Existence of Primitive pairs with two prescribed traces over finite fields

By
Aakash Choudhary

A joint work with
Dr. R. K. Sharma

July 4, 2023

Department of Mathematics
Indian Institute of Technology Delhi

Outline of the Presentation

Notations

- p is arbitrary prime power.
- $\mathbb{F}^* := \mathbb{F} - \{0\}$ for a field $\mathbb{F}$.
- ϕ is the Euler's phi-function.
- μ is the Mobius function.
- $\widehat{G}$ is the group of characters of the group G.
- $\omega(m)$ is the number of distinct prime divisors of m.
- $W(m) := 2^{\omega(m)}$ is the number of square free divisors of m.
- $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \epsilon + \epsilon^p + \cdots + \epsilon^{p^{t-1}}$.

Character

Let G be a finite abelian group. A character χ is a homomorphism from G into the multiplicative group $Z = \{z \in \mathbb{C} : |z| = 1\}$ of complex numbers of absolute value 1,

$$\chi : G \longrightarrow Z.$$

Among the characters of G, the trivial character of G, denoted by χ_1, is defined as $\chi_1(a) = 1$ for all $a \in G$.

Basic definitions and results

Theorem [9, Lidl, R., Niederreiter, H.]

1. If χ is a non-trivial character of a finite abelian group G, then $\sum_{a\in G}\chi(a)=0$.
2. If $a\in G$ is a non trivial element and $\widehat{G}$ is the group of all characters of group G, then $\sum_{\chi\in\widehat{G}}\chi(a)=0$.

Basic definitions and results

Theorem [9, Lidl, R., Niederreiter, H.]

1. If χ is a non-trivial character of a finite abelian group G, then $\sum_{a \in G} \chi(a) = 0$.
2. If $a \in G$ is a non trivial element and $\widehat{G}$ is the group of all characters of group G, then $\sum_{\chi \in \widehat{G}} \chi(a) = 0$.

Primitive pair

An element is said to be a primitive element over $\mathbb{F}_p$ if it generates $\mathbb{F}_p{}^*$. We call $(\epsilon, f(\epsilon))$ a primitive pair in $\mathbb{F}_p$ if both ϵ and $f(\epsilon)$ are primitive elements of $\mathbb{F}_p$, for $f \in \mathbb{F}_p(x)$.

Trace

For $\epsilon \in \mathbb{F}_{p^t}$, the Trace, denoted by $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon)$ of ϵ over $\mathbb{F}_p$, is defined by

$$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \epsilon + \epsilon^p + \cdots + \epsilon^{p^{t-1}}.$$

Trace

For $\epsilon \in \mathbb{F}_{p^t}$, the Trace, denoted by $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon)$ of ϵ over $\mathbb{F}_p$, is defined by

$$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \epsilon + \epsilon^p + \cdots + \epsilon^{p^{t-1}}.$$

Characteristic function for the subset of $\mathbb{F}_{p^t}$ with $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$.

For $a \in \mathbb{F}_p$, characteristic function for the subset of $\mathbb{F}_{p^t}$ with $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ is given by

$$\tau_a : \epsilon \longmapsto \frac{1}{p} \sum_{\psi \in \widehat{\mathbb{F}}_p} \psi(Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) - a).$$

Basic definitions and results

u- free element

For u, a divisor of $p-1$, an element $\epsilon \in \mathbb{F}_p$ is called u - free, if $\epsilon = \beta^d$, where $\beta \in \mathbb{F}_p$ and $d|u$, implies $d = 1$.
Clearly an element ϵ is primitive if and only if it is $(p-1)$ - free.

u- free element

For u, a divisor of $p-1$, an element $\epsilon \in \mathbb{F}_p$ is called u - free, if $\epsilon = \beta^d$, where $\beta \in \mathbb{F}_p$ and $d|u$, implies $d = 1$.
Clearly an element ϵ is primitive if and only if it is $(p-1)$ - free.

Characteristic function [5, Fan, S., Han, W. (2004)]:-

For $u \mid p-1$, the characteristic function for the subset of u-free elements of $\mathbb{F}_p^*$ is given by

$$\rho_u : \epsilon \longmapsto \theta(u) = \frac{\phi(u)}{u} \sum_{d|u} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\epsilon),$$

u- free element

For u, a divisor of $p-1$, an element $\epsilon \in \mathbb{F}_p$ is called u - free, if $\epsilon = \beta^d$, where $\beta \in \mathbb{F}_p$ and $d|u$, implies $d = 1$.
Clearly an element ϵ is primitive if and only if it is $(p-1)$ - free.

