Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 10(1): 38–55.
DOI: 10.3934/math.2025003
Received: 23 October 2024
Revised: 05 December 2024
Accepted: 11 December 2024
Published: 02 January 2025

Research article

Families of sequences with good family complexity and cross-correlation measure[†]

Kenan Doğan[1,*], **Murat Şahin**[2] **and Oğuz Yayla**[3]

[1] Graduate School of Natural and Applied Sciences, Department of Mathematics, Ankara University, Altındağ 06110, Ankara, Türkiye

[2] Department of Mathematics, Ankara University, Tandoğan 06100, Ankara, Türkiye

[3] Institute of Applied of Mathematics, Middle East Technical University, Çankaya 06800, Ankara, Türkiye

* **Correspondence:** Email: knndogan@gmail.com.

Abstract: In this paper, we examine the pseudorandomness of a family of sequences with respect to two key measures: family complexity (f-complexity) and cross-correlation measure of order ℓ. Our study encompasses sequences over both binary and k-symbol (k-ary) alphabets. We first extend known methods for constructing families of binary pseudorandom sequences and establish a bound on the f-complexity of a large family of binary sequences generated from the Legendre symbols of certain irreducible polynomials. We demonstrate that this family, as well as its dual, exhibits both high family complexity and low cross-correlation measure up to a relatively high order. Additionally, we present a second family of binary sequences with similarly high f-complexity and low cross-correlation measure. Finally, we generalize our results to families of sequences over the k-symbol alphabets.

Keywords: binary sequences; cross-correlation measure; family complexity; k-symbols sequences; pseudorandomness
Mathematics Subject Classification: 11K45, 94A55, 94A60

1. Introduction

Pseudorandom sequence is a sequence of numbers generated deterministically and looks random. It is called a binary (k-ary or k-symbol) sequence if its elements are in {-1,+1} (resp. $\{a_1, a_2, \dots, a_k\}$ for some numbers a_i). Pseudorandom sequences have a wide array of application areas, including telecommunication, cryptography, simulation, numerical integration, spread-spectrum

[†]This publication is a part of the doctoral thesis of Kenan Doğan.

communications, and randomized algorithms, among others [8, 12, 34, 39]. In telecommunication, pseudorandom sequences are essential for tasks such as channel coding, error detection and correction, and synchronization in spread-spectrum and CDMA systems. In cryptography, they underpin the generation of secure keys, stream ciphers, and various cryptographic protocols, ensuring data confidentiality and integrity. Simulation applications, particularly in Monte Carlo methods, rely on pseudorandom sequences to model and analyze complex systems and stochastic processes with high accuracy.

According to their application area, the quality of a pseudorandom sequence is evaluated in multiple dimensions. There are several statistical test packages available for assessing the quality of pseudorandom sequences, such as L'Ecuyer's TESTU01 [20], Marsaglia's Diehard [25], and the NIST Statistical Test Suite [35]. These tools perform a battery of tests to evaluate properties like uniform distribution, independence, and absence of detectable patterns. In addition to empirical testing, there are established theoretical results concerning various randomness measures that a pseudorandom sequence must satisfy. These measures include linear complexity, which assesses the sequence's resistance to linear attacks; (auto)correlation, which evaluates the sequence's suitability for synchronization and multiple access; discrepancy, which measures the uniformity of distribution in multi-dimensional spaces; and well-distribution, which ensures that the sequence covers the space evenly [17, 39].

In certain applications, particularly in cryptography, there is a need to generate multiple pseudorandom binary sequences simultaneously. This requirement requires that the sequences maintain high levels of randomness in several metrics to prevent vulnerabilities. Therefore, their randomness must be validated using multiple figures of merit, such as family complexity, which measures the difficulty of distinguishing any single sequence from others in the family; cross-correlation, which assesses the independence between different sequences; collision resistance, which ensures that sequences do not inadvertently produce the same output; minimum distance, which evaluates the separation between sequences in the family; and the avalanche effect, which ensures that small changes in input lead to significant changes in output [37]. These measures collectively enhance the robustness and security of cryptographic systems by ensuring that the pseudorandom sequences are sufficiently unpredictable and resilient against various attack vectors.

Furthermore, pseudorandom sequences are integral to numerical integration techniques, particularly in quasi-Monte Carlo methods, where low-discrepancy sequences improve the convergence rate compared to purely random sequences [32]. In randomized algorithms, pseudorandomness ensures that algorithms perform efficiently on average, providing reliable performance across diverse problem instances. Additionally, in error correction and detection schemes, pseudorandom sequences facilitate encoding and decoding processes by introducing controlled randomness that helps to identify and correct errors.

The typical values of certain randomness measures for truly random sequences have been established in foundational works [3, 5, 32], offering benchmarks to evaluate the adequacy of pseudorandom sequences in specific applications. Sequences that meet these typical values are termed *good* sequences. Following Mauduit and Sárközy's work [27], which introduced a method to construct good binary sequences using the Legendre symbol, other construction methods have been developed, enriching the literature with various techniques [6, 7, 21].

In 2004, Goubin, Mauduit, and Sárközy [14] pioneered the construction of large families of pseudo-random binary sequences. Subsequent research expanded upon this, leading to various new constructions [10, 15, 26, 29, 30] and complexity bounds [31, 33, 36], with further developments documented in [37]. The measures of pseudorandomness originally defined for binary sequences have also been generalized to sequences over k-symbol alphabets [11, 28, 40], and constructions of good sequences for k-symbol alphabets have been proposed [2, 9, 13, 22, 24].

Recently, Huaning Liu and Xi Liu [23] constructed a new family of binary sequences with both a low cross-correlation measure and high family complexity. In this paper, we investigate the family complexity (abbreviated as f-complexity) and the cross-correlation measure of order ℓ for families of binary and k-ary sequences, considering not only binary alphabets but also sequences over k-symbol (or k-ary) alphabets.

We begin by presenting established definitions in this section to facilitate a clear introduction of our results. Ahlswede et al. [1] defined the f-complexity as follows.

Definition 1. *The f-complexity $C(\mathcal{F})$ of a family $\mathcal{F}$ of binary sequences $E_N \in \{-1, +1\}^N$ of length N is the greatest integer $j \geq 0$ such that for any $1 \leq i_1 < i_2 < \cdots < i_j \leq N$ and any $\epsilon_1, \epsilon_2, \ldots, \epsilon_j \in \{-1, +1\}$, there is a sequence $E_N = (e_1, e_2, \ldots, e_N) \in \mathcal{F}$ with*

$$e_{i_1} = \epsilon_1, e_{i_2} = \epsilon_2, \ldots, e_{i_j} = \epsilon_j.$$

We have the trivial upper bound

$$2^{C(\mathcal{F})} \leq |\mathcal{F}|, \tag{1.1}$$

where $|\mathcal{F}| = F$ denotes the size of the family $\mathcal{F}$. Gyarmati et al. [18] introduced the cross-correlation measure of order ℓ.

