EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 13, No. 1, 2020, 108-112
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

Proof of Golomb's conjecture in $\mathbb{F}_q$ with $\mathit{\Gamma}_{\varpi}$-pseudorandom sequences

Yonghong Liu

School of Automation, Wuhan University of Technology, 205 Luoshi Road, Wuhan, China

---

Abstract. This article offers a short proof of Golomb's conjecture, and then our results show that the sequences are pseudorandom in $\mathbb{F}_2$.

2020 Mathematics Subject Classifications: 11A41, 11A07, 12E20, 11B50

Key Words and Phrases: Primes, Primitive roots, Finite fields, Sequences, Golomb's conjecture

---

1. Introduction

Question 10208b (1992) of the American Mathematical Monthly asked: does there exist an increasing sequence $\{a_k\}$ of positive integers and a constant $B > 0$ having the property that $\{a_k + n\}$ contains no more than B primes for every integer n? If it turns out that a positive answer to this question became known as Golomb's conjecture [1].

Let $\mathbb{F}_q$ denote the finite field of order q, where $q = p^n$, and p is a prime, if n=1, Golomb's conjecture equivalent to:

Conjecture 1. Let α and β be two primitive roots of $f(x)(\text{mod } p)$ in $\mathbb{F}_q$, then

$$f(\alpha) + f(\beta) \equiv 1 \pmod p. \tag{1}$$

Moreno and Sotero [2] proved that Golombs conjecture is true for all $q < 2^{60}$. Golomb [3] pointed out that the conjecture associated with sequences and prime numbers. Elsholtz [4] proved in 2017 that Golomb's conjecture was false. Elsholtz gave an example to explain the Fermat numbers contains at least $B + 1$ primes, but his research has shown that we cannot conclude that there is any fixed n such that the sequence $\{2^{2^i} + n\}$ contains innitely many primes. Certainly! the conjecture is true for the special case.

Because of pseudorandom sequences unique characteristic they have been widely used in many fields. In this paper we prove that the Golombs conjecture in $\mathbb{F}_q$, and we show that a new pseudorandom sequence (denote $\mathit{\Gamma}_{\varpi}$) in $\mathbb{F}_2$ is existent by Golomb conjecture and additive groups.

DOI: https://doi.org/10.29020/nybg.ejpam.v13i1.3594

Email address: `hylinin@whut.edu.cn` (Y. Liu)

2. Proof of the Golomb conjecture

Theorem 1. *If*

$$\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n}=p, \tag{2}$$

is prime, then ϖ is prime.

Proof. If $\varpi=1$, then p is not prime. Let ϖ be composite and let m be divisor. Since $\varpi=km$ satisfies $1<k<\varpi$, and that

$$\sum_{n=1}^{k}(-1)^{n+1}2^{k-n}\Bigg|\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n}. \tag{3}$$

We have

$$1<\sum_{n=1}^{k}(-1)^{n+1}2^{k-n}<\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n}, \tag{4}$$

and so p is not prime, a contradiction. □

For our next discussion, $\mathit{\Gamma}_\varpi$ numbers are defined by

$$\mathit{\Gamma}_\varpi=\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n}, \tag{5}$$

so that

$$\begin{cases}\mathit{\Gamma}_3\ =3, & \mathit{\Gamma}_5\ =11,\\ \mathit{\Gamma}_7\ =43, & \mathit{\Gamma}_{11}=683,\\ \mathit{\Gamma}_{13}=2731, & \mathit{\Gamma}_{17}=43691,\\ \mathit{\Gamma}_{19}=174763, & \mathit{\Gamma}_{23}=2796203.\end{cases} \tag{6}$$

As an application of the $\mathit{\Gamma}_\varpi$ numbers, we give the following theorem.

Theorem 2. 3 *is a primitive root of $\mathit{\Gamma}_7$ (or $\mathit{\Gamma}_{11}$).*

Theorem 3. *Golomb's conjecture* (Conjecture 1) *on $\mathbb{F}_{\mathit{\Gamma}_{17}}$, which is true.*

Proof. We can now find tow primitive roots of $f(x)$. By Theorem 1. Since $\mathit{\Gamma}_{17}$ prime is 43691, *and we have*

$$f(\alpha)=3^{\varpi-2}\quad\text{and}\quad f(\beta)=2\cdot3^{\varpi-2}. \tag{7}$$

It follows that

$$f(\alpha) = 3^{15} \pmod{43691} \quad \text{and} \quad f(\beta) = 2 \cdot 3^{15} \pmod{43691}. \tag{8}$$

The same result is primitive root of modulus 34961. Hence

$$3^{15} + 2 \cdot 3^{15} = 3^{16} \equiv (-1)^{16} \equiv 1 \pmod{43691}, \tag{9}$$

as desired. □

Theorem 4. *Golomb's conjecture* (Conjecture 1) *on* $\mathbb{F}_{\Gamma_7}$ *(or* $\mathbb{F}_{\Gamma_{11}}$*), which is true.*

Combining the Theorem 2.3 and Theorem 2.4, we obtain the following corollary.

