On the complexity of a family based on irreducible polynomials

Katalin Gyarmati

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 [7], 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 pseudorandomness is to use computational

2010 Mathematics Subject Classification: Primary: 11K45, Secondary: 12E05.

Keywords and phrases: pseudorandom, f-complexity, irreducible polynomials

Research partially supported by Hungarian National Foundation for Scientific Research, grants no. and K100291 and NK104183, the János Bolyai Research Fellowship.

complexity. However this approach has certain weak points thus in 1997 Mauduit and Sárközy [13] 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 [13] 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 [5] 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 zero in $\overline{\mathbb{F}}_p$, then define the binary sequence $E_p(f) = E_p = (e_1, \ldots, e_p)$ 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 [10] 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.

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

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \dots, e_{i_j} = \varepsilon_j, \tag{1.2}$$

then we say that the sequence E_N *satisfies the* specification (1.2).

Definition 1.2 *The* f-complexity *of a family* $\mathcal{F}$ *of binary sequences* $E_N \in \{-1, +1\}^N$ *is defined as the greatest integer* j *so that for any specification* (1.2) *there is at least one* $E_N \in \mathcal{F}$ *which satisfies it. The* f*-complexity of* $\mathcal{F}$ *is denoted by* $\Gamma(F)$. *(If there is no* $j \in \mathbb{N}$ *with the property above, then we set* $\Gamma(\mathcal{F}) = 0$.*)*

As it was shown in [1] we have:

Proposition 1.A (Ahlswede, Khachatrian, Mauduit, Sárközy)

$$\Gamma(\mathcal{F}) \le \frac{\log |\mathcal{F}|}{\log 2}.$$

From the opposite side it was shown in [1]:

Theorem 1.A (Ahlswede, Khachatrian, Mauduit, Sárközy)

$$\Gamma(\mathcal{F}(K, p)) \ge K. \tag{1.3}$$

By Proposition 1.A it is clear that

$$|\Gamma(\mathcal{F}(K, p)| \le \frac{\log |\mathcal{F}(K, p)|}{\log 2} \le \frac{K}{\log 2} \log p + 1. \tag{1.4}$$

The family complexity measure have been studied in several papers [2], [3], [4], [7], [8], [9], [12], [14], [16].

In [7] I improved on the bound (1.3) and proved the following:

Theorem 1.B

$$\Gamma(\mathcal{F}(K,p)) \geq \frac{K-1}{2\log 2}\log p - O(K\log(K\log p)). \tag{1.5}$$

We remark that for $K=1$ we also have $\Gamma(\mathcal{F}(K,p)) \gg \log p$, which result also follows from the proof of Theorem 1.B, or earlier, from Exercises 5.63 and 5.64 in Lidl and Niederreiter's book [11] (see below Lemma 3.1 and Lemma 3.2).

In this paper, answering a question of Gábor Halász I will prove a sharpening of my result Theorem 1.B: By (1.4) the bound in (1.5) is optimal apart from constant factor only for $K \leq p^{1/2}$. However in certain applications it is also important that we can achieve the optimal bound for families $\mathcal{F}(K,p)$ for larger K's. In order to achieve this I will restrict $\mathcal{F}(K,p)$ for a certain subfamily of it which contains sequences with even stronger pseudorandom properties but its f-complexity measure is still optimal even for K values much greater than the ones considered in [1], [5] and [7]. I propose the use of irreducible polynomials:

Definition 1.3 *Define* $E_p(f)$ *by* (1.1). *Let*

$$\mathcal{F}_{irred}(k,p) = \{E_p(f) : f \text{ is monic irreducible polynomial over } \mathbb{F}_p,$$
$$\deg\ f = k\}$$

The following proposition is an easy consequence of the proof of Theorem 1 in [5], and a stronger form of it is proved in Theorem 4 in [6].

Proposition 1.B *For* $E_p \in \mathcal{F}_{irred}(k,p)$ *we have*

$$W(E_p) < 10kp^{1/2}\log p,$$
$$C_\ell(E_p) < 10k\ell p^{1/2}\log p,$$

where the definitions of W and C_ℓ can be found in [13].