Definition 2. *The cross-correlation measure of order ℓ of a family $\mathcal{F}$ of binary sequences*

$$E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N}) \in \{-1 + 1\}^N, i = 1, 2, \ldots, F,$$

is defined as

$$\Phi_\ell(\mathcal{F}) = \max_{M,D,I} \left| \sum_{n=1}^{M} e_{i_1,n+d_1} \cdots e_{i_\ell,n+d_\ell} \right|,$$

where D denotes an ℓ tuple $(d_1, d_2, \ldots, d_\ell)$ of integers such that $0 \leq d_1 \leq d_2 \leq \cdots \leq d_\ell < M + d_\ell \leq N$ and $d_i \neq d_j$ if $E_{i,N} = E_{j,N}$ for $i \neq j$, and I denotes an ℓ tuple $(i_1, i_2, \ldots, i_\ell) \in \{1, 2, \ldots, F\}^\ell$.

For a family $\mathcal{F}$ of binary sequences of length N with $|\mathcal{F}| < 2^{N/12}$, the expected value of the cross-correlation measure of order $\ell \leq N/(6 \log_2 |\mathcal{F}|)$ is

$$\Phi_\ell(\mathcal{F}) \approx \left(N \log \binom{N}{\ell} + \ell \log |\mathcal{F}| \right)^{1/2},$$

see [32]. We use the notation Φ_ℓ° for the cross-correlation Φ_ℓ evaluated for fixed $M = F$ and $d_i = 0$ for all $i \in \{1, 2, \ldots, l\}$.

Winterhof and the third author in [43] proved the estimation of the f-complexity $C(\mathcal{F})$ of a family $\mathcal{F}$ of binary sequences

$$E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N}) \in \{-1 + 1\}^N, \quad i = 1, \ldots, F,$$

in terms of the cross-correlation measure $\Phi_\ell(\overline{\mathcal{F}})$, $\ell \in \{1, 2, \ldots, \log_2 F\}$ of the *dual family* $\overline{\mathcal{F}}$ of binary sequences

$$E_{i,F} = (e_{1,i}, e_{2,i}, \ldots, e_{F,i}) \in \{-1+1\}^F, \quad i = 1, \ldots, N \tag{1.2}$$

as follows:

$$C(\mathcal{F}) \geq \left\lceil \log_2 F - \log_2 \max_{1 \leq i \leq \log_2 F} \Phi_i(\overline{\mathcal{F}}) \right\rceil - 1. \tag{1.3}$$

Contribution and Outline. In Section 2, we generalize the construction of a family of binary pseudorandom sequences presented in [43]. We establish a bound on the f-complexity of a family of binary sequences generated from the Legendre symbols of irreducible polynomials of the form

$$f_i(x) = x^d + a_2 i^2 x^{d-2} + a_3 i^3 x^{d-3} + \cdots + a_{d-2} i^{d-2} x^2 + a_d i^d \in \mathbb{F}_p[x]$$

for an odd prime number p, defined as

$$\mathcal{F}_1 = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\}.$$

We demonstrate that both this family and its dual family exhibit a high family complexity and a low cross-correlation measure up to a large order. Unlike the results in [43], we show that the cross-correlation measure of this family increases and the lower bound on family complexity decreases as the degree d increases (see Theorem 1).

In Section 3, we analyze a different family of binary sequences

$$\mathcal{F}_2 = \left\{ \left(\frac{f(n)}{p} \right)_{n=1}^{p-1} : f \text{ is irreducible of degree } d \text{ over } \mathbb{F}_p \text{ with vanishing } x^{d-1} \right\}$$

for a positive integer $d \leq \sqrt{p}/2$. We prove that $\mathcal{F}_2$ has high f-complexity and a low cross-correlation measure based on (1.3). We observe that, similar to $\mathcal{F}_1$, these measures weaken as d increases. On the other hand, the family size of $\mathcal{F}_2$ is larger, on the order of p^{d-2} (see Theorem 2), which is also achieved by a different construction in [23].

In Section 4, we extend the relation (1.3) to families of sequences over a k-symbol alphabet. Finally, in Section 5, we demonstrate that an extension of the family $\mathcal{F}_2$ to a k-symbol alphabet also maintains high f-complexity and a low cross-correlation measure.

Throughout this paper, the notations $U \ll V$ and $U = O(V)$ indicate that $|U| \leq cV$ for some positive constant c. Additionally, $f(n) = o(1)$ denotes that $\lim_{n\to\infty} f(n) = 0$.

2. A family and its dual with bounded cross-correlation and family complexity measures

We note that there are several related constructions of families of binary sequences defined with the Legendre symbol and polynomials; see [16, 18, 43]. In this section we present similar families of sequences as given in [43], where a family of sequences of Legendre symbols with irreducible quadratic polynomials and its dual family were given. It was shown that both families have high family complexity and small cross-correlation measures up to a large order ℓ. Namely, for $p > 2$ a prime and b a quadratic nonresidue modulo p, they study the following family $\mathcal{F}$ and its dual family $\overline{\mathcal{F}}$:

$$\mathcal{F} = \left\{ \left(\frac{n^2 - bi^2}{p} \right)_{i=1}^{(p-1)/2} : n = 1, \ldots, (p-1)/2 \right\},$$

and they show

$$\Phi_k(\mathcal{F}) \ll kp^{1/2} \log p \quad \text{and} \quad \Phi_k(\overline{\mathcal{F}}) \ll kp^{1/2} \log p$$

for each integer $k = 1, 2, \ldots$ and the dual of a family is defined as in (1.2). Then (1.3) immediately implies

$$C(\mathcal{F}) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log p}{\log 2} \text{ and } C(\overline{\mathcal{F}}) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log p}{\log 2}.$$

We now present a generalization of this result to higher degree polynomials over prime finite fields. Note that for these families we also obtain analog bounds for their duals.

Let $p > 2$ be a prime number, $d \geq 5$, and $\Omega_{p,d}$ be a set of irreducible polynomials over $\mathbb{F}_p$ of degree d defined as

$$\Omega_{p,d} = \{ x^d + a_2 x^{d-2} + \cdots + a_{d-2} x^2 + a_d \in \mathbb{F}_p[x] | a_2, a_3 \neq 0 \}.$$

Theorem 1. *Let $\mathcal{F}_f$ be a family of binary sequences for some $f \in \Omega_{p,d}$ defined as*

$$\mathcal{F}_f = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \ldots, p-1 \right\},$$

where $f_i(X) = i^d f(X/i)$ for $i \in \{1, 2, \ldots, p-1\}$ and $d < p^{1/2}/2$. Let $\overline{\mathcal{F}_f}$ be the dual of $\mathcal{F}_f$. Then we have

$$\Phi_k(\mathcal{F}_f) \ll dkp^{1/2} \log p \textit{ and } \Phi_k(\overline{\mathcal{F}_f}) \ll dkp^{1/2} \log p \tag{2.1}$$

for each integer $k \in \{1, 2, \ldots, p-1\}$ and

$$C(\mathcal{F}_f) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2} \tag{2.2}$$

and

$$C(\overline{\mathcal{F}_f}) \geq \left(\frac{1}{2} - o(1) \right) \frac{\log(p/d^2)}{\log 2}. \tag{2.3}$$

If $d = p^{\varepsilon}$, then we obtain the lower bound $\left(\frac{1}{2} - \varepsilon - o(1) \right) \frac{\log p}{\log 2}$. In particular, the bound becomes trivial for $\varepsilon \geq 1/2$.