Characteristic function [5, Fan, S., Han, W. (2004)]:-

For $u \mid p-1$, the characteristic function for the subset of u-free elements of $\mathbb{F}_p^*$ is given by

$$\rho_u : \epsilon \longmapsto \theta(u) = \frac{\phi(u)}{u} \sum_{d|u} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\epsilon),$$

where χ_d denotes the multiplicative character of $\mathbb{F}_p$ of order d.

Literature Survey

In 1948, Weil [11] gave the following bound:

Literature Survey

In 1948, Weil [11] gave the following bound:

Lemma

Let $F(x) \in \mathbb{F}_p(x)$ be a rational function. Write $F(x) = \prod_{j=1}^{k} F_j(x)^{r_j}$, where where $F_j(x) \in \mathbb{F}_p[x]$ are irreducible polynomials and r_j non zero integers. Let χ be a multiplicative character of $\mathbb{F}_p$ of precise square-free order d (a divisor of $q-1$). Suppose that $F(x)$ is not of the form $cG(x)^d$ for some rational function $G(x) \in \mathbb{F}_{p^t}(x)$ and $c \in \mathbb{F}_p^*$. Then we have

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

Literature Survey

In 2014 Fu.L.,Wan.D. [6] gave the following lemma:-

Literature Survey

In 2014 Fu.L.,Wan.D. [6] gave the following lemma:-

Lemma

Let $f(x)$, $g(x) \in \mathbb{F}_{p^t}(x)$ be rational functions. Write $f(x) = \prod_{j=1}^{k} f_j(x)^{n_j}$, where $f_j(x) \in \mathbb{F}_{p^t}[x]$ are irreducible polynomials and n_j are non-zero integers. Let $D_1 = \sum_{j=1}^{k} deg(f_j)$, $D_2 = max\{deg(g), 0\}$, D_3 be the degree of denominator of $g(x)$ and D_4 be the sum of degrees of those irreducible polynomials dividing denomiator of g but distinct from $f_j(x)$ $(j = 1, 2, ..., k)$. Let χ be a multiplicative character of $\mathbb{F}_{p^t}$, and let ψ be a nontrivial additive character of $\mathbb{F}_{p^t}$. Suppose $g(x)$ is not of the form $r(x)^{p^t} - r(x)$ in $\mathbb{F}(x)$. Then we have

$$\left| \sum_{\epsilon \in \mathbb{F}_{p^t}, f(\epsilon) \neq 0, \infty, g(\epsilon) \neq \infty} \chi(f(\epsilon))\psi(g(\epsilon)) \right| \leq (D_1 + D_2 + D_3 + D_4 - 1)q^{\frac{m}{2}}.$$

Literature Survey

- In 1985, Cohen [3] introduced the term *"primitive pair"* and verified the existence of primitive pairs $(\epsilon, f(\epsilon))$ in $\mathbb{F}_p$ for linear polynomials $f(x) = x + k \in \mathbb{F}_p[x]$.

Literature Survey

- In 1985, Cohen [3] introduced the term *"primitive pair"* and verified the existence of primitive pairs $(\epsilon, f(\epsilon))$ in $\mathbb{F}_p$ for linear polynomials $f(x) = x + k \in \mathbb{F}_p[x]$.
- Jungnickel, Vanstone [8] identified a sufficient condition for the occurrence of primitive elements $\epsilon \in \mathbb{F}_{p^t}$ with a prescribed trace of ϵ. Later Cohen [4] extended the result with some exceptions.

Literature Survey

- In 1985, Cohen [3] introduced the term *"primitive pair"* and verified the existence of primitive pairs $(\epsilon, f(\epsilon))$ in $\mathbb{F}_p$ for linear polynomials $f(x) = x + k \in \mathbb{F}_p[x]$.
- Jungnickel, Vanstone [8] identified a sufficient condition for the occurrence of primitive elements $\epsilon \in \mathbb{F}_{p^t}$ with a prescribed trace of ϵ. Later Cohen [4] extended the result with some exceptions.
- In 2014, Chou and Cohen [2] addressed the issue of the existence of primitive element $\epsilon \in \mathbb{F}_{p^t}$ such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$.