In the present paper I will prove that the f-complexity measure of $\mathcal{F}_{irred}(k,p)$ is optimal apart from constant factor:

Theorem 1.1 *Let $p \geq 19$ be a prime and k be an integer. Define $c = 1/2$ if $k \leq \frac{p^{1/4}}{10\log p}$ and $c = 5/2$ if $k > \frac{p^{1/4}}{10\log p}$ then*

$$\Gamma(\mathcal{F}_{irred}(k,p)) \geq \min\left\{p,\ \frac{k-c}{2\log 2}\log p\right\}. \tag{1.6}$$

This theorem shows that $\mathcal{F}_{irred}(k,p)$ can be very useful in the applications: By Proposition 1.B for $k = o(\frac{p^{1/2}}{\log p})$ every sequence in it has strong pseudorandom properties and by Theorem 1.1 for every k it has optimal f-complexity measure. Since $\mathcal{F}(K,p) \supset \mathcal{F}_{irred}(K,p)$ thus we also have

Corollary 1.1 *Let $p \geq 19$ be a prime and K be an integer. Define $c = 1/2$ if $K \leq \frac{p^{1/4}}{10\log p}$ and $c = 5/2$ if $K > \frac{p^{1/4}}{10\log p}$ then*

$$\Gamma(\mathcal{F}(K,p)) \geq \min\left\{p,\ \frac{K-c}{2\log 2}\log p\right\}.$$

This theorem considerably improves on Theorem 1.B and it is optimal apart from constant factor for every K and not only for small K's.

Acknowledgements. I would like to thank professors Gábor Halász and Harald Niederreiter for their valuable advice.

2 Auxiliary lemmas

In the proof of Theorem 1.1 we will need some lemmas on finite fields, these lemmas can be proved relatively easily, one or two of them can be considered as folklore. For the sake of completeness of the paper I will present the proofs of all these lemmas.

Let q be a prime power and denote $\mathbb{F}_q$ the finite field with q elements.

Definition 2.1 *For $\alpha \in \mathbb{F}_{q^n}$ the norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ is defined by*

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

Then $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is always an element of $\mathbb{F}_q$.

Definition 2.2 *A generator of the cyclic group $\mathbb{F}_q^*$ is called a* primitive element of $\mathbb{F}_q$.

Lemma 2.1 *Suppose that g is a primitive element of $\mathbb{F}_{q^n}$. Then $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g)$ is a primitive element of $\mathbb{F}_q$.*

Proof of Lemma 2.1. Let $h = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g)$. Then $h \in \mathbb{F}_q$. So $1, h, h^2, \ldots, h^{q-2} \in \mathbb{F}_q$. Here

$$1 = g^0,\ h = g^{(q^n-1)/(q-1)},\ h^2 = g^{2(q^n-1)/(q-1)}, \ldots,\ h^{q-2} = g^{(q-2)(q^n-1)/(q-1)}.$$

Since the exponents $0, (q^n-1)/(q-1), 2(q^n-1)/(q-1), \ldots, (q-2)(q^n-1)/(q-1)$ are between 0 and q^n-2 and they are distinct and g is a primitive elements of $\mathbb{F}_{q^n}$ we get $1, h, h^2, \ldots, h^{q-2}$ are distinct. Thus $h = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g)$ is a primitive element of $\mathbb{F}_q$.

Let g be a fixed primitive element of $\mathbb{F}_q$. For each $j = 0, 1, 2, \ldots, q-2$ the function

$$\chi_j(g^k) = e^{2\pi jk/(q-1)}$$

defines a multiplicative character of $\mathbb{F}_q$, and every multiplicative character of $\mathbb{F}_q$ is obtained in this way.