Proof. Since otherwise the cross-correlation values, bounded by $p - 1$ the length of the sequences, become greater than p, we may assume $d < p^{1/2}/2$. We note that $f(X, i) := f_i(X)$ is an homogeneous polynomial of degree d. Thus, it is enough to choose an irreducible polynomial

$$f(X) = X^d + a_2 X^{d-2} + a_3 X^{d-3} + \cdots + a_{d-2} X^2 + a_d \in \mathbb{F}_p[X]$$

such that $a_2, a_3 \not\equiv 0 \pmod p$. It is clear that each f_i is irreducible for $i \in \{1, 2, \dots p-1\}$ whenever $f(X)$ is irreducible.

According to Definition 2 we need to estimate

$$\left|\sum_{n=1}^{M}\left(\frac{f_{i_1}(n+d_1)}{p}\right)\cdots\left(\frac{f_{i_k}(n+d_k)}{p}\right)\right| = \left|\sum_{n=1}^{M}\left(\frac{f_{i_1}(n+d_1)\cdots f_{i_k}(n+d_k)}{p}\right)\right|.$$

We will first show that

$$h(X) := f_{i_1}(X+d_1)\cdots f_{i_k}(X+d_k)$$

is a monic square-free polynomial and then apply Weil's Theorem, see [19,38,42]. Since each f_{i_j}, $j = 1, 2, \dots, k$ is an irreducible polynomial, it is enough to show that they are distinct from each other. Assume that $f_{i_j}(X+d_j) = f_{i_\ell}(X+d_\ell)$ for some $j, \ell = 1, 2, \dots, k$. Then by comparing the coefficients of the term X^{d-1} we have $d_j = d_\ell$ since $p \nmid d$. Hence, we have the equality $f_{i_j}(X) = f_{i_\ell}(X)$. But then by comparing the coefficients of the terms X^{d-2} and X^{d-3}, we have

$$a_2 i_j^2 = a_2 i_\ell^2 \text{ and } a_3 i_j^3 = a_3 i_\ell^3.$$

Since a_2 and a_3 are non-zero, we have

$$i_j^2 = i_\ell^2 \text{ and } i_j^3 = i_\ell^3.$$

This implies that $i_j = i_\ell$, a contradiction. Therefore, h is a square-free polynomial. Since the degree of $h(x)$ is dk then the following holds

$$\Phi_k(\mathcal{F}_f) \ll dkp^{1/2}\log p.$$

Similarly, we can show that

$$\Phi_k(\overline{\mathcal{F}_f}) \ll dkp^{1/2}\log p$$

for $k \in \{1, 2, \dots, p-1\}$. Next, we use (1.3) to obtain the bounds on the family complexity.

$$\begin{aligned}
C(\mathcal{F}_f) &\geq \log_2 \frac{F}{\max_{1\leq\ell\leq\log_2 F}\Phi_\ell^\circ(\overline{\mathcal{F}_f})} \\
&\geq \log_2 \frac{p-1}{d\,k\,p^{1/2}\,\log p} \\
&= \log_2 \frac{p-1}{d\,(\log_2 p)\,p^{1/2}\,\log p} \\
&\geq \log_2 \frac{p^{1/2}}{d\,(\log_2 p)\,\log p} \\
&\geq \log_2 \frac{p^{1/2}}{d} - \log_2 \log^2 p \\
&\geq \frac{1}{2}\log_2 \frac{p}{d^2} - \log_2 \log^2 p \\
&\geq (\frac{1}{2} - o(1))\frac{\log p/d^2}{\log 2}.
\end{aligned}$$

□

Remark 1. *We note that the results in Theorem 1 become weaker with increasing degree, but the size of the family stays the same. The family complexity of a 'good' family of sequences is expected to be roughly of the order of magnitude* $\log(F)$*, where F is the size of the family. Note that the family* $\mathcal{F}_f$ *constructed in Theorem 1 has the family complexity lower bounded by* $\frac{\log(\mathcal{F}_f)}{2\log 2}$ *for small d where* $|\mathcal{F}_f| = p - 1$*. Thus,* $\mathcal{F}_f$ *would be a good family of sequence if* $C(\mathcal{F}_f)$ *is upper bounded similarly and this lower bound is improved.*

Example 1. *Let* $d = 5$ *and* $p = 11$*. The polynomial* $f = x^5 + x^3 + 2x^2 + 3$ *is in the set* $\Omega_{11,5}$*. The irreducible polynomials generated by* $f_i(X) = i^5 f(X/i)$ *for* $i \in \{1, 2, \ldots, 10\}$ *are* $f_1(x) = x^5 + x^3 + 2x^2 + 3$, $f_2(x) = x^5 + 4x^3 + 5x^2 + 8$, $f_3(x) = x^5 + 9x^3 + 10x^2 + 3$, $f_4(x) = x^5 + 5x^3 + 7x^2 + 3$, $f_5(x) = x^5 + 3x^3 + 8x^2 + 3$, $f_6(x) = x^5 + 3x^3 + 3x^2 + 8$, $f_7(x) = x^5 + 5x^3 + 4x^2 + 8$, $f_8(x) = x^5 + 9x^3 + x^2 + 8$, $f_9(x) = x^5 + 4x^3 + 6x^2 + 3$, $f_{10}(x) = x^5 + x^3 + 9x^2 + 8$. *The sequences generated by these polynomials are*

[[-1, -1, 1, 1, 1, 1, 1, 1, 1, 1],
[-1, 1, -1, 1, -1, -1, -1, -1, -1, -1],
[1, 1, -1, 1, 1, -1, 1, 1, 1, 1],
[1, 1, 1, -1, 1, 1, 1, -1, 1, 1],
[1, 1, 1, 1, -1, 1, 1, 1, 1, -1],
[1, -1, -1, -1, -1, 1, -1, -1, -1, -1],
[-1, -1, 1, -1, -1, -1, 1, -1, -1, -1],
[-1, -1, -1, -1, 1, -1, -1, 1, -1, -1],
[1, 1, 1, 1, 1, 1, -1, 1, -1, 1],
[-1, -1, -1, -1, -1, -1, -1, -1, 1, 1]].

