The existence of primitive pair over finite fields

Jyotsna Sharma

(Joint work with S. Laishram and R. Sarma)

32 émes Journées Arithmétiques 2023, Nancy(France)

Department of Mathematics
Indian Institute of Technology Delhi, India

July 4, 2023

Notations

- $\mathbb{F}^{\times} := \mathbb{F} - \{0\}$ for a field $\mathbb{F}$.
- ϕ is the Euler's totient function.
- μ is the Mobius function.
- $\hat{G}$ is the group of characters of the group G.
- $\omega(m)$ is number of distinct prime divisors of m.
- $W(m) = 2^{\omega(m)}$ is number of square free divisors of m.

Basic Definitions

Character

Let G be a finite abelian group with identity e. A character χ of G is a homomorphism from G into $\mathbb{C}^\times$.

$$\chi : G \longrightarrow \mathbb{C}^\times.$$

that is,

- $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in G$.
- Among the characters of G, the trivial character of G is χ_1 with $\chi_1(a) = 1$, for all $a \in G$.
- The order of a character χ is the least positive integer d such that $\chi^d = \chi_1$.
- $|\widehat{G}| = |G|$.

Some basic results

Theorem

If χ is a non-trivial character of a finite abelian group G, then

$$\sum_{a \in G} \chi(a) = 0.$$

Some basic results

Theorem

If χ is a non-trivial character of a finite abelian group G, then

$$\sum_{a \in G} \chi(a) = 0.$$

Theorem

If $a \in G$ is a non trivial element and $\widehat{G}$ is the group of all characters of group G, then

$$\sum_{\chi \in \widehat{G}} \chi(a) = 0.$$

Definitions

Primitive element

An element is said to be a primitive element over $\mathbb{F}_q$ if it generates $\mathbb{F}_q^{\times}$.

- For $f \in \mathbb{F}_q(x)$, we call $(\alpha, f(\alpha))$ a primitive pair in $\mathbb{F}_q$ if both α and $f(\alpha)$ are primitive elements of $\mathbb{F}_q$.

Definitions

Primitive element

An element is said to be a primitive element over $\mathbb{F}_q$ if it generates $\mathbb{F}_q{}^{\times}$.

- For $f \in \mathbb{F}_q(x)$, we call $(\alpha, f(\alpha))$ a primitive pair in $\mathbb{F}_q$ if both α and $f(\alpha)$ are primitive elements of $\mathbb{F}_q$.

u - free element

For u a divisor of $q-1$, an element $\alpha \in \mathbb{F}_q$ is called u - free, if $\alpha = \beta^d$, where $\beta \in \mathbb{F}_q$ and $d|u$, $\implies d = 1$.

- Note that an element α is primitive iff it is $(q-1)$ - free.

The following assertion is a particular case of [10, Lemma 10], given by Shuqin et. al. (2004).

Lemma

Let u be a divisor of $q-1$ and let $\alpha \in \mathbb{F}_q^\times$. Then

$$\sum_{l|u} \frac{\mu(l)}{\varphi(l)} \sum_{\chi_l} \chi_l(\alpha) = \begin{cases} \frac{u}{\varphi(u)} & \text{if } \alpha \text{ is } u\text{-free}, \\ 0 & \text{otherwise.} \end{cases}$$

Characteristic function

Characteristic function for the subset of u-free elements of $\mathbb{F}_q^\times$

For each divisor u of $q-1$, the characteristic function for the subset of u-free elements of $\mathbb{F}_q^\times$ is a map $\rho_u : \mathbb{F}_q^\times \longrightarrow \{0,1\}$ defined by

$$\rho_u : \alpha \longmapsto \theta(u) \sum_{d|u} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha), \tag{1}$$

where $\theta(u) = \dfrac{\phi(u)}{u}$ and χ_d denotes the multiplicative character of $\mathbb{F}_q$ of order d.

