Applicable Algebra in Engineering, Communication and Computing (2022) 33:173–192
https://doi.org/10.1007/s00200-020-00442-y

ORIGINAL PAPER

A new lower bound on the family complexity of Legendre sequences

Yağmur Çakıroğlu[1] · Oğuz Yayla[1]

Received: 23 October 2019 / Revised: 16 May 2020 / Accepted: 8 June 2020 / Published online: 22 June 2020

Abstract

In this paper we study a family of Legendre sequences and its pseudo-randomness in terms of their family complexity. We present an improved lower bound on the family complexity of a family based on the Legendre symbol of polynomials over a finite field. The new bound depends on the Lambert W function and the number of elements in a finite field belonging to its proper subfield. Moreover, we present another lower bound which is a simplified version and approximates the new bound. We show that both bounds are better than previously known ones.

Keywords Pseudo-randomness · Family complexity · Family of Legendre sequences · Lambert W function · Polynomials over finite fields

Mathematics Subject Classification 11K45 · 94A55 · 94A60

1 Introduction

A pseudo-random sequence is a sequence of numbers which is generated by a deterministic algorithm and looks truly random. By truly random we mean that each element of the sequence can not be predicted from others, for instance a sequence generated by samples of atmospheric noise. A pseudo-random sequence in the interval [0, 1) is called a sequence of pseudo-random numbers. Pseudo-random sequences were widely studied in the literature (see [31, 32, 36]). Randomness measures of a sequence depend on its application area, for instance, it has to be unpredictable for cryptographic applications [26], uncorrelated for wireless communication applications [13] and uniformly distributed for quasi-Monte Carlo methods [28, 29]. In this paper we consider the *Legendre sequence* which is the binary sequence $E_p(f) = (e_1, \dots, e_p)$ defined by

✉ Oğuz Yayla
oguz.yayla@hacettepe.edu.tr

Yağmur Çakıroğlu
yagmur.cakiroglu@hacettepe.edu.tr

1 Hacettepe University, Department of Mathematics, Beytepe 06800, Ankara, Turkey

$$e_j = \begin{cases} \left(\frac{f(j)}{p}\right) & \text{for } \gcd(f(j), p) = 1, \\ 1 & \text{for } p|f(j), \end{cases}$$

where p is a prime number, $j = 1, 2, \dots, p$ and f is a polynomial over a finite field with p elements.

It is known that the Legendre sequence has several good randomness measures such as high linear complexity [4, 8, 33, 37] and small correlation measure up to rather high orders [23] for cryptography, and a small (aperiodic) auto-correlation [25, 30] for wireless communication, GPS, radar or sonar.

When a family of sequences is considered for an application, e.g. as a key-space of a cryptosystem, then its randomness in terms of many directions is concerned. For instance, a family of sequences must have a large family size, large family complexity, and low cross-correlation. Family complexity (f-complexity) was first introduced as a randomness measure by Ahlswede, Khachatrian, Mauduit and Sárközy [1]. Then they studied families of pseudo-random sequences on k-symbols and their f-complexity [2, 3]. Mauduit and Sárközy [24] studied the f-complexity of sequences of k-symbols and they also gave the connection between f-complexity and VC-dimension. Winterhof and the second author [40] gave a relation between f-complexity and cross-correlation measure. Moreover the complexity measures for different families have been studied in the literature [5, 11, 14, 17–19]. Sárközy [34] wrote a survey about definitions of various measures of family of binary sequences (e.g. f-complexity, collision, minimum distance, avalanche effect, and cross-correlation measure).

Gyarmati [16] presented a bound for the f-complexity of Legendre sequences constructed by some polynomials of degree k over a prime finite field $\mathbb{F}_p$. In this paper, we prove a new bound, which improves the bound given in [16] for any prime p and degree k (see Theorem 1). Moreover, we obtain a simplified lower bound and prove that our bound is better than the bound given in [16] (see Corollary 2). In particular, the new bound surpluses overwhelmingly the bound given in [16] for small k and it gets closer for large k (see Figs. 3, 4 and 5). We also see from these figures that our bound provides a better lower level. We also compare both bounds in terms of time complexity, for which we plot the difference between the elapsed times required to calculate both bounds (see Figs. 7 and 8).

The paper is organized as follows. The new bound we present in this paper depends on the Lambert W function, so we give its definition and some properties in Sect. 2. Then we present some auxiliary lemmas in Sect. 3 and previous results in Sect. 4. Next, we give our main contribution in Sect. 5. Finally we compare the new bound and Gyarmati's one in Sect. 6.

2 Lambert *W* function

In this section we introduce the definition of the Lambert W function and present some of its properties.

Definition 1 [7] The *Lambert W function*, also called the omega function or product logarithm, is defined as the multivalued function W that satisfies

$$z = W(z)e^{W(z)}$$

for any complex number z.

Equivalently, the Lambert W function is known as the inverse function of $f(z) = ze^z$. Note that the multivaluedness of the Lambert W function means that there are multiple solutions for some values since the function f is not injective. The equation $y = ze^z$ is by definition solved by

$$z = W(y),$$

and the equation $y = z\log z$ is solved by

$$z = \frac{y}{W(y)}. \tag{1}$$

So, equations containing exponential expressions can be solved by the Lambert W function. For instance, the equation $xa^x = b$ is solved by $x = \frac{W(b\ln(a))}{\ln(a)}$, the equation $a^x = x + b$ is solved by $x = \frac{-b-W\left(-a^{-b}\ln(a)\right)}{\ln(a)}$, and the equation $x^{x^a} = b$ is solved by $\exp\left(\frac{W(a\log(b))}{a}\right)$, where "ln" stands for the natural logarithm. The Lambert W function stems from the equation proposed by Johann Heinrich Lambert in 1758

$$x^\alpha - x^\beta = (\alpha - \beta)vx^{\alpha+\beta},$$

which is known as Lambert's transcendental equation. Then in 1779 Euler wrote a paper [10] about this equation and introduced a special case which is nearly the definition of the W function. He referenced work by Lambert in his paper, and so this function is called Lambert W function. From now on we will use W as the Lambert W function. The W function, which has applications in many fields from past to present, was applied to problems ranging from quantum physics to population dynamics, to the complexity of algorithms (see [7, 38]). The new bound we obtain for family complexity given in this paper is related to this function. Now we give a simple example in order to show how we use this function.

Example 1 Let us solve $4^{-t} = 3t$ for t. We first multiply both sides by $\frac{\ln 4}{3}4^t$ to get:

$$\frac{\ln 4}{3} = t\ln 4\, 4^t = t\ln 4\, e^{t\ln 4}$$

Since the right hand side of the equation is of the form ze^z for $z = t\ln 4$, we can write the solution using the definition of the W function

$$t = \frac{W\left(\frac{\ln 4}{3}\right)}{\ln 4},$$

which is approximately $t \approx 0.239243358717019$.