Corollary 1. *If* Γ_ϖ *is prime and*

$$f(\alpha) = 3^{\varpi-2}, \quad f(\beta) = 2 \cdot 3^{\varpi-2} \tag{10}$$

is primitive root of $f(x) \pmod{\Gamma_\varpi}$*, then*

$$f(\alpha) + f(\beta) \equiv 1 \pmod{\Gamma_\varpi}. \tag{11}$$

3. Γ_ϖ-pseudorandom sequences

Definition 1. Let ϖ is prime and let μ is primitive root of modulus Γ_ϖ such that Eq. (5). We say that Γ_ϖ is a period of pseudorandom sequence if

$$X = [a_0 \ a_1 \ a_2 \ \cdots \ a_{p-2} \ a_{p-1}] \quad (a_i \in \mathbb{F}_q) \tag{12}$$

with the following properties:

$$a_0 = +1. \tag{13}$$

$$a_i = (-1)^t = \begin{cases} +1 & \text{if } t \text{ is even} \\ -1 & \text{if } t \text{ is odd,} \end{cases} \tag{14}$$

for

$$i \equiv \mu^t \pmod{\Gamma_\varpi}, \tag{15}$$

where $1 < i < p{-}1$.

Definition 2. Let η be an additive group of $\mathbb{F}_2$ (for $+1$ and -1). Then multiplicative group is isomorphic which constitutes by these two integers, and we have

$$\eta(0) = 1, \quad \eta(1) = -1. \tag{16}$$

Our new result is the following theorem.

Theorem 5. *Suppose that the pseudorandom periodic sequence $\mathit{\Gamma}_{\varpi}$ acts transitively on the $\mathbb{F}_2$. Then*

$$C_x(j) = \begin{cases} \mathit{\Gamma}_{\varpi} & \text{if } j \equiv 0 \pmod{\mathit{\Gamma}_{\varpi}} \\ -1 & \text{if } j \not\equiv 0 \pmod{\mathit{\Gamma}_{\varpi}}. \end{cases} \tag{17}$$

Proof. By Definition 1. First, we have

$$C_x(0) = \mathit{\Gamma}_{\varpi}. \tag{18}$$

Let $j \not\equiv 0 \pmod{\mathit{\Gamma}_{\varpi}}$. We define X by

$$X = (x_0,\ x_1,\ \cdots). \tag{19}$$

Next let $f(y)$ be a minimal polynomial of X with $X \in G(f)$. Now If $f(x)$ is nth order primitive polynomial

$$f(y) = c_n y^n + c_{n-1} y^{n-1} + \cdots + c_1 y + c_0 \quad (c_0 c_n \neq 0). \tag{20}$$

Then X satisfies the homogeneous linear difference equation of nth order

$$\sum_{i=0}^{n} c_i x_{k-i} = 0 \quad (k \geq n). \tag{21}$$

We have

$$c_0 = 1 = c_n. \tag{22}$$

To find that the linear recursive relation for Eq.(21) so that X moves that S steps to the left, we have

$$T^s(X) = (x_s,\ x_{s+1},\ x_{s+2},\ \cdots) \in G(f), \tag{23}$$

and

$$X + T^s(X) = (x_0 + x_s,\ x_1 + x_{s+1},\ x_2 + x_{s+2},\ \cdots) \in G(f). \tag{24}$$

If

$$s \not\equiv 0 \pmod{\mathit{\Gamma}_{\varpi}}, \tag{25}$$

since period X is $\mathit{\Gamma}_{\varpi}$, then

$$X + T^s(X) \neq 0. \tag{26}$$

But nonzero sequence is $\mathit{\Gamma}_{\varpi}$ in $G(f)$, so 1 there are

$$\sum_{n=1}^{\varpi} (-1)^{n+1} 2^{\varpi-n-1}$$

times in a period in $X + T^s(X)$ *and* 0 *there are*

$$\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n-1}-1$$

times in a period in $X + T^s(X)$.

Finally, by Definition 2, we have

$$\begin{aligned} C_x(j) &= \sum_{i=0}^{c_x(0)} \eta(x_i)\eta(x_{i+s}) \\ &= \sum_{i=0}^{c_x(0)} \eta(x_i + x_{i+s}) \\ &= \sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n-1}\cdot(-1) + \Big(\sum_{n=1}^{\varpi}(-1)^{n+1}2^{\varpi-n-1}-1\Big)\cdot 1 \\ &= -1, \end{aligned} \tag{27}$$

as desired. □

References

[1] *S. W. Golomb, Infinite sequences with finite cross-correlation, In SETA (2010), LNCS, Springer, Berlin,* ***6338****(2010), 430-441.*

[2] *O. Moreno & J. Sotero, Computational approach to conjecture A of Golomb,* Congressus Numerantium, **70**(1990), 7-16.

[3] S. W. Golomb, "Conjectures involving sequences and prime numbers. Sequences and their applications", In SETA (2014), LNCS, Springer, Cham, Switzerland, **8865**(2014), 263-266.

[4] C. Elsholtz, *Golombs conjecture on prime gaps,* Amer. Math. Monthly, **124**(2017), 365-368. https//doi:10.4169/amer.math.monthly.124.4.365