Literature Survey

- For $t \geq 29$, Cao and Wang [1] established a condition for the existence of primitive pair $(\epsilon, f(\epsilon))$ with $f(x) = \frac{x^2+1}{x} \in \mathbb{F}_{p^t}(x)$ such that for prescribed $a, b \in \mathbb{F}_p^*$, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$.

Literature Survey

- For $t \geq 29$, Cao and Wang [1] established a condition for the existence of primitive pair $(\epsilon, f(\epsilon))$ with $f(x) = \frac{x^2+1}{x} \in \mathbb{F}_{p^t}(x)$ such that for prescribed $a, b \in \mathbb{F}_p^*$, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$.
- In 2018, Gupta, Sharma and Cohen [7], for the same rational function and prescribed $a \in \mathbb{F}_p$, presented a condition that ensures the existence of primitive pair $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{p^t}$ with $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ for $t \geq 5$.

Literature Survey

- In 2021, Sharma and Sharma [10] examined the rational function $f = f_1/f_2$ in $\mathbb{F}_{p^t}(x)$, where f_1 and f_2 are distinct, irreducible polynomials and proved that for prescribed $a, b \in \mathbb{F}_p$, the existence of primitive pair $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{p^t}$ such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$ for $t \geq 7$.

Literature Survey

- In 2021, Sharma and Sharma [10] examined the rational function $f = f_1/f_2$ in $\mathbb{F}_{p^t}(x)$, where f_1 and f_2 are distinct, irreducible polynomials and proved that for prescribed $a, b \in \mathbb{F}_p$, the existence of primitive pair $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{p^t}$ such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$ for $t \geq 7$.

2021, Sharma H., Sharma R.K. [10]

Let $t, n, p \in \mathbb{N}$, where p is prime power. Suppose

$$p^{\frac{t}{2}-2} > (n+2)W(p^t-1)^2,$$

then there exist an element $\epsilon \in \mathbb{F}_{p^t}^*$ such that $(\epsilon, f(\epsilon))$ is a primitive pair in $\mathbb{F}_{p^t}$ with $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$.

Result

Prior to this article, for primitive pairs, traces were considered for ϵ and ϵ^{-1}. We consider the trace onto the element ϵ and its image under f, i.e., $f(\epsilon)$, where f is a rational function with some conditions. For this we prove the following theorem.

Result

Prior to this article, for primitive pairs, traces were considered for ϵ and ϵ^{-1}. We consider the trace onto the element ϵ and its image under f, i.e., $f(\epsilon)$, where f is a rational function with some conditions. For this we prove the following theorem.

Theorem

Let p, n, $t \in \mathbb{N}$ and p is prime power. Suppose that

$$p^{\frac{t}{2}-2} > (2n+1)W(p^t-1)^2.$$

then there exist an element $\epsilon \in \mathbb{F}_{p^t}^*$ such that $(\epsilon, f(\epsilon))$ is a primitive pair in $\mathbb{F}_{p^t}$ with $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.

Idea of the proof

For $n_1, n_2 \in \mathbb{N} \cup \{0\}$, define the following sets.

Idea of the proof

For $n_1, n_2 \in \mathbb{N} \cup \{0\}$, define the following sets.

- Define $R_{p,t}(n_1, n_2)$ as the set of all rational function $f(x) = \frac{f_1(x)}{f_2(x)} \in \mathbb{F}_{p^t}(x)$ such that f_1 and f_2 are distinct irreducible polynomials over $\mathbb{F}_{p^t}$ with $\deg(f_1) = n_1$, $\deg(f_2) = n_2$ and $n_1 + n_2 \leq p^t$.

Idea of the proof

For $n_1, n_2 \in \mathbb{N} \cup \{0\}$, define the following sets.

- Define $R_{p,t}(n_1, n_2)$ as the set of all rational function $f(x) = \frac{f_1(x)}{f_2(x)} \in \mathbb{F}_{p^t}(x)$ such that f_1 and f_2 are distinct irreducible polynomials over $\mathbb{F}_{p^t}$ with $\deg(f_1) = n_1$, $\deg(f_2) = n_2$ and $n_1 + n_2 \leq p^t$.
- Denote A_{n_1,n_2} as the set consisting of pairs $(p, t) \in \mathbb{N} \times \mathbb{N}$ such that for any $f \in R_{p,t}(n_1, n_2)$ and prescribed $a, b \in \mathbb{F}_p$, $\mathbb{F}_{p^t}$ contains an element ϵ such that $(\epsilon, f(\epsilon))$ is a primitive pair with $\text{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\text{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.