The graph of the W function on the real plane is plotted in Fig. 1.

We note that the W function can be approximately evaluated by using some root-finding methods as given in [7]. Futhermore, in [7] it is shown that

$$W(x) = L_1 - L_2 + \frac{L_2}{L_1} + \frac{L_2(-2 + L_2)}{2L_1^2} + \frac{L_2(6 - 9L_2 + 2L_2^2)}{6L_1^3} + \cdots \tag{2}$$

where $L_1 = \ln x$, $L_2 = \ln \ln x$. Then keeping only the first two terms of the expansion (2) we have

$$W(x) = \ln x - \ln \ln x + o(1). \tag{3}$$

In the following lemma, the bounds were given with error term $o\left(\frac{\ln \ln x}{\ln x}\right)$ instead of $o(1)$, with certain coefficients for error terms.

Lemma 1 [21] *For every $x \geq e$ we have*

$$\ln x - \ln \ln x + \frac{1}{2}\frac{\ln \ln x}{\ln x} \leq W(x) \leq \ln x - \ln \ln x + \frac{e}{e-1}\frac{\ln \ln x}{\ln x}, \tag{4}$$

with equality only when $x = e$.

3 Preliminaries

In this section we present some definitions and results which we need for the proof of the main results introduced in this paper.

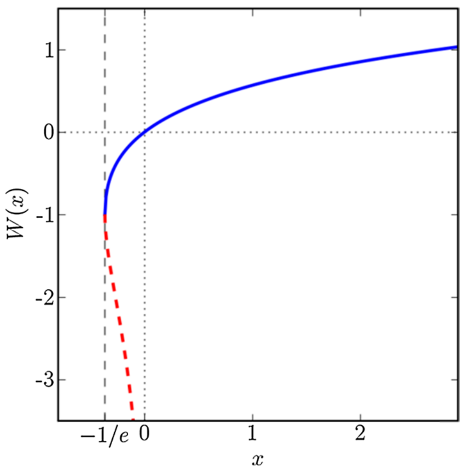

Fig. 1 The graph of the W function obtained in Example 1

Definition 2 Let q be a prime power and $\mathbb{F}_{q^n}$ denote the finite field of q^n elements and define $G_{q,n}$ as follows.

$$G_{q,n} = \{\alpha \in \mathbb{F}_{q^n} : \exists t, t|n, 0 < t < n \text{ such that } \alpha \in \mathbb{F}_{q^t} \subset \mathbb{F}_{q^n}\}$$

In other words, the set $G_{q,n}$ consists of all elements belonging to the proper subfields of $\mathbb{F}_{q^n}$.

One can calculate the number of elements in $G_{q,n}$ for given q and n by counting the elements in the proper subfields of $\mathbb{F}_{q^n}$. However, this method would be inefficient. Thus, we need a formula for $|G_{q,n}|$ and, in order to do that, we give some definitions and results below.

Definition 3 [27, Definition 2.1.22] The *Möbius* μ *function* is defined on the set of positive integers as

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^k & \text{if } m = m_1 m_2 \dots m_k \text{ where the } m_i \text{ are distinct primes,} \\ 0 & \text{if } p^2 \text{ divides } m \text{ for some prime } p. \end{cases}$$

Let $I_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ for a prime power q.

Gauss discovered the formula presented in the following result and so it was called after him [12].

Proposition 1 *For a positive integer n and a prime power q,*

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

For more details about this formula see [9, Chapter 14.3], [27, Theorem 2.1.24] or [6].

Lemma 2 *Let* $n \in \mathbb{N}$ *and q be a prime power. Then*

$$|G_{q,n}| = q^n - nI_q(n).$$

Proof It is clear that any root of an irreducible polynomial of degree n over $\mathbb{F}_q$ can not be an element of a proper subfield of $\mathbb{F}_{q^n}$. Hence the proof follows. □

Example 2 Let q be a prime power. Consider $\mathbb{F}_{q^n}$ for $n = 105$. Then, the possible divisors of n are $d = 1, 3, 5, 7, 15, 21, 35, 105$ and by Lemma 2 we get

$$|G_{q,n}| = q^{35} + q^{21} + q^{15} - q^7 - q^5 - q^3 + q.$$

Now we define the norm and the trace of an element in a finite field. (see [22, Chapter 2] for more details).

Definition 4 For $\alpha \in \mathbb{F}_{q^n}$ the *norm* $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ of α is defined by

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

and the *trace* $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ of α is defined by

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}.$$

In particular, $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ are elements of $\mathbb{F}_q$.

Definition 5 [22, Chapter 5] Let χ be an additive and ψ be a multiplicative character of $\mathbb{F}_q$. Then χ and ψ can be *lifted* to $\mathbb{F}_{q^n}$ by setting $\chi'(\alpha) = \chi(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha))$ for $\alpha \in \mathbb{F}_{q^n}$ and $\psi'(\alpha) = \psi(\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha))$ for $\alpha \in \mathbb{F}_{q^n}^*$. Also from the additivity of the trace and multiplicativity of the norm, χ' is an additive and ψ' is a multiplicative character of $\mathbb{F}_{q^n}$.

We need the following lemma for the proof of Theorem 1.

Lemma 3 [16, Corollary 2.1.] *Let $p > 2$ be a prime number and $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol. Let γ be the quadratic character of $\mathbb{F}_{p^n}$. Then for $\alpha \in \mathbb{F}_{p^n}^*$,*

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

Next, we define two new polynomials obtained from a given polynomial over a finite field.

Definition 6 Given $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{F}_{q^n}[x]$, we define

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

for $0 \le s \le n-1$ and

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

Next, we give a result which will be the basis of the proof of our main theorem.

Lemma 4 [22, Exercise 5.64] *Let $i_1, \ldots, i_j$ be distinct elements of $\mathbb{F}_{p^k}$, p odd prime, and $\epsilon_1, \ldots, \epsilon_j \in \{-1, +1\}$. Let $N(\epsilon_1, \ldots, \epsilon_j)$ denote the number of $\alpha \in \mathbb{F}_{p^k}$ with $\gamma(\alpha + i_s) = \epsilon_s$ for $s = 1, 2, \ldots, j$ where γ is the quadratic character of $\mathbb{F}_{p^k}$. Then,*

$$\left| N(\epsilon_1, \ldots, \epsilon_j) - \frac{p^k}{2^j} \right| \le \left(\frac{j-2}{2} + \frac{1}{2^j}\right) p^{k/2} + \frac{j}{2}.$$