Exceptional Rational function

We say that a rational function $f \in \mathbb{F}_q(x)$ is exceptional if $f = cx^i g^d$ for some $c \in \mathbb{F}_q$, $i \in \mathbb{Z}$, $g \in \mathbb{F}_q(x)$ and $d > 1$ divides $q - 1$.

Literature Survey

In 2020, Cohen et al. [3] gave the following result for a general (n_1, n_2)-function. For each positive integer n, let

- $\mathbf{R}_n$:=$\{f = f_1/f_2$, non-exceptional rational functions over $\mathbb{F}_q$ of degree sum n that is, $n = n_1 + n_2$ and with $(f_1,\ f_2) = 1$ $\}$.
- $\mathbf{Q}_n$:= $\{q$, a prime power s.t. for every $f \in \mathbf{R}_n$ there exists a primitive element α (depending on f) in $\mathbb{F}_q$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_q\}$.

Literature Survey

In 2020, Cohen et al. [3] gave the following result for a general (n_1, n_2)-function. For each positive integer n, let

- $\mathbf{R}_n$:=$\{f = f_1/f_2$, non-exceptional rational functions over $\mathbb{F}_q$ of degree sum n that is, $n = n_1 + n_2$ and with $(f_1, f_2) = 1$ $\}$.
- $\mathbf{Q}_n$:= $\{q$, a prime power s.t. for every $f \in \mathbf{R}_n$ there exists a primitive element α (depending on f) in $\mathbb{F}_q$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_q\}$.

2020, S.D.Cohen et al.

Let $n \geq 2$, and q be a prime power. Suppose that

$$q^{\frac{1}{2}} > nW(q-1)^2.$$

Then $q \in \mathbf{Q}_n$.

Literature survey

We will use the following result of Weil [11], as described in [1].; (1948)

Lemma

Let $F(x) \in \mathbb{F}_q(x)$ be a rational function. Suppose $F(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$, where $f_j \in \mathbb{F}_q[x]$ is an irreducible polynomial and $r_j \in \mathbb{Z} \setminus \{0\}$ for $1 \leq j \leq k$. Let χ be a multiplicative character of $\mathbb{F}_q$. Suppose that the rational function $F(x)$ is not of the form $cH(x)^{ord(\chi)} \in \mathbb{F}_q(x)$ for some $H(x) \in \mathbb{F}_q(x)$ and $c \in \mathbb{F}_q^{\times}$, where $ord(\chi)$ is the order of χ. Then we have

$$\left| \sum_{\alpha \in \mathbb{F}_q, F(\alpha) \neq \infty} \chi(F(\alpha)) \right| \leq \left(\sum_{j=1}^{k} \deg(f_j) - 1 \right) q^{\frac{1}{2}}.$$

Inequality due to Robin [7, Theorem 11];

Lemma

For all $n \geq 3$, $\omega(n) \leq \frac{1.38402 \ \log n}{\log \ \log n}$.

Define,

- $\mathcal{R}_n$:=$\{f = f_1/f_2$, even or odd non-exceptional rational functions over $\mathbb{F}_q$ of degree sum n that is, $n = n_1 + n_2$ and with $(f_1, f_2) = 1$ $\}$.
- $\mathcal{Q}_n$:=$\{$ q, a prime power with $q \equiv 3 \pmod 4$ s.t. for every $f \in \mathcal{R}_n$ there exists a primitive element α (depending on f) in $\mathbb{F}_q$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_q\}$.

Define,

- $\mathcal{R}_n$:=$\{f = f_1/f_2$, even or odd non-exceptional rational functions over $\mathbb{F}_q$ of degree sum n that is, $n = n_1 + n_2$ and with $(f_1, f_2) = 1$ $\}$.
- $\mathcal{Q}_n$:=$\{$ q, a prime power with $q \equiv 3 \pmod 4$ s.t. for every $f \in \mathcal{R}_n$ there exists a primitive element α (depending on f) in $\mathbb{F}_q$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_q\}$.

Lemma

If χ_d is a multiplicative character of $\mathbb{F}_q^\times$ of even order d and $q \equiv 3 \pmod 4$, then $\chi_d(-1) = -1$.

