A better lower bound on the family complexity of binary Legendre sequence

Yağmur Çağiroğlu and Oğuz Yayla
Department of Mathematics, Hacettepe University
Beytepe, 06800, Ankara, Turkey
yagmur.cakiroglu@hacettepe.edu.tr
oguz.yayla@hacettepe.edu.tr
December 24, 2018

Abstract

In this paper we study a family of binary Legendre sequences and its family complexity. Family complexity is a pseudorandomness measure introduced by Ahlswede et. al in 2003. A lower bound on the family complexity of a family based on the Legendre symbol of polynomials over a finite field was given by Gyarmati in 2015. In this article we improve the bound given by Gyarmati on family complexity of binary Legendre sequences. The bound depends on the Lambert W function and the number of elements in a finite field belonging to its proper subfield. Moreover, we present a fast method for calculating the bound.

Keywords: pseudorandomness, binary sequences, family complexity, family of binary Legendre sequences, Lambert W Function, polynomials over finite field

1 Introduction

Finite pseudorandom binary sequences are used in many areas such as telecommunication, simulation, spectroscopy and in several areas of cryptography, see [14, 16, 20]. Especially they are used as the key in stream ciphers. Hence, it is important whether a given binary sequence is pseudorandom or not. In other words, these sequences have to be unpredictable and must have strong randomness measures. In 1997 Mauduit and Sárközy introduced measures (normality, well-distribution and correlation measure) of pseudorandomness [17]. And they tested the Legendre sequence for pseudorandomness. Then many other measures and new pseudorandom sequences are introduced, see [19, Chapter 5] and [22] for details.

In case of a family of sequences in used in an application, for instance 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 large family size, large family complexity and low crosscorrelation. In 2003, Ahlswede, Khachatrian, Mauduit and Sárközy [1] estimated family complexity of a large family of Legendre sequences introduced by Goubin, Mauduit and Sárközy [7], which was improved...
by Gyarmati [9] in 2009. In 2006 Ahlswede, Khachatrian, Mauduit and Sarkozy studied families of pseudorandom sequences on $k$ symbols and their family complexity [2, 3]. In 2013 Mauduit and Sarkozy studied family complexity measure of sequences of $k$ symbols and they also gave the connection between family complexity and VC-dimension [18]. In 2013 Mauduit and Sarkozy studied family complexity measure of sequences of $k$ symbols and they also gave the connection between family complexity and VC-dimension [18]. In 2016 Yayla and Winterhof gave a relation between family complexity and cross correlation measure [23]. Moreover the complexity measure for different families has been studied in some papers [4, 6, 11, 21]. Recently Gyarmati [10] presented a bound for family complexity of binary Legendre sequences in 2015. In this paper we improve the bound given in [10].

We begin with the definition of well known Legendre sequence [7, 17].

**Construction 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 has no multiple zeros in $\mathbb{F}_p$, then define the binary sequence $E_p(f) = (e_1, \ldots, e_p)$ by

$$e_n = \begin{cases} \frac{f(n)}{p} & \text{for } (f(n), p) = 1 \\ 1 & \text{for } p | f(n) \end{cases}$$

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

Hoffstein and Lieman [13] presented the use of the polynomials $f$ given in Construction (1) but they did not give a proof for its pseudorandom properties. Goubin, Mauduit and Sarkozy [7] proved that the sequences obtained in this way have strong pseudorandom properties.

We now give the definition of the $f$-complexity of a family $F$, which was first defined by Ahlswede et. al. [1] in 2003.

**Definition 1.** The family complexity (or briefly $f$-complexity) $C(F)$ of a family $F$ 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 $E_N = \{e_1, e_2, \ldots, e_N\} \in F$ with

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

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

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

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

We set the family of Legendre sequences generated by irreducible polynomials of degree $k$ over a prime field $\mathbb{F}_p$ by $F_{\text{irred}}(k, p)$:

$$F_{\text{irred}}(k, p) := \{E_p(f) : f \in \mathbb{F}_p \text{ monic irreducible polynomial with degree } k\}$$

This family has been studied for different measures (crosscorrelation etc.) in several paper [7, 8, 12].

Gyarmati [10] recently proved a lower bound on the $f$-complexity of the family $F_{\text{irred}}(k, p)$, which says that the $f$-complexity is at least of order $\frac{p^{1/4}}{20 \log^2 p}$.