Proof By definition we have

$$N(\epsilon_1, \dots, \epsilon_j) = \frac{1}{2^j} \sum_{\alpha \in \mathbb{F}_{p^k}} [1 + \epsilon_1 \gamma(\alpha + i_1)] \cdots [1 + \epsilon_j \gamma(\alpha + i_j)] - A,$$

where $0 \leq A \leq j/2$. Note that $\gamma(\alpha + i_j)$ can be 0 for some $\alpha \in \mathbb{F}_{p^k}$ which adds 2^{j-1} to the summation, and this can occur at most j times. So, that is the reason why we have $0 \leq A \leq j/2$. By expanding the inner multiplication we get that

$$\begin{aligned} N(\epsilon_1, \dots, \epsilon_j) = \frac{1}{2^j} \sum_{\alpha \in \mathbb{F}_{p^k}} \Bigg[1 &+ \sum_{s_1} \epsilon_{s_1} \gamma(\alpha + i_{s_1}) \\ &+ \sum_{s_1, s_2} \epsilon_{s_1} \gamma(\alpha + i_{s_1}) \epsilon_{s_2} \gamma(\alpha + i_{s_2}) \\ &+ \cdots + [\epsilon_1 \gamma(\alpha + i_1) \cdots \epsilon_j \gamma(\alpha + i_j)] \Bigg] - A. \end{aligned}$$

Then by using the Weil theorem [39] (or [22, Theorem 5.41]),

$$\begin{aligned} \left| N(\epsilon_1, \dots, \epsilon_j) - \frac{p^k}{2^j} \right| &\leq \frac{1}{2^j} \sum_{i=1}^{j} \binom{j}{i} (i-1) p^{k/2} + \frac{j}{2} \\ &= \frac{1}{2^j} \left(\sum_{i=1}^{j} \binom{j}{i} i - \sum_{i=1}^{j} \binom{j}{i} \right) p^{k/2} + \frac{j}{2} \\ &= \frac{1}{2^j} (j 2^{j-1} - (2^j - 1)) p^{k/2} + \frac{j}{2}. \end{aligned}$$

Therefore, the result follows. □

4 Previous results

In this section we will give a construction method for Legendre sequences, and the definition of family complexity. Then we will recall a result given in [16]. We begin with the definition of Legendre sequence [14, 23].

Definition 7 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 $\mathbb{F}_p$, then we define the binary sequence $E_p(f) = E_p = (e_1, \dots, e_p)$ by

$$e_j = \begin{cases} \left(\frac{f(j)}{p} \right) & \text{for } \gcd(f(j), p) = 1, \\ 1 & \text{for } p | f(j), \end{cases}$$

for $j = 1, 2, \dots, p$. Let $\mathcal{F}(K, p)$ denote the set of all sequences obtained in this way.

Hoffstein and Lieman [20] proposed using the polynomials f to construct the binary sequences given in Definition 7. Goubin, Mauduit and Sárközy [14] proved that the sequences obtained in this way have strong pseudo-random properties.

We now give the definition of f-complexity of a family $\mathcal{F}$, which was first introduced by Ahlswede et al. [1].

Definition 8 The *family complexity* (in short *f-complexity*) 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

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

The f-complexity of a family $\mathcal{F}$ is denoted by $\Gamma(\mathcal{F})$.

We note that the trivial upper bound on the f-complexity $\Gamma(\mathcal{F})$ in terms of the family size $|\mathcal{F}|$ is

$$2^{\Gamma(\mathcal{F})} \leq |\mathcal{F}|. \tag{5}$$

Now we give an example for calculating the f-complexity of a family of binary sequences.

Example 3 Consider the family of binary sequences

$$\mathcal{F} = \{(1,1,1,1), (-1,-1,1,-1), (-1,-1,-1,-1), (1,1,-1,-1), (-1,1,1,1)\}.$$

It is clear that both -1 and 1 occur at the i-th location of the sequences for all $i = 1, 2, 3, 4$. In other words, the set obtained from the first entries of the sequences has both -1 and 1, similarly the other entries have both -1 and 1. Hence, the f-complexity of $\mathcal{F}$ is at least 1. On the other hand, there is no sequence in $\mathcal{F}$ consisting of the pair $(1,-1)$ in the first two entries. So we say that the f-complexity of $\mathcal{F}$ is equal to 1. Similarly, the family of binary sequences

$$\mathcal{G} = \{(1,1,1,1), (-1,1,1,-1), (-1,1,-1,-1), (1,1,-1,-1), (-1,1,1,1)\}.$$

has f-complexity 0 since -1 does not appear in the second entry of any sequences in $\mathcal{G}$.

Let $\mathcal{F}_{\text{irred}}(k,p)$ denote the family of Legendre sequences generated by irreducible polynomials of degree k over a prime field $\mathbb{F}_p$,

$$\mathcal{F}_{\text{irred}}(k,p) := \{E_p(f) : f \in \mathbb{F}_p[x] \text{ monic irreducible polynomial with degree } k\}.$$

Different properties of this family have been studied in the literature [14, 15, 18]. A lower bound on the f-complexity of the family $\mathcal{F}_{\text{irred}}(k,p)$ was proved in [16], which we present in the following theorem.

Theorem A [16] *Let p be an odd prime and k be a positive integer. Define*

$$c = \begin{cases} \frac{1}{2} \text{ if } k \le \frac{p^{1/4}}{10 \ln p}, \\ \frac{5}{2} \text{ otherwise.} \end{cases}$$

Then

$$\Gamma(\mathcal{F}_{\text{irred}}(k, p)) \ge \min \left\{ p, \frac{k - c}{2 \ln 2} \ln p \right\}.$$

Theorem A says that the *f*-complexity is at least of order $\frac{p^{1/4}}{20 \ln 2}$. In the next section, for the same family of sequences as in Theorem A, we give a new bound by using the formula $|G_{p,k}|$ given in Lemma 2 and the W function given in Definition 1.

5 Main method

The main contribution of this paper is given in this section, which is a new bound on the *f*-complexity of Legendre sequences generated by irreducible polynomials. This new bound improves the bound given in [16]. The comparison of both bounds is given in the next section.

Theorem 1 *Let p be an odd prime and k be a positive integer. Let A and B be defined as*

$$A = \frac{2p^{k/2} - 2}{1 + p^{-k/2}} \text{ and } B = \frac{2|G_{p,k}|p^{-k/2} - 2}{1 + p^{-k/2}}.$$

Then

$$\Gamma(\mathcal{F}_{\text{irred}}(k, p)) \ge \min \left\{ p, \log_2 \left(\frac{A}{W(2^B A)} \right) \right\}.$$

We first give an example for calculating the *f*-complexity of Legendre sequences.

Example 4 Let $p = 3$ and $k = 2$. Then by the definition of Legendre sequences, we get the following family of sequences.

$$\mathcal{F}_{\text{irred}}(2, 3) = \{(1, -1, -1), (-1, 1, -1), (-1, -1, 1)\}.$$

As $|\mathcal{F}_{\text{irred}}(2, 3)| = 3$, by using (5) we have $2^{\Gamma(\mathcal{F}_{\text{irred}}(2,3))} \le 3$. And by Theorem 1, we obtain

$$\Gamma(\mathcal{F}_{\text{irred}}(2, 3)) \ge \log_2 \left(\frac{3}{W(3)} \right) > 0.58167368954.$$

Therefore, we get $\Gamma(\mathcal{F}_{\text{irred}}(2, 3)) = 1$.

