $|\mathcal{F}(K, p)| \leq 2p^K$.

In many applications of cryptography it is not enough to know that the family contains many binary sequences with strong pseudorandom properties; it is also important that the family has a "rich", "complex" structure, there are many "independent" sequences in it. Ahlswede, Khachatrian, Mauduit and Sárközy [1] introduced the notion of *f-complexity* ("f" for family) defined in the following way:

Definition 1.1. If $N, j \in \mathbb{N}$, $j \leq N$, $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_j) \in \{-1, +1\}^j$, $i_1, i_2, \dots, i_j$ are integers with $1 \leq i_1 < i_2 < \dots < i_j \leq N$ and $E_N = (e_1, e_2, \dots, e_N) \in \{-1, +1\}^N$ is a binary sequence such that