This sequence family does not have the complexity 3, since the tuples $\{[1,1,1], [1,1,-1], [1,-1,1], [1,-1,-1], [-1,1,1], [-1,1,-1], [-1,-1,1], [-1,-1,-1]\}$ *in the vector space* $\mathbb{F}_2^3$ *are not in the all possible 3 tuples of the sequence family. For example, the first three bits of sequence family are* $[[-1,-1,1], [-1,1,-1], [1,1,-1], [1,1,1], [1,1,1], [1,-1,-1], [-1,-1,1], [-1,-1,-1], [1,1,1], [-1,-1,-1]]$. *However, this multi-list does not contain all the vectors in* $\mathbb{F}_2^3$*. On the other hand, its family complexity is 2. The cross-correlation measure of order 5 of the family gets the maximum value of 10 with M=10, I=[2,6,7,8,10] and D=[0,0,0,0,0]. The dual family* $\overline{\mathcal{F}_f}$ *gets the cross-correlation measure 9 of order 5 with I=[3,4,6,9,10] and D=[0,0,0,1,1]. The complexity of the dual family is 1. We note that the right-hand side of* (2.1) *is approximately 75, and so it is far from being close for small primes p. But, as it is an asymptotic bound, it requires computations for large primes.On the other hand, the lower bound in* (2.2) *and* (2.2) *is* $-\frac{1}{2}$*, and so it is seen that the family complexities in this example are very close to this bound. Similarly, we note that this bound holds for large primes p.*

We note that each two sequences in $\mathcal{F}_f$ (resp. $\overline{\mathcal{F}_f}$) given in Theorem 1 are distinct as $\Phi_2(\mathcal{F}_f) < p$ (resp. $\Phi_2(\overline{\mathcal{F}_f}) < p$). Hence, we have the family size $|\mathcal{F}_f| = p - 1$ for the family. In the next result, we give an upper bound on the number $\#\{\mathcal{F}_f | f \in \Omega_{p,n}\}$ of distinct families. This result is a direct consequence from the paper [4]. Before that we will give some notation. Let $C_\alpha : x(y^p + y) = \alpha(x^2 + 1)$ be curves over $\mathbb{F}_p$ for $\alpha \in \mathbb{F}_p^\times$. Let $\#C_\alpha(\mathbb{F}_{p^n})$ denote the number of points $(x, y) \in \mathbb{F}_{p^n}$ on C_α and define $S_\alpha(\mathbb{F}_{p^n}) := \#C_\alpha(\mathbb{F}_{p^n}) - (p^n + 1)$. Let μ denote the Möbius function and [p divides n] denote its truth value, i.e., [p divides n] := 1 if p divides n, and [p divides n] := 0 otherwise.

Corollary 1.

$$\#\{\mathcal{F}_f | f \in \Omega_{p,n}\} < \frac{1}{n} \sum_{d|n, p\nmid d} \mu(d)\left(F_p(n/d) - [p \text{ divides } n]p^{n/pd}\right),$$

where

$$F_p(n) = p^{n-2} + \frac{(p-1)^2}{p^2} + \frac{1}{p^2}\sum_{\alpha\in\mathbb{F}_p^\times} S_\alpha(\mathbb{F}_{p^n}).$$

Proof. The family $\mathcal{F}$ is constructed by using irreducible polynomials $f \in \Omega_{p,n}$. By [4, Theorem 1], we obtain the number of irreducible polynomials in terms of $F_p(n)$. Then, [4, Theorem 5] gives the result. □

3. A large family of sequences with low cross-correlation and high family complexity

Now we construct a larger family with both a small cross-correlation measure and high f-complexity. However, for these families of sequences we cannot say anything about their duals.

Theorem 2. *Let $p > 2$ be a prime number, $d \in \mathbb{Z}^+$ and $p \nmid d$. Let Ω_d be the set defined as*

$$\Omega_d = \{f(X) = X^d + a_2X^{d-2} + \cdots + a_d \in \mathbb{F}_p[X] : f \text{ is irreducible over } \mathbb{F}_p\}.$$

Let a family $\mathcal{F}_d$ of binary sequences be defined as

$$\mathcal{F}_d = \left\{\left(\frac{f(n)}{p}\right)_{n=1}^{p-1} : f \in \Omega_d\right\}.$$

Then,

$$C(\mathcal{F}_d) \geq (\frac{1}{2} - o(1))\frac{\log(p^{d-2}/d^2)}{\log 2}. \tag{3.1}$$

The family size equals

$$|\mathcal{F}_d| = \frac{p^{d-1}}{d} - O(p^{\lfloor d/2 \rfloor})$$

for $3 \leq d < p^{1/2}/2$.

Proof. It is clear by the Weil bound that each irreducible polynomial generates a distinct sequence in $\mathcal{F}$. Yucas [44] proved that the number of irreducible polynomials over $\mathbb{F}_p$ of degree d with $p \nmid d$ and trace nonzero equals

$$\frac{1}{dp}\sum_{t|d}\mu(t)p^{d/t}.$$

By doing calculations, we obtain

$$\sum_{i=1}^{d/2} p^i = p(\frac{p^{d/2}-1}{p-1}) = \frac{p}{p-1}p^{d/2} - \frac{p}{p-1}.$$

With the smallest $p = 3$, we see that

$$\frac{1}{dp}\sum_{t|d}\mu(t)p^{d/t} \geq \frac{p^d}{dp} - \sum_{i=1}^{\lfloor d/2\rfloor} p^i \geq \frac{p^{d-1}}{d} - \frac{3}{2}p^{\lfloor d/2\rfloor}.$$

Hence,

$$|\mathcal{F}_d| = \frac{p^{d-1}}{d} - O(p^{\lfloor d/2\rfloor})$$

and we have proved the size of family.

Next, we prove the bound on family complexity by using (1.3) with Φ_k° instead Φ_k. Because estimating Φ_k° is easier in this case. In order to calculate $\Phi_k^\circ(\overline{\mathcal{F}})$ we need to estimate

$$V = \left|\sum_{f\in\Omega_d}\left(\frac{f(i_1)}{p}\right)\cdots\left(\frac{f(i_k)}{p}\right)\right|, 1 \leq i_1 < \cdots < i_k \leq p-1.$$

Note that $f(X) \in \Omega_d$ if and only if

$$f(X) = (X-\beta)(X-\beta^p)\cdots(X-\beta^{p^{d-1}})$$

for some $\beta \in \mathbb{F}_{p^d}$ with $\mathrm{Tr}(\beta) = 0$ and $\beta \notin \mathbb{F}_{p^t}$ for any $t \mid d, t < d$. Hence, we rewrite V as given in (3.2),

$$\begin{aligned} V &= \frac{1}{d}\left|\sum_{\substack{\beta\in\mathbb{F}_{p^d}\\ \mathbb{F}_{p^d}=\mathbb{F}_p(\beta)\\ \mathrm{Tr}(\beta)=0}}\left(\frac{(i_1-\beta)(i_1-\beta^p)\cdots(i_1-\beta^{p^{d-1}})}{p}\right)\cdots\left(\frac{(i_k-\beta)(i_k-\beta^p)\cdots(i_k-\beta^{p^{d-1}})}{p}\right)\right| \\ &= \frac{1}{d}\left|\sum_{\substack{\beta\in\mathbb{F}_{p^d}\\ \mathbb{F}_{p^d}=\mathbb{F}_p(\beta)\\ \mathrm{Tr}(\beta)=0}}\left(\frac{N(i_1-\beta)}{p}\right)\cdots\left(\frac{N(i_k-\beta)}{p}\right)\right|, \end{aligned} \tag{3.2}$$