Before proving the Theorem 1, we will give two auxiliary lemmas. In the first lemma, the solution of a logarithmic equation is obtained by the W function. In the second lemma, we give an upper bound on j such that $|G_{p,k}| < N(\epsilon_1, \dots, \epsilon_j)$.

Lemma 5 *Let $A, B \in \mathbb{R}$. If $Bx + x\log_2 x - A = 0$, then $x = \frac{A}{W(2^B A)}$.*

Proof We have

$$x(B + \log_2 x) = A$$

or equivalently,

$$2^B x(B + \log_2 x) = 2^B A.$$

Then we get

$$2^B x(\log_2 2^B + \log_2 x) = 2^B A \implies 2^B x(\log_2(2^B x)) = 2^B A.$$

Thus by (1) we have

$$2^B x = \frac{2^B A}{W(2^B A)},$$

that is

$$x = \frac{A}{W(2^B A)}.$$

□

Lemma 6 *Let p be an odd prime and k be a positive integer. Let $|G_{p,k}|$ be defined as in Lemma 2. Let A and B be defined as*

$$A = \frac{2p^{k/2} - 2}{1 + p^{-k/2}} \text{ and } B = \frac{2|G_{p,k}|p^{-k/2} - 2}{1 + p^{-k/2}}.$$

Let j be an integer such that $j < \log_2\left(\frac{A}{W(2^B A)}\right)$. Let $\epsilon_1, \dots, \epsilon_j \in \{-1, +1\}$ and $N(\epsilon_1, \dots, \epsilon_j)$ be defined as in Lemma 4. Then

$$|G_{p,k}| < N(\epsilon_1, \dots, \epsilon_j).$$

Proof Assume that $|G_{p,k}| \geq N(\epsilon_1, \dots, \epsilon_j)$. Then by Lemma 4

$$|G_{p,k}| \geq \frac{p^k}{2^j} - p^{k/2}\left(\frac{1}{2^j} + \frac{(j-2)}{2}\right) - \frac{j}{2}.$$

Divide both sides by $p^{k/2}$

$$|G_{p,k}|p^{-k/2} \geq \frac{p^{k/2}}{2^j} - \left(\frac{1}{2^j} + \frac{(j-2)}{2}\right) - \frac{jp^{-k/2}}{2}.$$

Multiply both sides by $2(2^j)$, and so get the following inequality:

$$\begin{aligned}
&2(2^j)|G_{p,k}|p^{-k/2} \geq 2p^{k/2} - 2 - 2^j(j-2) - 2^j jp^{-k/2},\\
&2(2^j)|G_{p,k}|p^{-k/2} - 2(2^j) + 2^j j + 2^j jp^{-k/2} \geq (2p^{k/2} - 2),\\
&(2|G_{p,k}|p^{-k/2} - 2)2^j + 2^j j(1 + p^{-k/2}) \geq (2p^{k/2} - 2).
\end{aligned}$$

Divide both sides by $(1 + p^{-k/2})$,

$$\frac{(2|G_{p,k}|p^{-k/2} - 2)}{(1 + p^{-k/2})}2^j + 2^j j \geq \frac{(2p^{k/2} - 2)}{(1 + p^{-k/2})}.$$

According to the definition of A and B, we have,

$$B2^j + 2^j j \geq A.$$

Hence, by Lemma 5 and the fact that $B2^j + 2^j j$ increases with respect to j, we obtain that

$$2^j \geq \frac{A}{W(2^B A)} \text{ or equivalently } j \geq \log_2\left(\frac{A}{W(2^B A)}\right),$$

which is a contradiction. □

Proof of Thoerem 1 For all integers $j < \log_2\left(\frac{A}{W(2^B A)}\right)$ and for all tuples $(\epsilon_1, \epsilon_2, \ldots, \epsilon_j) \in \{-1, +1\}^j$, we need to show the existence of an irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree k such that

$$\left(\frac{g(i_s)}{p}\right) = \epsilon_s \text{ for } s = 1, 2, \ldots, j \tag{6}$$

for some $1 \leq i_1 < i_2 < \cdots < i_j \leq p$. Then the definition of f-complexity gives that $\Gamma(\mathcal{F}_{\text{irred}}(k, p)) \geq \log_2\left(\frac{A}{W(2^B A)}\right)$. By Lemma 6 we know that

$$|G_{p,k}| < N(\epsilon_1, \ldots, \epsilon_j).$$

By the definition of $N(\epsilon_1, \ldots, \epsilon_j)$ we get that there exists $\alpha \in \mathbb{F}_{p^k} \backslash G_{p,k}$ such that

$$\gamma(\alpha + i_s) = \epsilon_s \text{ for } s = 1, 2, \ldots, j. \tag{7}$$

Let $f(x) = x + \alpha \in \mathbb{F}_{p^k}[x]$ and we define $g(x) := N_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f(x)) \in \mathbb{F}_p[x]$. We note that g is an irreducible polynomial by using [16, Lemma 2.4]. We know that if p is a prime number, $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol and γ is the quadratic character of $\mathbb{F}_{p^k}$ then for $\alpha \in \mathbb{F}_{p^k}^*$ we have

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

By [16, Lemma 2.3], we know that if $f \in \mathbb{F}_{p^k}[x]$ then for $\alpha \in \mathbb{F}_p$ we have

$$N_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f(\alpha)) = N_{\mathbb{F}_{p^k}/\mathbb{F}_p}(f)(\alpha).$$

Finally, using (7) we get

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

as desired. □

Corollary 1 *Let p be an odd prime and K be a positive integer. Let A and B be defined as in Theorem 1. Then*

$$\Gamma(\mathcal{F}(K,p)) \geq \min\left\{p, \log_2\left(\frac{A}{W(2^B A)}\right)\right\}.$$

Proof We know that $\mathcal{F}_{\text{irred}}(K,p) \subset \mathcal{F}(K,p)$ and $\Gamma(\mathcal{F}_{\text{irred}}(k,p)) \geq \log_2 \frac{A}{W(2^B A)}$ by Theorem 1. Thus we get the result. □

Now, we consider the upper bound for the W function given in Lemma 1 and we get an approximation for the bound given in Theorem 1. Before that, we give a lemma which we use in Corollary 2 for proving that Theorem 1 provides a better bound than Theorem A.