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

$$N_f(m_1, m_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \rho_{m_1}(\alpha)\rho_{m_2}(f(\alpha))$$

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

$$N_f(m_1, m_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \rho_{m_1}(\alpha)\rho_{m_2}(f(\alpha))$$

$$N_f(m_1, m_2) = \theta(m_1)\theta(m_2) \sum_{d_1|m_1, d_2|m_2} \frac{\mu(d_1)}{\varphi(d_1)} \frac{\mu(d_2)}{\varphi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \chi_f(\chi_{d_1}, \chi_{d_2})$$

$$\text{where, } \chi_f(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)).$$

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

$$N_f(m_1, m_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \rho_{m_1}(\alpha)\rho_{m_2}(f(\alpha))$$

$$N_f(m_1, m_2) = \theta(m_1)\theta(m_2) \sum_{d_1 | m_1, d_2 | m_2} \frac{\mu(d_1)}{\varphi(d_1)} \frac{\mu(d_2)}{\varphi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \chi_f(\chi_{d_1}, \chi_{d_2})$$

$$\text{where, } \chi_f(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)).$$

- CASE 1: If f is an odd rational function and exactly one of d_1 or d_2 is even.
- CASE 2: If f is an even rational function and d_1 is even.

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

$$N_f(m_1, m_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \rho_{m_1}(\alpha)\rho_{m_2}(f(\alpha))$$

$$N_f(m_1, m_2) = \theta(m_1)\theta(m_2) \sum_{d_1|m_1, d_2|m_2} \frac{\mu(d_1)}{\varphi(d_1)} \frac{\mu(d_2)}{\varphi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \chi_f(\chi_{d_1}, \chi_{d_2})$$

$$\text{where, } \chi_f(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)).$$

- CASE 1: If f is an odd rational function and exactly one of d_1 or d_2 is even.
- CASE 2: If f is an even rational function and d_1 is even.
- $\chi_f(\chi_{d_1}, \chi_{d_2}) = -\chi_f(\chi_{d_1}, \chi_{d_2}) \Longrightarrow \chi_f(\chi_{d_1}, \chi_{d_2}) = 0.$

Outline of proof

- $N_f(m_1, m_2) := |\{\alpha \in \mathbb{F}_q : \alpha$ is m_1- free and $f(\alpha)$ is m_2- free, for m_1, m_2 divisors of $q-1.\}|$

$$N_f(m_1, m_2) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \rho_{m_1}(\alpha)\rho_{m_2}(f(\alpha))$$

$$N_f(m_1, m_2) = \theta(m_1)\theta(m_2) \sum_{d_1 | m_1, d_2 | m_2} \frac{\mu(d_1)}{\varphi(d_1)} \frac{\mu(d_2)}{\varphi(d_2)} \sum_{\chi_{d_1}, \chi_{d_2}} \chi_f(\chi_{d_1}, \chi_{d_2})$$

$$\text{where, } \chi_f(\chi_{d_1}, \chi_{d_2}) = \sum_{\alpha \in \mathbb{F}_q \setminus S_f} \chi_{d_1}(\alpha)\chi_{d_2}(f(\alpha)).$$

- CASE 1: If f is an odd rational function and exactly one of d_1 or d_2 is even.
- CASE 2: If f is an even rational function and d_1 is even.
- $\chi_f(\chi_{d_1}, \chi_{d_2}) = -\chi_f(\chi_{d_1}, \chi_{d_2}) \implies \chi_f(\chi_{d_1}, \chi_{d_2}) = 0.$
- $N_f(m_1, m_2) > 0$ whenever $q^{\frac{1}{2}} \geq \frac{nW(m_1)W(m_2)}{2}$.