where N is the norm function from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$. We note that $\chi(\alpha) = \left(\frac{N(\alpha)}{p}\right)$ is the quadratic character of $\mathbb{F}_{p^d}$ and the number of elements $\alpha \in \mathbb{F}_{p^t},\ t \mid d$ and $t < d$ but $\alpha \notin \mathbb{F}_{p^d}$ is at most

$$\sum_{t|d,t<d} p^t \leq \frac{3}{2}p^{\lfloor d/2\rfloor}.$$

Thus, we can estimate V as follows:

$$\begin{aligned}
V &\le \frac{1}{d}\left|\sum_{\substack{\beta\in\mathbb{F}_{p^d}\\ \mathrm{Tr}(\beta)=0}} \chi((i_1-\beta)\cdots(i_k-\beta))\right| + O(p^{d/2}/d)\\
&\le \frac{1}{dp}\left|\sum_{\alpha\in\mathbb{F}_{p^d}} \chi((i_1-\alpha^p+\alpha)\cdots(i_k-\alpha^p+\alpha))\right| + O(p^{d/2}/d)\\
&\le \frac{pk\,p^{d/2}\log p}{dp} + O(p^{d/2}/d) \text{ (degree of the polynomial in } \chi \text{ is } pk)\\
&= k\,p^{d/2}/d\log p + O(p^{d/2}/d).
\end{aligned}$$

The last inequality follows by Weil's Theorem [41]. By (1.1), $2^{C(\mathcal{F})} \le |\mathcal{F}| = F$ and since $k = C(\mathcal{F})$ we obtain $k \le \log_2 F$. Therefore, by using (1.3) we have

$$\begin{aligned}
C(\mathcal{F}_d) &\ge \log_2 \frac{F}{\max_{1\le\ell\le\log_2 F} \Phi^{\circ}_{\ell}(\overline{\mathcal{F}_d})}\\
&\ge \log_2 \frac{\frac{p^{d-1}}{d} - O(p^{\lfloor d/2\rfloor})}{k\frac{p^{d/2}}{d}\log p + O(p^{d/2}/d)}\\
&= \log_2 \frac{\frac{p^{d-1}}{d} - O(p^{\lfloor d/2\rfloor})}{\frac{1}{d}(\log_2 F)\,p^{d/2}\log p + O(p^{d/2}/d)} \qquad \text{by (1.1)}\\
&= \log_2 \frac{p^{d/2}(\frac{p^{d/2-1}}{d} - c_1)}{\frac{1}{d}\log_2(F)\,p^{d/2}\log p + O(p^{d/2}/d)}\\
&\ge \log_2 \frac{\frac{p^{d/2-1}}{d} - c_1}{\frac{1}{d}\log_2(\frac{p^{d-1}}{d} - O(p^{\lfloor d/2\rfloor}))\ \log p + c_2}\\
&\ge \log_2 \frac{\frac{p^{d/2-1}}{d} - c_1}{\frac{1}{d}(\log_2 p^d)\log p + c_2}\\
&= \log_2 \frac{\frac{p^{d/2-1}}{d} - c_1}{(\log_2 p)\log p + c_2}\\
&\ge \frac{1}{2}\log_2(\frac{p^{d/2-1}}{d} - c_1)^2 - \log_2(\log^2 p + c_2)\\
&\ge \frac{1}{2}\log_2(\frac{p^{d-2}}{d^2} - 2\,c_1\,\frac{p^{d/2-1}}{d} + {c_1}^2) - \log_2(\log^2 p + c_2)\\
&\ge (\frac{1}{2} - o(1))\frac{\log p^{d-2}/d^2}{\log 2}.
\end{aligned}$$

□

We note that the lower bound in Theorem 2 on $C(\mathcal{F}_d)$ increases when d increases. In particular, it reduces to $\left(\frac{1}{2} - o(1)\right)\frac{\log p}{\log 2}$ if $d = 3$.

Gyarmati et. al. proved that the cross-correlation measure of the family given in Theorem 2 is small and satisfies

$$\Phi_k(\mathcal{F}_d) \ll kdp^{1/2}\log p \tag{3.3}$$

for each integer $k \in \{1, 2, 3, \ldots, p-1\}$, see [18, Theorem 8.14].

Example 2. *Let $p = 11$ and $d = 5$.*

$$\Omega_5 = \{f(x) = x^5 + a_2x^3 + a_3x^2 + a_4x + a_5 \in \mathbb{F}_{11}[x] : f \text{ is irreducible over } \mathbb{F}_{11}\}.$$

This family consists of 2640 irreducible polynomials. The f-complexity of this family is 8. The lower bound in (3.1) *is approximately 3, which is convenient with this example. However, the lower bound is not close for small primes. On the other hand, the cross-correlation measure of order 5 of the family gets the maximum value 10 with M=10, I=[2573, 244, 2118, 1629, 740] and D=[0,0,0,0,0]. This value is also far from the asymptotic bound in* (3.3).

4. Sequences on k-symbols alphabet

In [28] the correlation measure of a sequence consisting of symbols $\{a_1, a_2, \ldots, a_k\}$ is defined. We similarly extend the definition of cross-correlation measure for a family of sequences consisting of k-symbols in the following.

Definition 3. *The cross-correlation measure of order ℓ of a family $\mathcal{F}$ of sequences $E_{i,N} = (e_{i,1}, e_{i,2}, \ldots, e_{i,N}) \in \{a_1, a_2, \ldots, a_k\}^N$, $i = 1, 2, \ldots, F$, is defined as*

$$\gamma_\ell(\mathcal{F}) = \max_{W,M,D,I} \left| g(\mathcal{F}, W, M, D, I) - \frac{M}{k^\ell} \right|$$

for

$$g(\mathcal{F}, W, M, D, I) := |\{n : 1 \le n \le M, (e_{i_1,n+d_1}, \ldots, e_{i_\ell,n+d_\ell}) = W\}|,$$

where $W \in \{a_1, a_2, \ldots, a_k\}^\ell$, D denotes an ℓ tuple $(d_1, d_2, \ldots, d_\ell)$ of integers such that $0 \le d_1 \le d_2 \le \cdots \le d_\ell < M + d_\ell \le N$ and $d_i \ne d_j$ if $E_{i,N} = E_{j,N}$ for $i \ne j$, and I denotes an ℓ tuple $(i_1, i_2, \ldots, i_\ell) \in \{1, 2, \ldots, F\}^\ell$.

The definition of f-complexity $\mathrm{C}(\mathcal{F})$ for a family $\mathcal{F}$ of binary sequences can be directly generalized to a family of sequences consisting of k-symbols.