Lemma 7 *Let p be an odd prime, k be a positive integer and c be defined as in Theorem A. Then,*

$$\min\left\{p, \log_2 \frac{p^{k/2}}{\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right)}\right\} \geq \min\left\{p, \frac{k-c}{2\ln 2}\ln p\right\}.$$

Proof For $k \leq \frac{p^{1/4}}{10\ln p}$, we have $c = 1/2$ and so

$$\frac{k-1/2}{2\ln 2}\ln p = \log_2 p^{k/2} - \log_2 p^{1/4}.$$

Hence, we need to show that

$$\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right) < p^{1/4}.$$

We have the following upper bound for the left hand side

$$\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right) = \ln\left(\frac{8}{\ln 8p^{k/2}}\right) + \ln p^{k/2} \leq \ln\left(\frac{8}{\ln 8p^{k/2}}\right) + \ln p^{\frac{p^{1/4}}{20\ln p}}$$
$$= \ln\left(\frac{8}{\ln 8p^{k/2}}\right) + \frac{p^{1/4}}{20}$$

which is obviously less than $p^{1/4}$ for all primes p and positive integers k.

For $k > \frac{p^{1/4}}{10\ln p}$, the proof follows by using the fact that the f-complexity can not exceed p, that is

$$p \geq \log_2 \frac{p^{k/2}}{\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right)}.$$

□

Corollary 2 *Let* $p > 41$ *be a prime and* k *be a positive integer. Then,*

$$\Gamma(\mathcal{F}_{\text{irred}}(k,p)) \geq \min\left\{p, \log_2 \frac{p^{k/2}}{\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right)}\right\}.$$

Moreover, this lower bound is greater than the lower bound given in Theorem A.

Proof We know that $|G_{p,k}| \leq 2p^{k/2}$ by [16, Lemma 2.5]. Hence, $B < 2$ and $A = \frac{2p^{k/2}(1-p^{-k/2})}{1+p^{-k/2}} < 2p^{(k/2)}$ where A and B are defined as in Theorem 1. By these inequalities and Lemma 1, we get

$$\begin{aligned}
\log_2\left(\frac{A}{W(2^B A)}\right) &\geq \log_2\left(\frac{A}{\ln(4A) - \ln\ln(4A) + \frac{e}{e-1}\frac{\ln\ln(4A)}{\ln(4A)}}\right) \\
&= \log_2 A - \log_2\left(\ln\left(\frac{4A}{\ln(4A)}\right) + \frac{e}{e-1}\frac{\ln\ln(4A)}{\ln(4A)}\right) \\
&\geq \log_2 A - \log_2\left(\ln\left(\frac{8p^{k/2}}{\ln(8p^{k/2})}\right) + \frac{e}{e-1}\frac{\ln\ln(8p^{k/2})}{\ln(8p^{k/2})}\right) \\
&\geq \log_2 p^{k/2} - \log_2\left(\ln\left(\frac{8p^{k/2}}{\ln 8p^{k/2}}\right)\right) \\
&\quad + \log_2\left(\frac{1-p^{-k/2}}{1+p^{-k/2}}\right) - \frac{e}{e-1}\frac{\ln\ln 8p^{k/2}}{\ln 8p^{k/2}} + 1.
\end{aligned} \tag{8}$$

where the last inequality follows from the definition of A and the properties of natural logarithm. Finally, let the error part $E(p, k)$ be defined as

$$E(p,k) := \log_2\left(\frac{1-p^{-k/2}}{1+p^{-k/2}}\right) - \frac{e}{e-1}\frac{\ln\ln 8p^{k/2}}{\ln 8p^{k/2}} + 1.$$

$E(p, k)$ increases when k increases and $E(p, 1) > 0$ for $p > 41$. Therefore, the first part of the corollary follows from Theorem 1. The second part is a direct consequence of Lemma 7. □

Remark 1 We compare the ceiling values of the bounds given in Theorem 1, Corollary 2 and Eq. (8) for $k = 10$ and $p < 8000$ in Fig. 2, where we just plot the gap between the bounds. We see that the bound given in Theorem 1 differs from the bound (8) in at most 1, and at most 2 from the bound given in Corollary 2.

6 Comparison

In this section, we compare the lower bounds given in Theorem 1 and Theorem A.

Firstly in Figs. 3, 4 and 5 we show that the bound given in Theorem 1 is better than the bound given in Theorem A. The red line shows the bound given in Theorem A and the blue line the bound given in Theorem 1. Both bounds are plotted with respect to primes $p < 8000$ for $k = 1, 2, \ldots, 10$, respectively. For $k = 1$ and $k = 2$, the bound given in [16] is negative for the primes in the range, on the other hand, the bound given in Theorem 1 is always positive. We note that the bound given in [16] turns into positive for $p \geq 2128240847$ and $k = 1$. For $3 \leq k \leq 10$, we see that both bounds are positive and the bound given in Theorem 1 is better than the bound given in Theorem A for all $p < 8000$. We conclude that our bound is better than the bound given in Theorem A for small values of k, but they are close to each other for

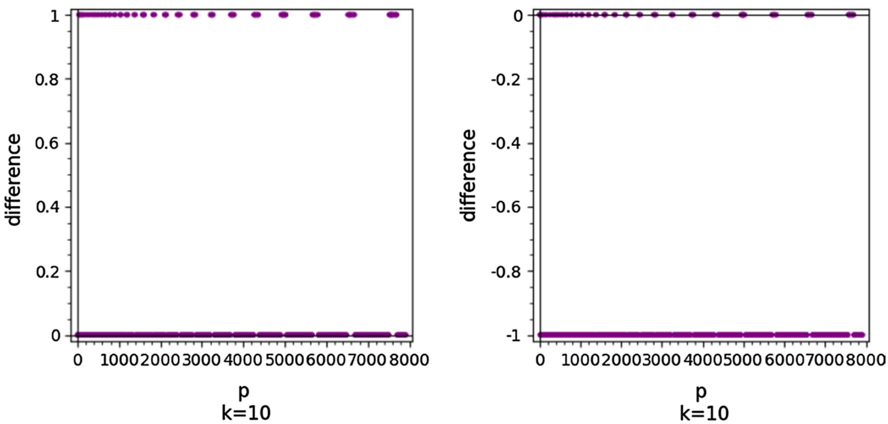

Fig. 2 Gap between the bounds given in Theorem 1 and Eq. (8), Corollary 2 and Eq. (8), respectively

large values of k. In Fig. 6, the lower bound on the f-complexity of the sequences given in Definition 7 is plotted in the range $k \in [1, 50]$ for $p = 10000019$ and $p = 2128240847$, respectively. Here, $p = 10000019$ is the first prime greater than 10^7 and $p = 2128240847$ is the first prime for which the bound given in Theorem A turns into positive for $k = 1$. In both cases, both lower bounds are close, but the one in Theorem 1 is better.

Secondly, we compare the two bounds in terms of time complexity. The bound given in Theorem 1 is based on the W function, so it can be argued that it would take more time. However, calculating the W function is not slow. In particular, Figs. 7 and 8 show the time difference between the bounds given in Theorem A and Theorem 1. We first measure the time (in seconds) it takes for calculating both bounds for all values of p and k that we have already examined in Figs. 3, 4 and 5. Then we plot the difference in seconds between both bounds in Figs. 7 and 8, which show that both bounds take time quite close to each other for all p and k.