Idea of the proof

For $n_1, n_2 \in \mathbb{N} \cup \{0\}$, define the following sets.

- Define $R_{p,t}(n_1, n_2)$ as the set of all rational function $f(x) = \frac{f_1(x)}{f_2(x)} \in \mathbb{F}_{p^t}(x)$ such that f_1 and f_2 are distinct irreducible polynomials over $\mathbb{F}_{p^t}$ with $\deg(f_1) = n_1$, $\deg(f_2) = n_2$ and $n_1 + n_2 \leq p^t$.
- Denote A_{n_1,n_2} as the set consisting of pairs $(p, t) \in \mathbb{N} \times \mathbb{N}$ such that for any $f \in R_{p,t}(n_1, n_2)$ and prescribed $a, b \in \mathbb{F}_p$, $\mathbb{F}_{p^t}$ contains an element ϵ such that $(\epsilon, f(\epsilon))$ is a primitive pair with $\text{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\text{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.
- Define, $R_{p,t}(n) = \bigcup_{n_1+n_2=n} R_{p,t}(n_1, n_2)$ and $A_n = \bigcap_{n_1+n_2=n} A_{n_1,n_2}$.

Idea of the proof

- Let $k_1, k_2, p, t \in \mathbb{N}$ be such that k_1 and k_2 are positive divisors of $p^t - 1$. Let $a, b \in \mathbb{F}_p$ and $f(x) \in R_{p,t}(n)$.

Idea of the proof

- Let $k_1, k_2, p, t \in \mathbb{N}$ be such that k_1 and k_2 are positive divisors of $p^t - 1$. Let $a, b \in \mathbb{F}_p$ and $f(x) \in R_{p,t}(n)$.
- $A_{f,n,a,b}(k_1, k_2)$ denotes the cardinality of the set consisting of all those elements $\epsilon \in \mathbb{F}_{p^t}$ such that ϵ is k_1-free, $f(\epsilon)$ is k_2-free, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.

Idea of the proof

- Let $k_1, k_2, p, t \in \mathbb{N}$ be such that k_1 and k_2 are positive divisors of $p^t - 1$. Let $a, b \in \mathbb{F}_p$ and $f(x) \in R_{p,t}(n)$.
- $A_{f,n,a,b}(k_1, k_2)$ denotes the cardinality of the set consisting of all those elements $\epsilon \in \mathbb{F}_{p^t}$ such that ϵ is k_1-free, $f(\epsilon)$ is k_2-free, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.
- We want to find sufficient condition that imply $A_{f,n,a,b}(k_1, k_2) > 0$.

Idea of the proof

- Let $k_1, k_2, p, t \in \mathbb{N}$ be such that k_1 and k_2 are positive divisors of $p^t - 1$. Let $a, b \in \mathbb{F}_p$ and $f(x) \in R_{p,t}(n)$.
- $A_{f,n,a,b}(k_1, k_2)$ denotes the cardinality of the set consisting of all those elements $\epsilon \in \mathbb{F}_{p^t}$ such that ϵ is k_1-free, $f(\epsilon)$ is k_2-free, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.
- We want to find sufficient condition that imply $A_{f,n,a,b}(k_1, k_2) > 0$.
- From characteristics function, $A_{f,n,a,b}(k_1, k_2)$ will be given by

Idea of the proof

- Let $k_1, k_2, p, t \in \mathbb{N}$ be such that k_1 and k_2 are positive divisors of $p^t - 1$. Let $a, b \in \mathbb{F}_p$ and $f(x) \in R_{p,t}(n)$.
- $A_{f,n,a,b}(k_1, k_2)$ denotes the cardinality of the set consisting of all those elements $\epsilon \in \mathbb{F}_{p^t}$ such that ϵ is k_1-free, $f(\epsilon)$ is k_2-free, $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$.
- We want to find sufficient condition that imply $A_{f,n,a,b}(k_1, k_2) > 0$.
- From characteristics function, $A_{f,n,a,b}(k_1, k_2)$ will be given by