Definition 4. *The f-complexity $C(\mathcal{F})$ of a family $\mathcal{F}$ of k-symbol sequences $E_N \in \{a_1, a_2, \ldots, a_k\}^N$ of length N is the greatest integer $j \ge 0$ such that for any $1 \le i_1 < i_2 < \cdots < i_j \le N$ and any $\epsilon_1, \epsilon_2, \ldots, \epsilon_j \in \{a_1, a_2, \ldots, a_k\}$ there is a sequence $E_N = (e_1, e_2, \ldots, e_N) \in \mathcal{F}$ with*

$$e_{i_1} = \epsilon_1, e_{i_2} = \epsilon_2, \ldots, e_{i_j} = \epsilon_j.$$

Now we prove the following extension of (1.3).

Theorem 3. *Let $\mathcal{F}$ be a family of sequences $(e_{i,1},\dots,e_{i,N}) \in \{a_1,a_2,\dots,a_k\}^N$ for $i = 1,2,\dots,F$ and $\overline{\mathcal{F}}$ its dual family of binary sequences $(e_{1,n},e_{2,n},\dots,e_{F,n}) \in \{a_1,a_2,\dots,a_k\}^F$ for $n = 1,2,\dots,N$. Then we have*

$$C(\mathcal{F}) \geq \left\lceil \log_k F - \log_2 \max_{1\leq i\leq \log_k F} \gamma_i(\overline{\mathcal{F}}) \right\rceil - 1 \tag{4.1}$$

and

$$C(\overline{\mathcal{F}}) \geq \left\lceil \log_k F - \log_2 \max_{1\leq i\leq \log_k F} \Gamma_i(\overline{\mathcal{F}}) \right\rceil - 1, \tag{4.2}$$

where $\log_k$ *denotes the base k logarithm.*

Proof. Assume that for an integer j a specification

$$e_{k,n_1} = b_1, e_{k,n_2} = b_2, \dots, e_{k,n_j} = b_j \tag{4.3}$$

for $B = (b_1,b_2,\dots,b_j) \in \{a_1,a_2,\dots,a_k\}^j$ occurs in the family $\mathcal{F}$ for some $k \in \{1,2,\dots,F\}$. Let A denotes the number of sequences in $\mathcal{F}$ satisfying (4.3). By the definition of cross-correlation, we have

$$\begin{aligned}\gamma_j(\overline{\mathcal{F}}) &= \max_{W,M,D,I}\left|g(\overline{\mathcal{F}},W,M,D,I) - \frac{M}{k^j}\right| \\ &\geq \left|g(\overline{\mathcal{F}},B,F,(0,0,\dots,0),(n_1,\dots,n_j)) - \frac{F}{k^j}\right| \\ &\geq \left|A - \frac{F}{k^j}\right|.\end{aligned}$$

Hence, we obtain that

$$A \geq \frac{F}{k^j} + \gamma_j(\overline{\mathcal{F}}).$$

If $j < \log_k F - \log_k \gamma_j(\overline{\mathcal{F}})$ then there exists at least one sequence in $\mathcal{F}$ satisfying (4.3). Therefore, for all integers $j \geq 0$ satisfying

$$j < \log_2 F - \log_k \max_{1\leq \ell\leq \log_k F} \gamma_\ell(\overline{\mathcal{F}}),$$

we have $A > 0$ which completes the proof of (4.1). And the proof of (4.2) is done similarly. □

5. A large family of k-symbols sequences with low cross-correlation and high family complexity

In this section we extend the family of binary sequences that we have presented in Section 3 to the k-symbol alphabet. We prove the following generalization of Theorem 2. The proof is similar to proof of Theorem 2 see also [27, Theorem 3].

Theorem 4. *Let d and $p > 2$ be distinct prime numbers and k be a positive integer such that*

$$\gcd(k, \frac{p^d-1}{p-1}) = 1.$$

Let f_β be an irreducible polynomial of degree d over the finite field $\mathbb{F}_p$ such that

$$f_\beta(x) = (x-\beta)(x-\beta^p)\cdots(x-\beta^{p^{d-1}})$$

for an element $\beta \in \mathbb{F}_{p^d}$. Let a family $\mathcal{F}$ of k-ary sequences be defined as

$$\mathcal{F} = \left\{ \left(\chi(f_\beta(n))\right)_{n=1}^{p-1} : \beta \in \mathbb{F}_{p^d} \backslash \mathbb{F}_p \textit{ and } \mathrm{Tr}(\beta) = 0 \right\}$$

for some character χ of order k. Then we have

$$\gamma_\ell(\mathcal{F}) \ll \ell p^{1/2} \log p \tag{5.1}$$

for each integer $l \in \{2, 3, \ldots, p-1\}$ and

$$C(\mathcal{F}) \geq (\frac{d}{2} - 1) \log_2 p - \log_2 ((d-1)\log_2 p). \tag{5.2}$$

The family size equals

$$F = \frac{p^d - p}{dp}.$$

Proof. Let a be a k-th root of unity and $S(a, m)$ denote

$$S(a,m) = \frac{1}{k} \sum_{t=1}^{k} \overline{a} \chi(m)^t.$$

Then we have

$$S(a,m) = \begin{cases} 1 & \text{if } \chi(m) = a, \\ 0 & \text{if } \chi(m) \neq a. \end{cases}$$

Now we estimate $g(\mathcal{F}, W, M, D, I)$ as follows:

$$\begin{aligned} g(\mathcal{F}, W, M, D, I) &= |\{n : 1 \leq n \leq M, (e_{i_1, n+d_1}, \ldots, e_{i_\ell, n+d_\ell}) = W\}| \\ &= \sum_{n=1}^{M} \prod_{j=1}^{\ell} S(a_j, f_{i_j}(n+d_j)) \\ &= \sum_{n=1}^{M} \prod_{j=1}^{\ell} \frac{1}{k} \sum_{t_j=1}^{k} (\overline{a_j} \chi(f_{i_j}(n+d_j)))^{t_j} \\ &= \frac{1}{k^\ell} \sum_{t_1=1}^{k} \cdots \sum_{t_\ell=1}^{k} \overline{a_1^{t_1}} \cdots \overline{a_\ell^{t_\ell}} \sum_{n=1}^{M} \chi(f_{i_1}(n+d_1))^{t_1} \cdots \chi(f_{i_\ell}(n+d_\ell))^{t_\ell} \\ &= \frac{M}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \overline{a_1^{t_1} \cdots a_\ell^{t_\ell}} \sum_{n=1}^{M} \chi(f_{i_1}(n+d_1)^{t_1} \cdots f_{i_\ell}(n+d_\ell)^{t_\ell}) \\ &\leq \frac{M}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \left| \sum_{n=1}^{M} \chi(f_{i_1}(n+d_1)^{t_1} \cdots f_{i_\ell}(n+d_\ell)^{t_\ell}) \right|. \end{aligned}$$

Now consider the polynomial

$$f(n) = f_{i_1}(n+d_1)^{t_1} \cdots f_{i_\ell}(n+d_\ell)^{t_\ell}.$$

We will show that it is not a k-th power of a polynomial over $\mathbb{F}_p$. As $n + d_j < p$ for $j = 1, 2, \dots, \ell$, we can write f as follows:

$$f(n) = (n + d_1 - \beta_{i_1})^{t_1 \frac{p^d-1}{p-1}} \cdots (n + d_\ell - \beta_{i_\ell})^{t_\ell \frac{p^d-1}{p-1}}$$

for some $\beta_{i_1}, \dots, \beta_{i_\ell} \in \mathbb{F}_{p^d} \backslash \mathbb{F}_p$ and $\mathrm{Tr}(\beta_{i_j}) = 0$ for all $j \in \{1, 2, \dots, \ell\}$. Then, the linear terms $(n + d_1 - \beta_{i_1}), \dots, (n + d_\ell - \beta_{i_\ell})$ are distinct from each other. So it is enough to show that the power of each component is not divisible by k. And this holds as we have $t_1, \dots, t_\ell < k$ and $\gcd(k, \frac{p^d-1}{p-1}) = 1$.