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

$$\Gamma(F_{\text{irred}}(k, p)) \geq \min\{p, \frac{k-c}{2 \log p} \log p\}.$$  

2
In this paper we improve the lower bound given in Theorem A and prove the following theorem.

Let $G_{p,k}$ denote the set of elements of a finite field $\mathbb{F}_{p^k}$ belonging to its some proper subfield, and $W$ denote the Lambert function (see Definition 4).

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

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

Then

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

Since $\mathcal{F}(K,p) \supset \mathcal{F}_{\text{irred}}(K,p)$ thus we can give the following corollary.

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

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

The paper is organized as follows. In Section 2, we present some preliminary results and a fast method for calculating $|G_{p,k}|$. Then we present some auxiliary lemmas and the proof of Theorem 1 in Section 3. Finally we compare Theorem 1 and Theorem A in Section 4.

## 2 Preliminaries

Let $\mathbb{F}_{q^n}$ denote the finite field having $q^n$ elements and define $G_{q,n}$ as follows.

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

One can calculate the number of elements in $G_{q,n}$ for arbitrary $q,n$ by counting. But this method would be very slow. Thus, we need a formula for $|G_{q,n}|$, which we give in the following lemma.

**Lemma 1.** Let $n \in \mathbb{N}$ and $q$ be a prime power. Let $n$ have the prime factorization $n = \sum_i p_i^{k_i}$. Then

$$|G_{q,n}| = \sum_{p_i \mid n} q^{n_{p_i}} - \sum_{p_i, p_j \mid n} q^{\gcd\left(\frac{n_{p_i}}{p_i}, \frac{n_{p_j}}{p_j}\right)} + \sum_{p_i, p_j, p_k \mid n} q^{\gcd\left(\frac{n_{p_i}}{p_i}, \frac{n_{p_j}}{p_j}, \frac{n_{p_k}}{p_k}\right)} \ldots$$

**Proof.** From definition of $G_{q,n}$ we can write $G_{q,n} = \bigcup_{p_i \mid n} \mathbb{F}_{q^{p_i}}$. Then the proof follows by well known inclusion-exclusion rule from set theory. 

Note that the formula of $|G_{q,n}|$ depends on all subsets of factors of $n$. We present a fast Python code for calculating $|G_{q,n}|$ in Algorithm 1, and give an example below.

**Example 1.** Consider $\mathbb{F}_{q^n}$ for $n = 105$. Then we have $p_i = 3, 5, 7$ and by Lemma 1

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

Similarly, consider $\mathbb{F}_{q^n}$ for $n = 90$. We have $p_i = 2, 3, 5$ and

$$|G_{q,n}| = q^{45} + q^{30} + q^{18} - q^{15} - q^9 - q^6 + q^3.$$
Algorithm 1 A fast method to calculate $|G_{(q,n)}|$

Require: prime factors of $n$

Ensure: $|G_{q,n}| = \sum_{p_i \mid n} q^{n/p_i} - \sum_{p_i \neq p_j \mid n} q^{\gcd(n/p_i, n/p_j)} + \sum_{p_i \neq p_j \neq p_k \mid n} q^{\gcd(n/p_i, n/p_j, n/p_k)}$ ...

sum=0
D=primedivisors(n)
Dsubsets=list(subsets(D))
delete Dsubsets[0]
for s in Dsubsets:
    power=n
    for prime in s:
        power=gcd(power,n/prime)
    sum += ((-1)^length(s)-1)*q^power
return sum

Now we give the definition of a norm an element in a finite field.

Definition 2. For $\alpha \in \mathbb{F}_{q^n}$ the norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ of $\alpha$ over $\mathbb{F}_q$ is defined by

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

Next the definition of trace and norm of a polynomial over a finite field is given below.

Definition 3. Assume that

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

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

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

And let define

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

Lemma 2. \cite{15} Exercise 5.64] Let $i_1, \ldots, i_j$ be distinct elements of $\mathbb{F}_p^k$, $p$ odd, 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

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

where $\gamma$ is the quadratic character of $\mathbb{F}_p^k$. Then,

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

Definition 4. (Lambert W Function) 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, Lambert W Function is known as the inverse function of $f(z) = ze^z$. Thus the equation $y = ze^z$ is by definition solved by $z = W(y)$. And, the equation $y = z \log z$ is solved by $z = \frac{y}{W(y)}$. The Lambert W Function has many applications in pure and applied mathematics, see [5] for details about applications of Lambert W Function. The new bound we obtain for $f$-complexity given in this paper is related to this function.