$$A_{f,n,a,b}(k_1, k_2) = \sum_{\epsilon \in \mathbb{F}_{p^t}/P'} \rho_{k_1}(\epsilon)\rho_{k_2}(f(\epsilon))\tau_a(\epsilon)\tau_b(f(\epsilon))$$

$$= \frac{\phi(k_1)\phi(k_2)}{k_1 k_2 p^2} \sum_{s_1|k_1, s_2|k_2} \frac{\mu(s_1)\mu(s_2)}{\phi(s_1)\phi(s_2)} \sum_{\chi_{s_1}, \chi_{s_2}} \chi_{f,a,b}(s_1, s_2),$$

Idea of the proof

where

$$\chi_{f,a,b}(s_1,s_2) = \sum_{u,v\in\mathbb{F}_p} \psi_0(-au-bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{s_1}(\epsilon)\chi_{s_2}(\beta)\widehat{\psi_0}(u\epsilon+v\epsilon_0)$$

$$= \sum_{u,v\in\mathbb{F}_p} \psi_0(-au-bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{p^t-1}(\epsilon^{m_1}f(\epsilon)^{m_2})\widehat{\psi_0}(u\epsilon+v\epsilon_0).$$

Idea of the proof

where

$$\chi_{f,a,b}(s_1, s_2) = \sum_{u,v\in\mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{s_1}(\epsilon)\chi_{s_2}(\beta)\widehat{\psi_0}(u\epsilon + v\epsilon_0)$$

$$= \sum_{u,v\in\mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{p^t-1}(\epsilon^{m_1} f(\epsilon)^{m_2})\widehat{\psi_0}(u\epsilon + v\epsilon_0).$$

- If $(\chi_{s_1}, \chi_{s_2}, u, v) \neq (\chi_1, \chi_1, 0, 0)$, then using Lemma 1 and Lemma 2, we get $|\chi_{f,a,b}(\chi_{s_1}, \chi_{s_2})| \leq (2n+1)p^{\frac{t}{2}+2}$.

Idea of the proof

where

$$\chi_{f,a,b}(s_1, s_2) = \sum_{u,v \in \mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon \in \mathbb{F}_{p^t} \setminus P'} \chi_{s_1}(\epsilon)\chi_{s_2}(\beta)\widehat{\psi_0}(u\epsilon + v\epsilon_0)$$

$$= \sum_{u,v \in \mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon \in \mathbb{F}_{p^t} \setminus P'} \chi_{p^t-1}(\epsilon^{m_1} f(\epsilon)^{m_2})\widehat{\psi_0}(u\epsilon + v\epsilon_0).$$

- If $(\chi_{s_1}, \chi_{s_2}, u, v) \neq (\chi_1, \chi_1, 0, 0)$, then using Lemma 1 and Lemma 2, we get $|\chi_{f,a,b}(\chi_{s_1}, \chi_{s_2})| \leq (2n+1)p^{\frac{t}{2}+2}$.
- After doing some further manipulation we reach at

$$p^{\frac{t}{2}-2} > (2n+1)W(k_1)W(k_2) \implies A_{f,n,a,b}(k_1, k_2) > 0.$$

Idea of the proof

where

$$\chi_{f,a,b}(s_1, s_2) = \sum_{u,v\in\mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{s_1}(\epsilon)\chi_{s_2}(\beta)\widehat{\psi_0}(u\epsilon + v\epsilon_0)$$
$$= \sum_{u,v\in\mathbb{F}_p} \psi_0(-au - bv) \sum_{\epsilon\in\mathbb{F}_{p^t}\setminus P'} \chi_{p^t-1}(\epsilon^{m_1} f(\epsilon)^{m_2})\widehat{\psi_0}(u\epsilon + v\epsilon_0).$$

- If $(\chi_{s_1}, \chi_{s_2}, u, v) \neq (\chi_1, \chi_1, 0, 0)$, then using Lemma 1 and Lemma 2, we get $|\chi_{f,a,b}(\chi_{s_1}, \chi_{s_2})| \leq (2n+1)p^{\frac{t}{2}+2}$.
- After doing some further manipulation we reach at

$$p^{\frac{t}{2}-2} > (2n+1)W(k_1)W(k_2) \implies A_{f,n,a,b}(k_1, k_2) > 0.$$

and proof is completed.