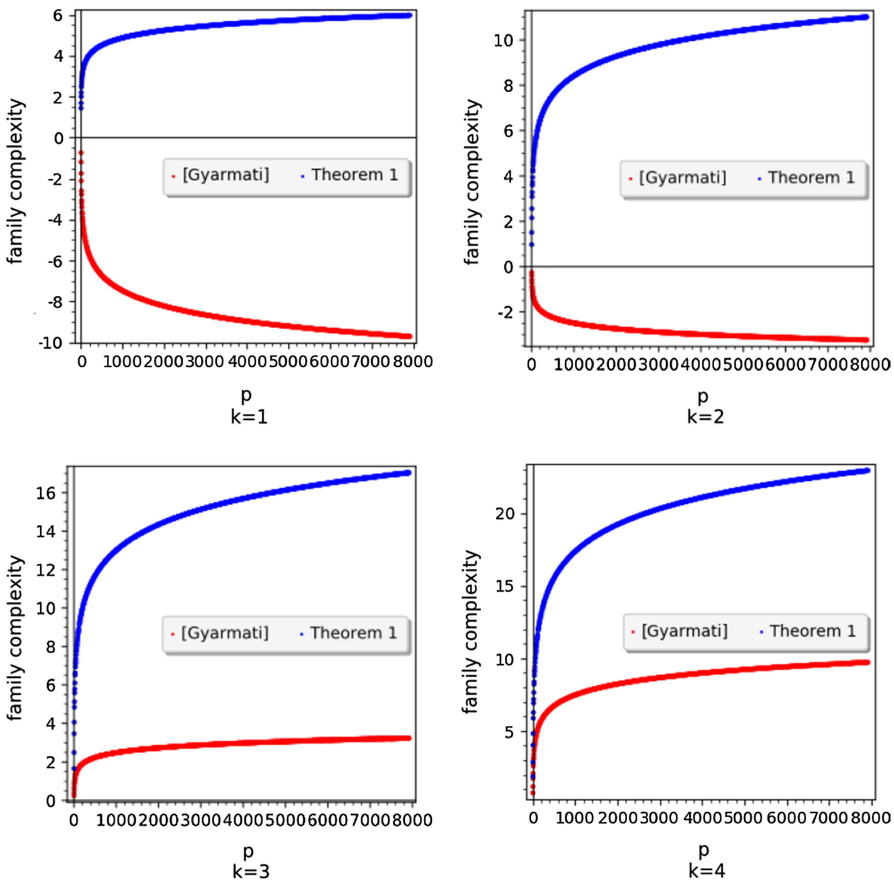

Fig. 3 Lower bound on the f-complexity of Legendre sequence with respect to p for $k = 1, 2, 3, 4$, respectively

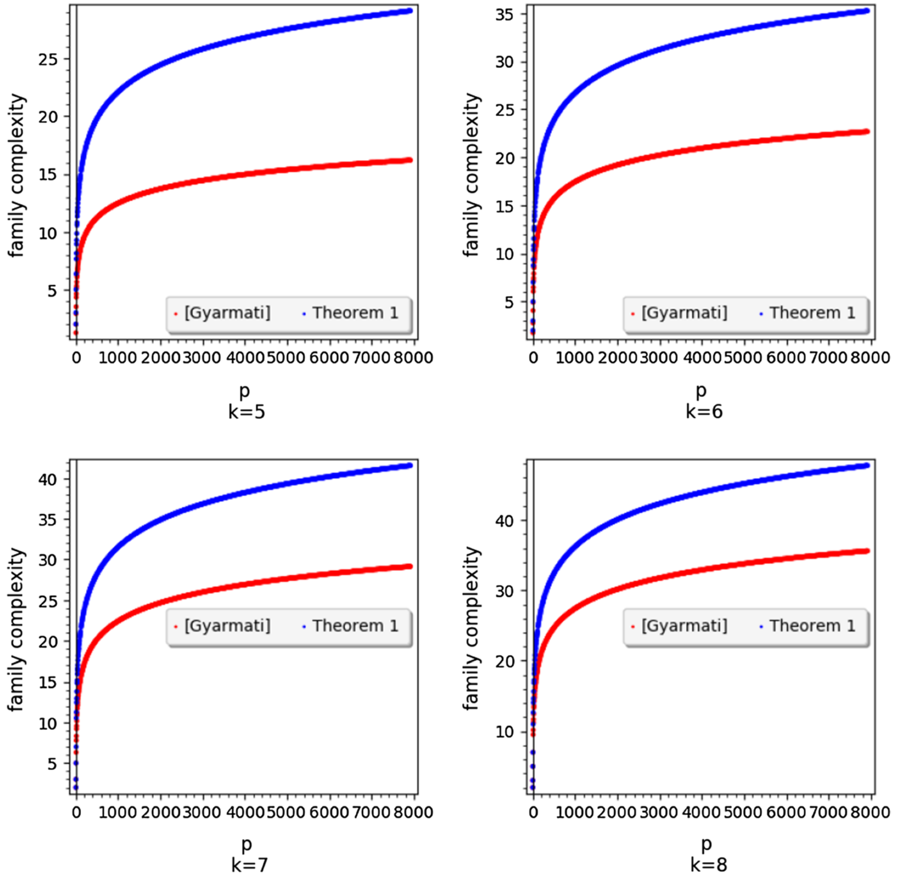

Fig. 4 Lower bound on the *f*-complexity of Legendre sequence with respect to p for $k = 5, 6, 7, 8$, respectively

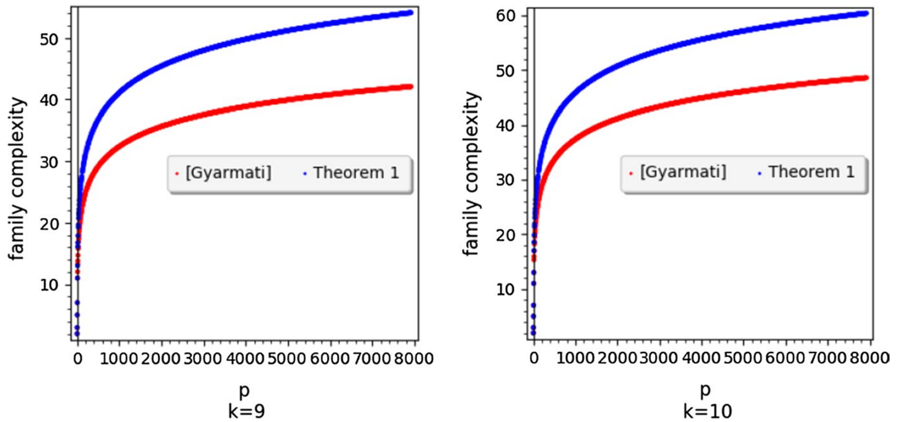

Fig. 5 Lower bound on the *f*-complexity of Legendre sequence with respect to p for $k = 9, 10$, respectively