Results

Theorem 1

Suppose $n \in \mathbb{N}$, $n \geq 2$ and $q \equiv 3 \pmod 4$ is a prime power. Then

$$q^{\frac{1}{2}} \geq \frac{nW(q-1)^2}{2} \implies q \in \mathcal{Q}_n. \tag{2}$$

Results

Theorem 1

Suppose $n \in \mathbb{N}$, $n \geq 2$ and $q \equiv 3 \pmod 4$ is a prime power. Then

$$q^{\frac{1}{2}} \geq \frac{nW(q-1)^2}{2} \Longrightarrow q \in \mathcal{Q}_n. \tag{2}$$

The following result is the sieve variation of Theorem 1.

Theorem 2

Let $e|(q-1)$, and let $\{p_1, p_2, ..., p_r\}$ be the collection of all primes dividing $(q-1)$ but not dividing e. Suppose $\delta := 1 - 2\sum_{i=1}^{r} \frac{1}{p_i} > 0$ and set $\Delta = \frac{(2r-1)}{\delta} + 2$. Then

$$q^{\frac{1}{2}} \geq \frac{n\Delta W(e)^2}{2} \Longrightarrow q \in \mathcal{Q}_n. \tag{3}$$

Outline of the proof of Theorem2

For the proof of Theorem2, we require the following lemma which give an upper bound for the absolute value of $N_f(pe, e) - \theta(p)N_f(e, e)$ and $N_f(e, pe) - \theta(p)N_f(e, e)$.

Lemma

Let e be a positive integer that divides $q-1$ and let p be a prime that divides $q-1$ but not e. If $f \in \mathcal{R}_n$ and $q \equiv 3 \pmod 4$, then

$$|N_f(pe, e) - \theta(p)N_f(e, e)| \leq \frac{\theta(e)^2\theta(p)}{2} nq^{\frac{1}{2}} W(e)^2$$

and

$$|N_f(e, pe) - \theta(p)N_f(e, e)| \leq \frac{\theta(e)^2\theta(p)}{2} nq^{\frac{1}{2}} W(e)^2.$$

Outline of the proof of Theorem2

Lemma

Let e be a positive integer that divides $q-1$ and let $\{p_1, p_2, \ldots, p_r\}$ be the collection of all primes that divides $q-1$ but not e. Then

$$N_f(q-1, q-1) \geq \sum_{i=1}^{r} N_f(p_i e, e) + \sum_{i=1}^{r} N_f(e, p_i e) - (2r-1)N_f(e, e).$$

Hence,

$$N_f(q-1, q-1) \geq \sum_{i=1}^{r}(N_f(p_i e, e) - \theta(p_i)N_f(e, e)) + \sum_{i=1}^{r}(N_f(e, p_i e) - \theta(p_i)N$$

$$\{1 - 2\sum_{i=1}^{r}(1 - \theta(p_i))\} \times N_f(e, e).$$

Outline of the proof of Theorem2

We have $q \in \mathcal{Q}_n$ if

$$q^{\frac{1}{2}} \geq \frac{nW(q-1)^2}{2} \iff \log q \geq 2\log n + 4\omega(q-1)\log 2 - 2\log 2.$$

which holds if,

$$\left(1 - \frac{5.5361\log 2}{\log\log q}\right)\frac{\log q}{2\log(\frac{n}{2})} \geq 1.$$

Outline of the proof of Theorem2

We have $q \in \mathcal{Q}_n$ if

$$q^{\frac{1}{2}} \geq \frac{nW(q-1)^2}{2} \iff \log q \geq 2\log n + 4\omega(q-1)\log 2 - 2\log 2.$$

which holds if,

$$\left(1 - \frac{5.5361\log 2}{\log\log q}\right)\frac{\log q}{2\log(\frac{n}{2})} \geq 1.$$

Theorem 3

Suppose $n \in \mathbb{N}$, $n \geq 2$ and q is a prime power such that $q \equiv 3 \pmod 4$. Let $n_0 = 2(\exp(2^{2\times 4.5361})$. Then

$$q \geq \begin{cases} (\frac{n}{2})^4 & \text{if } n \geq n_0, \\ \max\{(\frac{n}{2})^8, \exp(2^{\frac{4}{3}\times 5.5361})\} & \text{if } n < n_0, \end{cases} \tag{4}$$

implies $q \in \mathcal{Q}_n$.