By applying Weil's Theorem to the inner character sum, we obtain

$$\left| g(\mathcal{F}, W, M, D, I) - \frac{M}{k^\ell} \right| \ll \ell p^{1/2} \log(p),$$

and by substituting this into Definition 3 we complete the proof of (5.1).

Next we prove the bound (5.2). Before this we note that family size equals the number of irreducible polynomials of degree d over $\mathbb{F}_p$ having zero trace since they all produce a distinct sequence in $\mathcal{F}$. Note that there are $\frac{p^d-p}{p}$ distinct elements in $\mathbb{F}_{p^d} \backslash \mathbb{F}_p$ having zero trace, and d of them combines into an irreducible polynomial over $\mathbb{F}_p$. So we have

$$F = \frac{p^d - p}{dp}. \tag{5.3}$$

$$\begin{aligned}
\sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, f_n(i_j)) &\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \left| \sum_{n=1}^{F} \chi((i_1 - \beta_n)^{t_1 \frac{p^d-1}{p-1}} \cdots (i_\ell - \beta_n)^{t_\ell \frac{p^d-1}{p-1}}) \right| \\
&\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \left| \sum_{\substack{\beta \in \mathbb{F}_{p^d} \backslash \mathbb{F}_p, \mathrm{Tr}(\beta)=0 \\ nonconjugate}}^{F} \chi((i_1 - \beta)^{t_1 \frac{p^d-1}{p-1}} \cdots (i_\ell - \beta)^{t_\ell \frac{p^d-1}{p-1}}) \right| \qquad (5.4) \\
&\le \frac{F}{k^\ell} + \frac{1}{k^\ell} \sum_{t_1=1}^{k-1} \cdots \sum_{t_\ell=1}^{k-1} \frac{1}{dp} \left| \sum_{\beta \in \mathbb{F}_{p^d} \backslash \mathbb{F}_p}^{F} \chi((i_1 - \beta)^{t_1 \frac{p^d-1}{p-1}} \cdots (i_\ell - \beta)^{t_\ell \frac{p^d-1}{p-1}}) \right|.
\end{aligned}$$

Now we estimate

$$\begin{aligned}
g(\overline{\mathcal{F}}, W, F, 0, I) &= |\{n : 1 \le n \le F, (\overline{e}_{i_1, n+d_1}, \dots, \overline{e}_{i_\ell, n+d_\ell}) = W\}| \\
&= \sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, \overline{f}_{i_j}(n)) \\
&= \sum_{n=1}^{F} \prod_{j=1}^{\ell} S(a_j, f_n(i_j)).
\end{aligned}$$

Similar to the proof of (5.1), we have a similar equation array as given in (5.4).

Since $\mathrm{Tr}(\beta) = 0$ and $\gcd(k, \frac{p^d-1}{p-1}) = 1$, the polynomial inside the character sum is not a k-th power. Thus, by Weil's Theorem, we have

$$\left| g(\overline{\mathcal{F}}, W, F, 0, I) - \frac{F}{k^\ell} \right| \ll \frac{1}{dp} [(\ell p - 1) p^{d/2} + p],$$

and so by Definition 3 we have

$$\gamma^{\circ}(\overline{\mathcal{F}}) \ll \frac{1}{dp}[(\ell p-1)p^{d/2}+p]. \tag{5.5}$$

Therefore, by using (5.3) and (5.5), we obtain that

$$\begin{aligned} C(\mathcal{F}) &\geq \log_2 \frac{F}{\max_{1\leq \ell \leq \log_2 F} \gamma_{\ell}^{\circ}(\overline{\mathcal{F}})} \\ &\geq (\frac{d}{2}-1)\log_2 p - \log_2((d-1)\log_2 p) \end{aligned}$$

as desired. □

6. Conclusions

Pseudorandom sequences are used in many practical areas, and their quality is decided by statistical test packages as well as by proved results on certain measures. In addition, a large family of good pseudorandom sequences in terms of several directions is required in some applications. In this paper we studied two such measures: the f-complexity, and the cross-correlation measure of order ℓ for family of sequences on binary and k-symbols alphabets. We considered two families of binary sequences of Legendre-symbols

$$\mathcal{F}_1 = \left\{ \left(\frac{f_i(n)}{p} \right)_{n=1}^{p-1} : i = 1, \dots, p-1 \right\}$$

for irreducible polynomials $f_i(x) = x^d + a_2 i^2 x^{d-2} + a_3 i^3 x^{d-3} + \cdots + a_{d-2} i^{d-2} x^2 + a_d i^d$ and

$$\mathcal{F}_2 = \left\{ \left(\frac{f(n)}{p} \right)_{n=1}^{p-1} : f \text{ is irreducible of degree } d \text{ over } \mathbb{F}_p \right\}$$

for a positive integer d. We showed that the families $\mathcal{F}_1$ and $\mathcal{F}_2$ have both a large family complexity and a small cross-correlation measure up to a rather large order. Then we proved the analog results for the family of sequences on k-symbols alphabet, and constructed a good family of k-symbols sequences.

Author contributions

All authors contributed equally to all parts of the paper. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgement

The authors would like to thank anonymous reviewers for their careful reading and helpful suggestions, which improved the presentation of the paper.