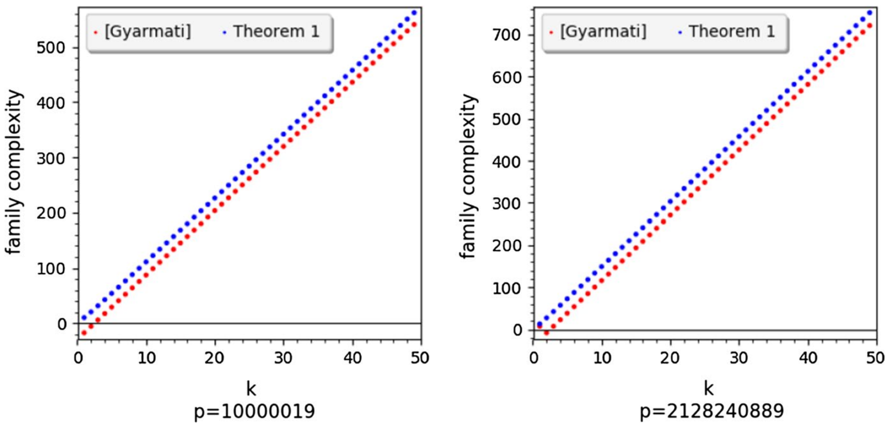

Fig. 6 Lower bound on the f-complexity of Legendre sequence with respect to k for $p = 10000019$ and $p = 2128240847$, respectively

For instance, in Fig. 7 for $k = 1$, the bound given in Theorem 1 takes more time, the difference is at most 0.005 seconds. On the other hand, for $k = 10$ the bound given in Theorem A takes more time and the difference is at most 0.01 s. Similarly, Fig. 8 shows that the time difference between both bounds is at most 0.06 s for primes $p = 10000019$, $p = 2128240847$ and $k \in \{1, 2, \ldots, 2000\}$. We conclude that the bound given in Theorem 1 can be calculated very fast for arbitrarily large prime powers and it only differs in a few milliseconds from calculation time of the bound depending only on p and k. We note that all figures in this paper were plotted using SageMath [35], and SageMath uses Eq. (2) for a numerical approximation on the W function.

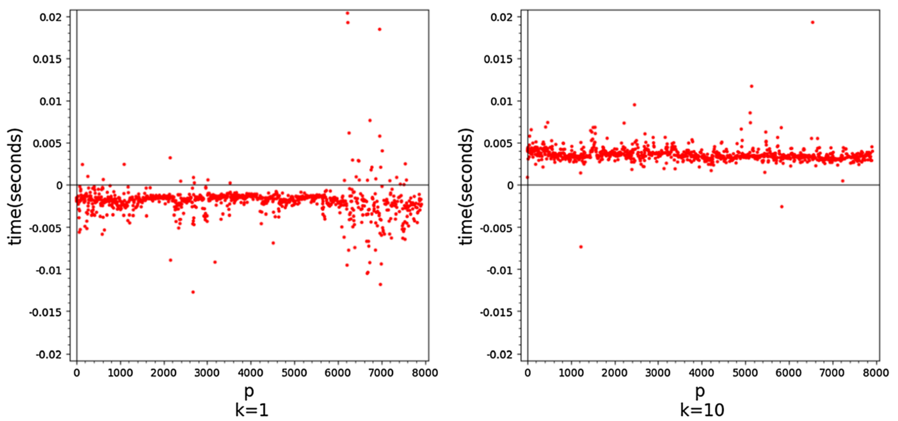

Fig. 7 Time difference between the bounds given in Theorem A and Theorem 1 with respect to p for $k = 1$ and $k = 10$, respectively

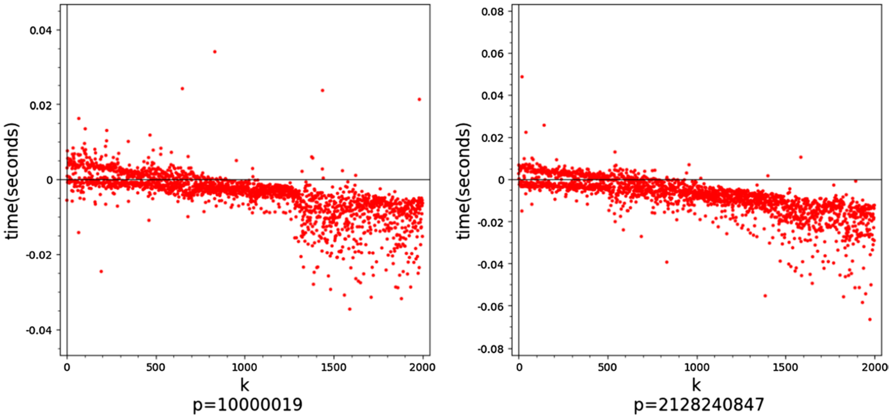

Fig. 8 Time difference between the bounds given in Theorem A and Theorem 1 with respect to k for $p = 10000019$ and $p = 2128240847$, respectively

7 Conclusion

In this paper we study the family of Legendre sequences generated by irreducible polynomials over a prime finite field and its f-complexity. The main aim of this work is to give a better bound on the f-complexity of this family. We present a new lower bound on the f-complexity depending on the Lambert W function. Then we approximate the W function so that we get another bound depending only on logarithmic functions. Also we prove that this bound strictly improves the previously known bounds. It would be a good future work to construct Legendre sequences by using the irreducibles of degree $k > k_0$ for some positive integer k_0 for getting a better family complexity bound, and to apply the bounds obtained in this paper to improve the bounds for other randomness measures.

Acknowledgements We would like to thank the anonymous reviewers for the detailed and carefully prepared suggestions, which improved not only the readability but also the quality of the paper. In particular, Corollary 2 is pointed out by the reviewers. The authors are supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Project No: 116R026.