The order of a character χ of $\mathbb{F}_q$ is the smallest positive integer m such that $\chi^m(a) = 1$ for all $a \in \mathbb{F}_q^*$. Clearly, for all multiplicative character χ of order d there exists an integer $0 \le j \le d-1$ such that

$$\chi(g^k) = e^{2\pi jk/d}.$$

Lemma 2.2 *Let χ be a multiplicative character of $\mathbb{F}_{q^n}$ whose order is d and suppose that $d \mid q-1$ holds. Then there is a multiplicative character χ' of $\mathbb{F}_q$ of order d such that for every $\alpha \in \mathbb{F}_{q^n}$ we have*

$$\chi(\alpha) = \chi'(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)).$$

Proof of Lemma 2.2. Let g be a primitive element of $\mathbb{F}_{q^n}$. Then by Lemma 2.1 we have $h \stackrel{\text{def}}{=} N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g) = g^{(q^n-1)/(q-1)}$ is a primitive element of $\mathbb{F}_q$. Since χ is a multiplicative character of $\mathbb{F}_{q^n}$ of order d there exists an integer $0 \leq j \leq d-1$ such that

$$\chi(g^k) = e^{2\pi jk/d}.$$

Define the multiplicative character χ' of $\mathbb{F}_q$ of order d by

$$\chi'(h^k) \stackrel{\text{def}}{=} e^{2\pi jk/d}.$$

Write $\alpha \in \mathbb{F}_{q^n}^*$ of the form g^k. Then

$$\begin{aligned}\chi'(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)) &= \chi'(\alpha^{(q^n-1)/(q-1)}) = \chi'(g^{k(q^n-1)/(q-1)}) = \chi'(h^k) = e^{2\pi ijk/d} \\ &= \chi(g^k) = \chi(\alpha)\end{aligned}$$

and this completes the proof of Lemma 2.2.

Corollary 2.1 *Let p be a prime number and $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. Denote by γ the quadratic character of $\mathbb{F}_{p^n}$. Then for $\alpha \in \mathbb{F}_{p^n}^*$ we have*

$$\gamma(\alpha) = \left(\frac{N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)}{p}\right).$$

Definition 2.3 *Suppose that*

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{F}_{q^n}[x].$$

Define for $0 \leq s \leq n-1$

$$\tau_s(f)(x) \stackrel{def}{=} a_k^{q^s} x^k + a_{k-1}^{q^s} x^{k-1} + \cdots + a_0^{q^s} \in \mathbb{F}_{q^n}[x]$$

and let

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) \stackrel{def}{=} \tau_0(f) \cdot \tau_1(f) \cdot \tau_2(f) \cdots \tau_{n-1}(f) \in \mathbb{F}_{q^n}[x].$$

By using these definitions it is clear that for $f, g \in \mathbb{F}_{q^n}[x]$

$$\tau_s(fg) = \tau_s(f) \cdot \tau_s(g)$$

and so

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(fg) = \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) \cdot \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g). \tag{2.1}$$

Lemma 2.3 *If $f \in \mathbb{F}_{q^n}[x]$ then $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) \in \mathbb{F}_q[x]$.*

Proof of Lemma 2.3. First we prove the lemma for monic irreducible polynomials. Let $f \in \mathbb{F}_{q^n}[x]$ be a monic irreducible polynomial of degree k and let ε a root of it. Then

$$f(x) = (x-\varepsilon)(x-\varepsilon^{q^n})(x-\varepsilon^{q^{2n}}) \cdots (x-\varepsilon^{q^{(k-1)n}})$$

(see e.g. Theorem 2.14 in [11]). Clearly

$$\varepsilon \in \mathbb{F}_{q^{nk}}.$$

We have

$$\tau_s(f)(x) = (x-\varepsilon^{q^s})(x-\varepsilon^{q^{n+s}})(x-\varepsilon^{q^{2n+s}}) \cdots (x-\varepsilon^{q^{(k-1)n+s}}) \tag{2.2}$$

and

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)(x) = \prod_{i=0}^{k-1} \prod_{s=0}^{n-1} (x-\varepsilon^{q^{in+s}}) = \prod_{j=0}^{kn-1} (x-\varepsilon^{q^j}). \tag{2.3}$$

Since $\varepsilon \in \mathbb{F}_{q^{nk}}$, the conjugates of ε with respect to $\mathbb{F}_q$ are $\varepsilon, \varepsilon^q, \varepsilon^{q^2}, \ldots, \varepsilon^{q^{kn-1}}$. By this and (2.3) we have $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) \in \mathbb{F}_q[x]$.