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. R. Ahlswede, L. H. Khachatrian, C. Mauduit, A. Sárközy, A complexity measure for families of binary sequences, *Period. Math. Hung.*, **46** (2003), 107–118. https://doi.org/10.1023/A:1025962825241
2. R. Ahlswede, C. Mauduit, A. Sárközy, Large families of pseudorandom sequences of k-symbols and their complexity, I-II, In: *General theory of information transfer and combinatorics*, Berlin: Springer, 2006.
3. N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl, Measures of pseudorandomness for finite sequences: Typical values, *Proc. Lond. Math. Soc.*, **95** (2007), 778–812. https://doi.org/10.1112/plms/pdm027
4. Y. Çakıroglu, O. Yayla, E. Sercan Yılmaz, The number of irreducible polynomials over finite fields with vanishing trace and reciprocal trace, *Des. Codes Cryptogr.*, **90** (2022), 2407–2417. https://doi.org/10.1007/s10623-022-01088-2
5. J. Cassaigne, C. Mauduit, A. Sarkozy, On finite pseudorandom binary sequences VII: The measures of pseudorandomness, *Acta Aritmetica-Warszawa*, **103** (2002), 97–118.
6. Z. Chen, Elliptic curve analogue of Legendre sequences, *Monatsh. Math.*, **154** (2008), 1–10. https://doi.org/10.1007/s00605-008-0520-x
7. Z. Chen, A. Ostafe, A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, In: *International Workshop on the Arithmetic of Finite Fields*, Berlin: Springer, **6087** (2010), 73–85. https://doi.org/10.1007/978-3-642-13797-6_6
8. J. Dick, F. Pillichshammer, *Digital nets and sequences: discrepancy theory and quasi–Monte Carlo integration*, Cambridge: Cambridge University Press, 2010.
9. X. Du, Z. Lin, On pseudorandom sequences of k-symbols constructed using finite fields, *Appl. Algebra Eng. Commun. Comput.*, **25** (2014), 265–285. https://doi.org/10.1007/s00200-014-0224-5
10. J. Folláth, Construction of pseudorandom binary sequences using additive characters over GF(2k), *Period. Math. Hung.*, **57** (2008), 73–81. https://doi.org/10.1007/s10998-008-7073-1
11. B. Gergely, On finite pseudorandom sequences of k-symbols, *Period. Math. Hung.*, **47** (2003), 29–44. https://doi.org/10.1023/b:mahu.0000010809.50836.79
12. S. W. Golomb, G. Gong, *Signal design for good correlation*, Cambridge: Cambridge University Press, 2005.

13. D. Gomez, A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hung.*, **64** (2012), 161–168. https://doi.org/10.1007/s10998-012-3747-1

14. L. Goubin, C. Mauduit, A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory*, **106** (2004), 56–69. https://doi.org/10.1016/j.jnt.2003.12.002

15. K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hung.*, **49** (2004), 45–63. https://doi.org/10.1007/s10998-004-0522-y

16. K. Gyarmati, On the complexity of a family related to the Legendre symbol, *Period. Math. Hung.*, **58** (2009), 209–215. https://doi.org/10.1007/s10998-009-10209-4

17. K. Gyarmati, Measures of pseudorandomness. In: *Finite fields and their applications: character sums and polynomials*, Berlin: Springer, **11** (2013), 43–64. https://doi.org/10.1515/9783110283600

18. K. Gyarmati, C. Mauduit, A. Sárközy, The cross-correlation measure for families of binary sequences, In: *Applied algebra and number theory*, Cambridge: Cambridge University Press, 126–143, 2014.

19. H. Iwaniec, E. Kowalski, *Analytic number theory*, Providence, RI: American Mathematical Society, 2004.

20. P. L'Ecuyer, R. Simard, Testu01: AC library for empirical testing of random number generators, *ACM Transact. Math. Software (TOMS)*, **33** (2007), 1–40. https://doi.org/10.1145/1268776.1268777

21. H. Liu, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, *Proc. Amer. Math. Soc.*, **135** (2007), 1309–1318. https://doi.org/10.1090/S0002-9939-06-08630-8

22. H. Liu, B. Gao, A large family of pseudorandom sequences of k symbols with length *pq*, *Acta Arith.*, **181** (2017), 1–26. https://doi.org/10.4064/aa8452-5-2017

23. H. Liu, X. Liu, Binary sequence family with both small cross-correlation and large family complexity, *Finite Fields Appl.*, **97** (2024), 102440. https://doi.org/10.1016/j.ffa.2024.102440

24. K. Mak, More constructions of pseudorandom sequences of k symbols, *Finite Fields Appl.*, **25** (2014), 222–233. https://doi.org/10.1016/j.ffa.2013.09.006

25. G. Marsaglia, Diehard: a battery of tests of randomness, 1996.

26. C. Mauduit, J. Rivat, A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatsh. Math.*, **141** (2004), 197–208. https://doi.org/10.1007/s00605-003-0112-8

27. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, **82** (1997), 365–377.

28. C. Mauduit, A. Sárközy, On finite pseudorandom sequences of k symbols, *Indag. Math.*, **13** (2002), 89–101.

29. C. Mauduit, A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Math. Hung.*, **108** (2005), 239–252. https://doi.org/10.1007/s10474-005-0222-y

30. L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters, *Publ. Math. Debrecen*, **80** (2012), 199–213.

31. L. Mérai, The cross-correlation measure of families of finite binary sequences: limiting distributions and minimal values, *Discrete Appl. Math.*, **214** (2016), 153–168. https://doi.org/10.1016/j.dam.2016.06.024

32. L. Mérai, On the typical values of the cross-correlation measure, *Monatsh. Math.*, **180** (2016), 83–99. https://doi.org/10.1007/s00605-016-0886-0

33. L. Mérai, O. Yayla, Improving results on the pseudorandomness of sequences generated via the additive order of a finite field, *Discrete Math.*, **338** (2015), 2020–2025. https://doi.org/10.1016/j.disc.2015.04.015

34. H. Niederreiter, A. Winterhof, *Applied number theory*, Berlin: Springer, 2015.

35. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, technical report, *DTIC Document*, 2001.

36. A. Sárközy, A. Winterhof, Measures of pseudorandomness for binary sequences constructed using finite fields, *Discrete Math.*, **309** (2009), 1327–1333. https://doi.org/10.1016/j.disc.2008.01.056

37. A. Sárközy, On pseudorandomness of families of binary sequences, *Discrete Appl. Math.*, **216** (2017), 670–676. https://doi.org/10.1016/j.dam.2015.07.031

38. A. Tietäväinen, Vinogradov's method and some applications, *Number Theory Appl.*, **204** (1999), 261–282.

39. A. Topuzoglu, A. Winterhof, Pseudorandom sequences, In: *Topics in Geometry, Coding Theory and Cryptography*, Dordrecht: Springer, **6** (2007), 135–166. https://doi.org/10.1007/1-4020-5334-4_4

40. V. Tóth, Extension of the notion of collision and avalanche effect to sequences of k symbols, *Period. Math. Hung.*, **65** (2012), 229–238. https://doi.org/10.1007/s10998-012-1005-1

41. A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci.*, **34** (1948), 204–207. https://doi.org/10.1073/pnas.34.5.204

42. A. Winterhof, Some estimates for character sums and applications, *Des. Codes Cryptogr.*, **22** (2001), 123–131. https://doi.org/10.1023/A:1008300619004

43. A. Winterhof, O. Yayla, Family complexity and cross-correlation measure for families of binary sequences, *Ramanujan J.*, **39** (2016), 639–645. https://doi.org/10.1007/s11139-014-9649-5

44. J. L. Yucas, Irreducible polynomials over finite fields with prescribed trace/prescribed constant term, *Finite Fields Appl.*, **12** (2006), 211–221. https://doi.org/10.1016/j.ffa.2005.04.006