3 Main Method

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

Lemma 3. Let $A, B \in \mathbb{R}$. If $Bx + x \log_2 x - A = 0$, then $x = \frac{A}{W(A2^B)}$.

Proof. We have

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

or equivalently,

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

Then we get

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

and

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

Thus by Definition 4 we have

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

that is

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

Lemma 4. Let $p$ be an odd prime and $k$ be a positive integer. Let $|G_{p,k}|$ be defined as in Lemma 1. 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 $\epsilon_1, \ldots, \epsilon_j \in \{-1, +1\}$ and $N(\epsilon_1, \ldots, \epsilon_j)$ be defined as in Lemma 2. Then

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

Proof. Assume that $|G_{p,k}| \geq N(\epsilon_1, \ldots, \epsilon_j)$. Then by Lemma 2

$$|G_{p,k}| \geq \frac{p^k}{2^j} - \frac{p^{k/2}}{2^j} \left( \frac{1}{2^j} + \frac{(j - 2)}{2} \right) - j.$$
Let $f$ be a polynomial, and from the definition of $N$, we know that

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

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

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

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

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

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

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

By definition of $A$ and $B$, we have

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

Hence, by Lemma 3, we obtain that

$$2^j \geq \frac{A}{W(2B^2 A)}$$

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

which is a contradiction.

\[\square\]

**Proof of Theorem 1.** We need to show the existence of $g \in \mathbb{F}_p[x]$ irreducible polynomial of degree $k$ such that

$$\left(\frac{g(i_s)}{p}\right) = \epsilon_s$$

for any tuple $(\epsilon_1, \epsilon_2, \ldots, \epsilon_j) \in \{-1, +1\}^j$ and for any integer $j < \log_2\left(\frac{A}{W(2B^2 A)}\right)$. By Lemma 4, we know that

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

From 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

$$\gamma(\alpha + i_s) = \epsilon_s$$

for $s = 1, \ldots, j$.

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

$$\gamma(\alpha) = \left(\frac{N_{F_{q^n}/F_q}(\alpha)}{p}\right).$$

We know that if $f \in F_{q^n}[x]$ then for $\alpha \in \mathbb{F}_q$ we have

$$N_{F_{q^n}/F_q}(f(\alpha)) = N_{F_{q^n}/F_q}(f)(\alpha).$$

Finally, using these and (1) we get

$$\epsilon_s = \gamma(\alpha + i_s) = \gamma(f(i_s)) = \left(\frac{N_{F_{q^n}/F_q}(f(i_s))}{p}\right) = \left(\frac{N_{F_{q^n}/F_q}(f)(i_s)}{p}\right) = \left(\frac{g(i_s)}{p}\right)$$

for $s = 1, \ldots, j$,

as desired. 

\[\square\]
Figure 1: Lower bound on family complexity of Legendre sequence with respect to $p$ for fixed $k = 1$ and $k = 10$ respectively.

Figure 2: Lower bound on family complexity of Legendre sequence with respect to $k$ for fixed $p = 10000019$ and $p = 2128240847$ respectively.

4 Comparison

Finally, we compare the bound given in Theorem 1 on family complexity of Construction 1 and the bound given in [10]. It is seen in Figures 1 and 2 that the lower bound given in Theorem 1 is better than Gyarmati’s bound [10]. Here the red lines show the bound in [10] (see also Theorem A in this paper) and the blue lines show the bound given Theorem 1 in this paper.

In Figure 1, both bounds on family complexity of Construction 1 is plotted with respect to primes $p < 8000$ for fixed $k = 1$ and $k = 10$ respectively. For $k = 1$, it is seen that Gyarmati’s bound is negative, on the other hand, the bound in Theorem 1 is always positive. We note that Gyarmati’s bound turns into positive for $p \geq 2128240847$. For $k = 10$, it is seen that both lower
bounds are positive and the lower bound given in Theorem 1 is better than Gyarmati’s bound for all \( p < 8000 \).