Next we prove Lemma 2.3 for arbitrary polynomial $f \in \mathbb{F}_{q^n}[x]$. Write f as a product of monic irreducible polynomials

$$f = a \cdot g_1 \cdot g_2 \cdots g_r$$

where $a \in \mathbb{F}_{q^n}$ and $g_i \in \mathbb{F}_{q^n}[x]$'s are monic irreducible polynomials. Then by (2.1)

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) \cdot \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_1) \cdot \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_2) \cdots \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_r).$$

Since g_i's are monic irreducible polynomials $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_i) \in \mathbb{F}_q[x]$ from which $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) \in \mathbb{F}_q[x]$ follows.

Lemma 2.4 *Let $f \in \mathbb{F}_{q^n}[x]$. Then for $a \in \mathbb{F}_q$ we have*

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(a)) = \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)(a).$$

Proof of Lemma 2.4. By $a^q = a$ we have $\tau_s(f)(a) = (f(a))^{q^s}$. From this the lemma follows.

Lemma 2.5 *Suppose that $f \in \mathbb{F}_{q^n}[x]$ is a monic polynomial and for $t \mid n$, $t < n$ we have $f \notin \mathbb{F}_{q^t}[x]$. Then the following two statements are equivalent:*

(i) f is irreducible over $\mathbb{F}_{q^n}$.

(ii) $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ is irreducible over $\mathbb{F}_q$.

Lemma 2.5 shows a natural connection between irreducibility over $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$.

Proof of Lemma 2.5. $(ii) \Rightarrow (i)$: Suppose that $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ is irreducible over $\mathbb{F}_q$ and we will prove that f is also irreducible over $\mathbb{F}_{q^n}$. Indeed, if f is not irreducible over $\mathbb{F}_{q^n}$ then f can be written of the form

$$f = g_1 g_2$$

over $\mathbb{F}_{q^n}$ where deg g_1, deg $g_2 \geq 1$. By (2.1)

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_1) \cdot \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g_2).$$

over $\mathbb{F}_q$, so $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ is not irreducible over $\mathbb{F}_q$, which is a contradiction.

$(i) \Rightarrow (ii)$: Suppose that f is irreducible over $\mathbb{F}_{q^n}$ and we will prove that $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ is irreducible over $\mathbb{F}_q$. Indeed, let ε a root of f. Then

$$\varepsilon \in \mathbb{F}_{q^{nk}},$$

where $k = \deg f$. Here the conjugates of ε with respect to $\mathbb{F}_q$ are $\varepsilon, \varepsilon^{q^1}, \varepsilon^{q^2}, \ldots, \varepsilon^{q^{kn-1}}$. Let $m \in \mathbb{F}_q[x]$ be the minimal polynomial of ε over $\mathbb{F}_q$ and let

$$d = \deg m.$$

Then m is irreducible over $\mathbb{F}_q$. By [11, page 53] the conjugates $\varepsilon, \varepsilon^{q^1}, \varepsilon^{q^2}, \ldots, \varepsilon^{q^{kn-1}}$ are the distinct elements $\varepsilon, \varepsilon^{q^1}, \varepsilon^{q^2}, \ldots, \varepsilon^{q^{d-1}}$, each is repeated by $(kn)/d$ times. We also have

$$\varepsilon \in \mathbb{F}_{q^d} \tag{2.4}$$

and

$$\varepsilon^{q^d} = \varepsilon. \tag{2.5}$$

Then

$$m(x) = \prod_{j=0}^{d-1}(x - \varepsilon^{q^j}), \tag{2.6}$$

and

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = m^{kn/d}. \tag{2.7}$$

Since $d \mid kn$ we have $\frac{d}{(n,d)} \mid k$ and thus

$$k(n,d)/d \text{ is an integer.}$$

Since f is irreducible over $\mathbb{F}_{q^n}$ and ε is a root of it we have

$$f(x) = \prod_{j=0}^{k-1}(x - \varepsilon^{q^{jn}}).$$

Using (2.5) and the fact that the congruence

$$jn \equiv a \pmod{d}, \quad 0 \le j \le k-1$$

is solvable in j if and only if $(d,n) \mid a$ and then the number of solutions is $k(n,d)/d$ we have