References

1. Ahlswede, R., Khachatrian, L.H., Mauduit, C., Sárközy, A.: A complexity measure for families of binary sequences. Period. Math. Hungar. **46**(2), 107–118 (2003). https://doi.org/10.1023/A:1025962825241
2. Ahlswede, R., Mauduit, C., Sárközy, A.: Large families of pseudorandom sequences of k symbols and their complexity. I. In: General theory of information transfer and combinatorics, *Lecture Notes in Comput. Sci.*, vol. 4123, pp. 293–307. Springer, Berlin (2006). https://doi.org/10.1007/11889342_16
3. Ahlswede, R., Mauduit, C., Sárközy, A.: Large families of pseudorandom sequences of k symbols and their complexity. II. In: General theory of information transfer and combinatorics, *Lecture Notes*

in Comput. Sci., vol. 4123, pp. 308–325. Springer, Berlin (2006). https://doi.org/10.1007/11889342_17

4. Aly, H., Winterhof, A.: On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences. Des. Codes Cryptogr. **40**(3), 369–374 (2006). https://doi.org/10.1007/s10623-006-0023-5
5. Balasubramanian, R., Dartyge, C., Mosaki, E.: Sur la complexité de familles d'ensembles pseudo-aléatoires. Annales de l'Institut Fourier **64**(1), 267–296 (2014). https://doi.org/10.5802/aif.2847
6. Chebolu, S.K., Mináč, J.: Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. Math. Mag. **84**(5), 369–371 (2011). https://doi.org/10.4169/math.mag.84.5.369
7. Corless, R.M., Gonnet, G.H., Hare, D.E.G., Jeffrey, D.J., Knuth, D.E.: On the Lambert W function. Adv. Comput. Math. **5**(4), 329–359 (1996). https://doi.org/10.1007/BF02124750
8. Ding, C., Hesseseth, T., Shan, W.: On the linear complexity of Legendre sequences. IEEE Trans. Inf. Theory **44**(3), 1276–1278 (1998)
9. Dummit, D.S., Foote, R.M.: Abstr. Algebra, 3rd edn. Wiley, Hoboken, NJ (2004)
10. Euler, L.: De serie lambertina plurimisque eius insignibus proprietatibus. Acta Academiae Scientarum Imperialis Petropolitinae 1779, 1783, pp. 29–51 **6**, 350–369 (1921 (orig. date 1779))
11. Folláth, J.: Construction of pseudorandom binary sequences using additive characters over GF(2^k) II. Periodica Mathematica Hungarica **60**(2), 127–135 (2010). https://doi.org/10.1007/s10998-010-2127-y
12. Gauss, C.F.: Untersuchungen über höhere Arithmetik. Deutsch herausgegeben von H. Maser. Chelsea Publishing Co., New York (1965)
13. Golomb, S.W., Gong, G.: Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. Cambridge University Press, Cambridge (2005)
14. Goubin, L., Mauduit, C., Sárközy, A.: Construction of large families of pseudorandom binary sequences. J. Number Theory **106**(1), 56–69 (2004). https://doi.org/10.1016/j.jnt.2003.12.002
15. Gyarmati, K.: Concatenation of pseudorandom binary sequences. Period. Math. Hungar. **58**(1), 99–120 (2009). https://doi.org/10.1007/s10998-009-9099-x
16. Gyarmati, K.: On the complexity of a family of Legendre sequences with irreducible polynomials. Finite Fields Appl. **33**, 175–186 (2015). https://doi.org/10.1016/j.ffa.2014.11.004
17. Gyarmati, K., Mauduit, C., Sárközy, A.: Measures of pseudorandomness of families of binary lattices, II (a further construction). Publ. Math. Debrecen **80**(3–4), 479–502 (2012). https://doi.org/10.5486/PMD.2012.5197
18. Gyarmati, K., Mauduit, C., Sárközy, A.: The cross-correlation measure for families of binary sequences, p. 126–143. Cambridge University Press (2014). https://doi.org/10.1017/CBO9781139696456.009
19. Hofer, R., Mérai, L., Winterhof, A.: Measures of pseudorandomness: arithmetic autocorrelation and correlation measure. Number theory–Diophantine problems. Uniform distribution and applications, pp. 303–312. Springer, Cham (2017)
20. Hoffstein, J., Lieman, D.: The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher. In: Cryptography and Computational Number Theory, pp. 59–68. Birkhäuser Basel, Basel (2001)
21. Hoorfar, A., Hassani, M.: Inequalities on the lambert w function and hyperpower function. J. Inequal. Pure and Appl. Math **9**(2), 5–9 (2008)
22. Lidl, R., Niederreiter, H.: Finite Fields, *Encyclopedia of Mathematics and its Applications*, vol. 20, 2nd edn. Cambridge University Press, Cambridge (1997). With a foreword by P. M. Cohn
23. Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. Acta Arith. **82**(4), 365–377 (1997). https://doi.org/10.4064/aa-82-4-365-377
24. Mauduit, C., Sárközy, A.: Family complexity and VC-dimension. In: Information Theory, Combinatorics, and Search Theory, *Lecture Notes in Comput. Sci.*, vol. 7777, pp. 346–363. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36899-8_15
25. Meidl, W., Winterhof, A.: On the autocorrelation of cyclotomic generators. In: Finite fields and applications, *Lecture Notes in Comput. Sci.*, vol. 2948, pp. 1–11. Springer, Berlin (2004). https://doi.org/10.1007/978-3-540-24633-6_1
26. Menezes, A.J., Katz, J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
27. Mullen, G.L., Panario, D. (eds.): Handbook of finite fields. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL (2013). https://doi.org/10.1201/b15006

28. Niederreiter, H.: Random number generation and quasi-Monte Carlo methods, vol. 63. Siam, Philadelphia (1992)
29. Niederreiter, H., Winterhof, A.: Applied Number Theory. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22321-6
30. Paley, R.E.: On orthogonal matrices. Journal of Mathematics and Physics **12**(1–4), 311–320 (1933)
31. Rivat, J., Sárközy, A.: On Pseudorandom Sequences and Their Application. Springer, Berlin (2006)
32. Sárközy, A.: A finite pseudorandom binary sequence. Studia Sci. Math. Hungar. **38**, 377–384 (2001). https://doi.org/10.1556/SScMath.38.2001.1-4.28
33. Shparlinski, I.: Cryptographic applications of analytic number theory, *Progress in Computer Science and Applied Logic*, vol. 22. Birkhäuser Verlag, Basel (2003). https://doi.org/10.1007/978-3-0348-8037-4. Complexity lower bounds and pseudorandomness
34. Sárközy, A.: On pseudorandomness of families of binary sequences. Discrete Appl. Math. **216**, 670–676 (2017). https://doi.org/10.1016/j.dam.2015.07.031
35. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.0) (2020). https://www.sagemath.org
36. Topuzoğlu, A., Winterhof, A.: Pseudorandom sequences. In: Topics in geometry, coding theory and cryptography, pp. 135–166. Springer, Berlin (2006)
37. Turyn, R.J.: The linear generation of the Legendre sequence. SIAM J. Appl. Math. **12**(1), 115 (1964)
38. Valluri, S.R., Jeffrey, D.J., Corless, R.M.: Some applications of the lambert W function to physics. Canad. J. Phys. **78**(9), 823–831 (2000). https://doi.org/10.1139/p00-065
39. Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris (1948)
40. Winterhof, A., Yayla, O.: Family complexity and cross-correlation measure for families of binary sequences. Ramanujan J. **39**(3), 639–645 (2016). https://doi.org/10.1007/s11139-014-9649-5