Next, in Figure 2 the lower bound on family complexity of Construction 1 is plotted in range \( k \in [1, 50] \) for fixed \( p = 10000019 \) and \( p = 2128240847 \) respectively. Here, \( p = 10000019 \) is the first prime greater than \( 10^7 \) and \( p = 2128240847 \) is the first prime Gyarmati’s bound turns into positive for \( k = 1 \). In both cases, lower bounds are near to each other, but the lower bound in Theorem 1 is better.

**Acknowledgement**

The authors are supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Project No: 116R026.

**References**

[1] Rudolf Ahlswede, Levon H. Khachatrian, Christian Mauduit, and András Sárközy. A complexity measure for families of binary sequences. *Period. Math. Hungar.*, 46(2):107–118, 2003.

[2] Rudolf Ahlswede, Christian Mauduit, and András Sárközy. Large families of pseudorandom sequences of \( k \) symbols and their complexity. I. In *General theory of information transfer and combinatorics*, volume 4123 of *Lecture Notes in Comput. Sci.*, pages 293–307. Springer, Berlin, 2006.

[3] Rudolf Ahlswede, Christian Mauduit, and András Sárközy. Large families of pseudorandom sequences of \( k \) symbols and their complexity. II. In *General theory of information transfer and combinatorics*, volume 4123 of *Lecture Notes in Comput. Sci.*, pages 308–325. Springer, Berlin, 2006.

[4] Ramachandran Balasubramanian, Cécile Dartyge, and Élie Mosaki. Sur la complexité de familles d’ensembles pseudo-aléatoires. *Annales de l’Institut Fourier*, 64(1):267–296, 2014.

[5] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert \( W \) function. *Adv. Comput. Math.*, 5(4):329–359, 1996.

[6] János Folláth. Construction of pseudorandom binary sequences using additive characters over \( GF(2^k) \) II. *Periodica Mathematica Hungarica*, 60(2):127–135, 2010.

[7] Louis Goubin, Christian Mauduit, and András Sárközy. Construction of large families of pseudorandom binary sequences. *J. Number Theory*, 106(1):56–69, 2004.

[8] Katalin Gyarmati. Concatenation of pseudorandom binary sequences. *Period. Math. Hungar.*, 58(1):99–120, 2009.

[9] Katalin Gyarmati. On the complexity of a family related to the Legendre symbol. *Period. Math. Hungar.*, 58(2):209–215, 2009.

[10] Katalin Gyarmati. On the complexity of a family of Legendre sequences with irreducible polynomials. *Finite Fields Appl.*, 33:175–186, 2015.
[11] Katalin Gyarmati, Christian Mauduit, and András Sárközy. Measures of pseudorandomness of families of binary lattices, II (a further construction). Publ. Math. Debrecen, 80(3-4):479–502, 2012.

[12] Katalin Gyarmati, Christian Mauduit, and András Sárközy. The cross-correlation measure for families of binary sequences.

[13] Jeffrey Hoffstein and Daniel Lieman. The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher. In Cryptography and Computational Number Theory, pages 59–68, Basel, 2001. Birkhäuser Basel.

[14] Pierre L’Ecuyer. Testing random number generators. In Winter Simulation Conference, pages 305–313, 1992.

[15] Rudolf Lidl and Harald Niederreiter. Finite Fields, volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[16] George Marsaglia. The Marsaglia random number CDROM including the Diehard battery of tests of randomness. http://www.stat.fsu.edu/pub/diehard/, 2008.

[17] Christian Mauduit and András Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. Acta Arith., 82(4):365–377, 1997.

[18] Christian Mauduit and András Sárközy. Family complexity and VC-dimension. In Information Theory, Combinatorics, and Search Theory, volume 7777 of Lecture Notes in Comput. Sci., pages 346–363. Springer, Heidelberg, 2013.

[19] Harald Niederreiter and Arne Winterhof. Applied Number Theory. Springer, Cham, 2015.

[20] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2001.

[21] András Sárközy. On pseudorandomness of families of binary sequences. Discrete Applied Mathematics, 216:670–676, 2017.

[22] Alev Topuzoğlu and Arne Winterhof. Pseudorandom sequences. In Topics in Geometry, Coding Theory and Cryptography, pages 135–166. Springer, 2006.

[23] Arne Winterhof and Oğuz Yayla. Family complexity and cross-correlation measure for families of binary sequences. Ramanujan J., 39(3):639–645, 2016.