$$f(x) = \left(\prod_{\ell=0}^{d/(n,d)-1} (x - \varepsilon^{q^{\ell(n,d)}}) \right)^{k(n,d)/d}.$$

Let

$$h(x) = \prod_{\ell=0}^{d/(n,d)-1} (x - \varepsilon^{q^{\ell(n,d)}}).$$

Then

$$f = h^{k(n,d)/d}. \tag{2.8}$$

By (2.4) $\varepsilon \in \mathbb{F}_{q^d}$ and its conjugates respect with $\mathbb{F}_{q^{(n,d)}}$ are $\varepsilon, \varepsilon^{q^{(n,d)}}, \varepsilon^{q^{2(n,d)}}, \ldots, \varepsilon^{q^{(d/(n,d)-1)(n,d)}}$. Thus $h \in \mathbb{F}_{q^{(n,d)}}[x]$. By (2.8) we have $f \in \mathbb{F}_{q^{(n,d)}}[x]$. By the conditions of the lemma $f \notin \mathbb{F}_{q^t}[x]$ for $t \mid n$, $t < n$ thus we have $(n, d) = n$, so

$$n \mid d. \tag{2.9}$$

By definition and (2.7)

$$\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f) = \tau_0(f) \cdot \tau_1(f) \cdot \tau_2(f) \cdots \tau_{n-1}(f) = m^{kn/d}.$$

Since f is irreducible over $\mathbb{F}_{q^n}$, clearly $\tau_0(f), \tau_1(f), \tau_2(f) \ldots \tau_{n-1}(f)$ are also irreducible over $\mathbb{F}_{q^n}$ thus

$$m = \tau_{a_1}(f) \cdot \tau_{a_2}(f) \cdots \tau_{a_s}(f) \tag{2.10}$$

over $\mathbb{F}_{q^n}$ where $0 \le a_1 < a_2 < \cdots < a_s \le n-1$. Here (similarly to (2.2)) we have

$$\tau_{a_i}(f)(x) = (x - \varepsilon^{q^{a_i}})(x - \varepsilon^{q^{n+a_i}})(x - \varepsilon^{q^{2n+a_i}}) \cdots (x - \varepsilon^{q^{(k-1)n+a_i}}).$$

Thus by this, (2.6) and (2.10) we have

$$\prod_{j=0}^{d-1}(x - \varepsilon^{q^j}) = \prod_{i=1}^{s}\prod_{\ell=0}^{k-1}(x - \varepsilon^{q^{\ell n+a_i}}).$$

Thus the set

$$\{\ell n + a_i : \ 0 \le \ell \le k-1, \ i = 1, 2, \ldots, s\}$$

forms a complete residue system modulo d. By (2.9) we have that $\{a_1, a_2, \ldots, a_s\}$ contains a complete residue system modulo n. But since

$0 \le a_1 < a_2 < \cdots < a_s \le n-1$ this is possible only for $\{a_1, a_2, \ldots, a_s\} = \{0, 1, 2, \ldots, n-1\}$. Then

$$m = \tau_0(f) \cdot \tau_1(f) \cdot \tau_2(f) \cdots \tau_{n-1}(f) = \mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f),$$

which means that the polynomial $\mathcal{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f)$ is irreducible over $\mathbb{F}_q$ since the minimal polynomial m is irreducible over $\mathbb{F}_q$.