The following result is an analogue of the Theorem 3 for functions which are not necessarily even or odd; needless to say that it is a consequence of [3, Theorem 3.3].

Theorem 4

Let q be a prime power, $n \geq 2$ be an integer and let $f(x) \in \mathbb{F}_q(x)$ be a non-exceptional rational function of degree sum n. Set $\gamma = 0.9998$ and $n_0 = 2\gamma^{-1}\exp(2^{2\times 4.5361})$. If

$$q \geq \begin{cases} (n\gamma)^4 & \text{if } n \geq n_0, \\ \max\{(n\gamma)^8, \exp(2^{\frac{4}{3}\times 5.5361})\} & \text{if } n < n_0, \end{cases}$$

then there exists $\alpha \in \mathbb{F}_q$ such that both α and $f(\alpha)$ are primitive in $\mathbb{F}_q$.

The minimum number of prime factors of $q-1$ required for $\mathbb{F}_q$ to have a primitive pair is displayed in Table for certain degree sums of rational functions according to Theorem 3.1 in [3] and Theorem 1.

Degree sum (n)	2	3	4	5	6	7	8	9
$\omega(q-1)$ for general f	17	18	18	19	19	19	19	19
$\omega(q-1)$ for even or odd f	16	17	17	17	18	18	18	18

Table: Minimum value of $\omega(q-1)$ with respect to degree sum of f

The minimum number of prime factors of $q-1$ required for $\mathbb{F}_q$ to have a primitive pair is displayed in Table for certain degree sums of rational functions according to Theorem 3.1 in [3] and Theorem 1.

Degree sum (n)	2	3	4	5	6	7	8	9
$\omega(q-1)$ for general f	17	18	18	19	19	19	19	19
$\omega(q-1)$ for even or odd f	16	17	17	17	18	18	18	18

Table: Minimum value of $\omega(q-1)$ with respect to degree sum of f

For example, for a general non-exceptional rational function of degree sum 3, we require $q \geq 1.173 \times 10^{23}$ whereas for an even or an odd non-exceptional rational function function of degree sum 3, we require $q \geq 1.923 \times 10^{21}$.

Bibliography I

[1] Cochrane, T., Pinner, C. Using Stepanov's method for exponential sums involving rational functions. *J. Number Theory* 116(2):270-292, 2006.

[2] Cohen, S. D. Consecutive primitive roots in a finite field. *Proc. Amer. Math. Soc.* 93(2):189-197, 1985.

[3] Cohen, S .D., Sharma, H., Sharma, R. K. Primitive values of rational functions at primitive elements of a finite field. *J. Number Theory* 219:237-246, 2021.

[4] Cohen, S. D., Silva, T. O. e., Sutherland, N., Trudgian, T. A proof of the conjecture of Cohen and Mullen on sums of primitive roots. *Math. Comput.* 84 (296):2979-2986,2015.

[5] Fu, L., Wan, D. A class of incomplete character sums. *Q. J. Math.* 65(4):1195-1211, 2014.

[6] Lidl, R., Niederreiter, H.*Finite Field*, Vol. 20. Cambridge (UK): Cambridge University Press, 1997.

Bibliography II

[7] Robin, G. Estimation de la fonction de Tehebychef θ sur le k-ieme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arithmetica*:367-389, 1983.

[8] Sharma, R. K., Gupta, A. Pair of primitive elements with prescribed traces over finite fields. *Commun. Algebra* 47(3):1278-1286, 2019.

[9] The Sage Developers, SageMath, the Sage mathematics software system (version 9.0), https:// www.sagemath.org, 2020.

[10] Shuqin, F., Wenbao, H. Character sums over Galois rings and primitive polynomials over finite fields. *Finite Fields Appl.* 10(1):36-52, 2004.

[11] Weil, A. On some exponential sums. *Proc. Natl. Acad. Sci.* 34(5):204-207, 1948.


Thank you