Definition 2.4 *Denote $\mathcal{G}_{q^n}$ the following elements of $\mathbb{F}_{q^n}$:*

$$\mathcal{G}_{q^n} = \{\alpha \in \mathbb{F}_{q^n} : \exists\ t \mid n, t < n \text{ such that } \alpha \in \mathbb{F}_{q^t} \subset \mathbb{F}_{q^n}\}.$$

Lemma 2.6

$$|\mathcal{G}_{q^n}| \le 2q^{n/2}$$

Proof of Lemma 2.6. Let $b_n = 1$ if n is even and $b_n = 0$ if n is odd. Clearly:

$$|\mathcal{G}_n| \le \sum_{t|n,\ t<n} q^t \le b_n q^{n/2} + \sum_{t|n,\ t\le n/3} q^t \le b_n q^{n/2} + \sum_{t=1}^{[n/3]} q^t \le 2q^{n/2}.$$

3 Proof of Theorem 1.1

Let

$$1 \le j \le \min\left\{p,\ \frac{k-c}{2\log 2}\log p\right\}. \tag{3.1}$$

Suppose that $1 \le i_1 < i_2 < \cdots < i_j \le p$ and $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j \in \{-1, +1\}$, we will prove that there exists a monic irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree k such that

$$\left(\frac{g(i_s)}{p}\right) = \varepsilon_s \ \text{ for } s = 1, 2, \ldots, j.$$

From this (1.6) follows.

We will use the following lemmas due to Lidl and Niederreiter [11]:

Lemma 3.1 *Let $i_1, i_2, \dots i_j$ be j distinct elements of $\mathbb{F}_{p^k}$, p odd, and let $\varepsilon_1, \dots, \varepsilon_j \in \{-1, +1\}$. Let $N(\varepsilon_1, \dots, \varepsilon_j)$ denote the number of $\alpha \in \mathbb{F}_{p^k}$ with*

$$\gamma(\alpha + i_s) = \varepsilon_s \text{ for } s = 1, 2, \dots, j,$$

where γ is the quadratic character $\mathbb{F}_{p^k}$. Then

$$N(\varepsilon_1, \dots, \varepsilon_j) = \frac{1}{2^j} \sum_{a \in \mathbb{F}_{p^k}} (1 + \varepsilon_1 \gamma(a + i_1)) \cdots (1 + \varepsilon_j \gamma(a + i_j)) - A$$

where $0 \le A \le j/2$.

Lemma 3.2

$$\left| N(\varepsilon_1, \dots, \varepsilon_j) - \frac{p^k}{2^j} \right| \le \left(\frac{j-2}{2} + \frac{1}{2^j} \right) p^{k/2} + \frac{j}{2}.$$

These lemmas are Exercises 5.63 and 5.64 in [11] (the proof of Lemma 3.2 is based on the famous Weil theorem [15]).

Define $N(\varepsilon_1, \dots, \varepsilon_j)$ as in Lemma 3.1. Using (3.1), Lemma 3.2 and the triangle-inequality we get

$$\begin{aligned} N(\varepsilon_1, \dots, \varepsilon_j) &\ge \frac{p^k}{2^j} - \left(\frac{j-2}{2} + \frac{1}{2^j} \right) p^{k/2} - \frac{j}{2} \ge \frac{p^k}{2^j} - \frac{j-1}{2} p^{k/2} - \frac{j}{2} \\ &\ge \frac{p^k}{2^j} - \frac{j}{2} p^{k/2} \ge \left(p^{c/2} - \frac{j}{2} \right) p^{k/2}. \end{aligned} \tag{3.2}$$

Since $c = 1/2$ if $k \le \frac{p^{1/4}}{10 \log p}$ and $c = 5/2$ if $k > \frac{p^{1/4}}{10 \log p}$, for $k \le \frac{p^{1/4}}{10 \log p}$ by (3.1) we get

$$p^{c/2} p^{k/2} - \frac{j}{2} \ge p^{1/4} - \frac{k \log p}{4 \log 2} \ge \left(1 - \frac{1}{40 \log 2} \right) p^{1/4} > 2,$$

while for $k > \frac{p^{1/4}}{10 \log p}$ we get

$$p^{c/2} p^{k/2} - \frac{j}{2} \ge p^{5/4} - \frac{p}{2} > 2.$$

By this, (3.2) and Lemma 2.6 we get

$$N(\varepsilon_1, \dots, \varepsilon_j) > 2p^{k/2} \ge \left| \mathcal{G}_{\mathbb{F}_{p^k}} \right|.$$

Using this and the definition of $N(\varepsilon_1, \ldots, \varepsilon_j)$ we get there exists $\alpha \in F_{p^k} \setminus \mathcal{G}_{p^k}$ such that

$$\gamma(\alpha + i_s) = \varepsilon_s \quad \text{for } s = 1, 2, \ldots, j. \tag{3.3}$$

Let

$$f(x) = x + \alpha \in \mathbb{F}_{p^k}[x].$$

By $\alpha \in F_{p^k} \setminus \mathcal{G}_{p^k}$ we get that $f \notin \mathbb{F}_{p^t}[x]$ for $t \mid k$, $t < k$. Using Lemma 2.5 we get

$$g \stackrel{\text{def}}{=} \mathcal{N}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f) \in \mathbb{F}_p[x]$$

is irreducible over $\mathbb{F}_p$, and its degree is k. Using (3.3), Corollary 2.1 and Lemma 2.4 we get

$$\begin{aligned}\varepsilon_s = \gamma(\alpha + i_s) = \gamma(f(i_s)) &= \left(\frac{N_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f(i_s))}{p}\right) = \left(\frac{\mathcal{N}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f)(i_s)}{p}\right) \\ &= \left(\frac{g(i_s)}{p}\right) \text{ for } s = 1, 2, \ldots, j,\end{aligned}$$

which was to be proved.

References

[1] R. Ahlswede, L.H. Khachatrian, C. Mauduit and A. Sárközy, *A complexity measure for families of binary sequences*, Periodica Math. Hungar. 46 (2003), 107-118.

[2] R. Ahlswede, C. Mauduit and A. Sárközy, *Large Families of Pseudorandom Sequences of k Symbols and Their Complexity, Part I and II*, General Theory of Information Transfer and Combinatorics Lecture Notes in Computer Science Volume 4123, 2006, 293-307 and 308-325.

[3] R. Balasubramanian, C. Dartyge and E. Mosaki, *Sur la complexité de familles d'ensembles pseudo-aléatoires*, arXiv:1302.4622v1.

[4] J. Folláth, *Construction of pseudorandom binary sequences using additive characters over GF (2 k) II*, Period. Math. Hung. 60 (2010), 127-135.

[5] L. Goubin, C. Mauduit and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[6] K. Gyarmati, *Concatenation of pseudorandom binary sequences*, Period. Math. Hung. 58 (2009), 99-120.

[7] K. Gyarmati, *On the complexity of a family related to the Legendre symbol*, Period. Math. Hung. 58 (2009), 209-215.

[8] K. Gyarmati, C. Mauduit, A. Sárközy, *Generation of further pseudorandom binary sequences, I (Blowing up a single sequence)*, submitted.

[9] K. Gyarmati, C. Mauduit, A. Sárközy, *Measures of pseudorandomness of families of binary lattices, II (A further construction.),* Publi. Math. Debrecen 80 (2012), 479-502.

[10] J. Hoffstein and D. Lieman, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, Progress in Computer Science and Applied Logic, Vol. 20, Birkhäuser, Verlag, Basel, 2001; pp. 59-68.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its applications, Cambridge University Press, Second edition published in 1997.

[12] C. Mauduit and A. Sárközy, *Family Complexity and VC-Dimension*, Information Theory, Combinatorics, and Search Theory, Lecture Notes in Computer Science Volume 7777, 2013, 346-363.

[13] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.

[14] A. Sárközy, *On pseudorandomness of families of binary sequences*, volume dedicated to the memory of L. H. Khachatrian, submitted.

[15] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

[16] A. Winterhof and O. Yayla, *Family complexity and cross-correlation measure for families of binary sequences*, submitted.

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
Budapest, Pázmány Péter st. 1/C
H1117 Hungary
Email: gykati@cs.elte.hu