Sieve variation

Lemma

Let k be a positive divisor of $p^t - 1$ and m is a prime dividing $p^t - 1$ but not k. Then

1. $|A_{f,n,a,b}(mk, k) - \theta(m)A_{f,n,a,b}(k, k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2 p^{\frac{t}{2}+2}$.
2. $|A_{f,n,a,b}(k, mk) - \theta(m)A_{f,n,a,b}(k, k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2 p^{\frac{t}{2}+2}$.

Sieve variation

Lemma

Let k be a positive divisor of $p^t - 1$ and m is a prime dividing $p^t - 1$ but not k. Then

1. $|A_{f,n,a,b}(mk, k) - \theta(m)A_{f,n,a,b}(k, k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2p^{\frac{t}{2}+2}$.
2. $|A_{f,n,a,b}(k, mk) - \theta(m)A_{f,n,a,b}(k, k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2p^{\frac{t}{2}+2}$.

Lemma

Let k be a positive divisor of $p^t - 1$ and $\{q_1, q_2, \ldots, q_m\}$ be the collection of all primes dividing $p^t - 1$ but not k. Then

$$A(p^t - 1, p^t - 1) \geq \sum_{i=1}^{m} A(k, q_i k) + \sum_{i=1}^{m} A(q_i k, k) - (2m-1)A(k, k),$$

where $A = A_{f,n,a,b}$.

Sieve variation

Sieve variation of sufficient condition (Theorem 3) is given below, proof of which follows from Lemmas 4, Lemma 5 and ideas in [7].

Sieve variation

Sieve variation of sufficient condition (Theorem 3) is given below, proof of which follows from Lemmas 4, Lemma 5 and ideas in [7].

Theorem

Let $t, n, p, k \in \mathbb{N}$ be such that k divides $p^t - 1$. Let $\{q_1, q_2, \dots, q_m\}$ be the collection of all those primes that divide $p^t - 1$ but not k. Suppose $\delta = 1 - 2\sum_{i=1}^{m} \frac{1}{q_i} > 0$ and $\Delta = \frac{2m-1}{\delta} + 2$. If

$$p^{\frac{t}{2}-2} > (2n+1)\Delta W(k)^2$$

then $(p, t) \in A_n$.

Sieve variation

Sieve variation of sufficient condition (Theorem 3) is given below, proof of which follows from Lemmas 4, Lemma 5 and ideas in [7].

Theorem

Let $t, n, p, k \in \mathbb{N}$ be such that k divides $p^t - 1$. Let $\{q_1, q_2, \ldots, q_m\}$ be the collection of all those primes that divide $p^t - 1$ but not k. Suppose $\delta = 1 - 2\sum_{i=1}^{m} \frac{1}{q_i} > 0$ and $\Delta = \frac{2m-1}{\delta} + 2$. If

$$p^{\frac{t}{2}-2} > (2n+1)\Delta W(k)^2$$

then $(p, t) \in A_n$.

Lemma

Suppose $\kappa \in \mathbb{N}$ *is such that* $\omega(\kappa) \geq 1547$*, then* $W(\kappa) \leq \kappa^{1/12}$.

Calculation for A_2

Calculation is carried for the situation $t \geq 7$, as from [2, Chou, W. S., Cohen, S. D. (2001)] there is no primitive element ϵ, for $t \leq 4$, such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = 0$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$, and the cases $t = 5$ and $t = 6$ necessitate substantial computation and appear to demand a different technique.

Calculation for A_2

Calculation is carried for the situation $t \geq 7$, as from [2, Chou, W. S., Cohen, S. D. (2001)] there is no primitive element ϵ, for $t \leq 4$, such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = 0$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$, and the cases $t = 5$ and $t = 6$ necessitate substantial computation and appear to demand a different technique.

- For $\omega(p^t - 1) \geq 1547$. By Theorem 3 and Lemma 6, $(p, t) \in A_2$, if $p^{\frac{t}{2}-2} > 5p^{\frac{t}{6}}$. But $t \geq 7$ gives $\frac{3t}{t-6} \leq 21$. Hence $(p, t) \in A_2$, if $p^t > 5^{21}$, which is true for $\omega(p^t - 1) \geq 1547$.

Calculation for A_2

Calculation is carried for the situation $t \geq 7$, as from [2, Chou, W. S., Cohen, S. D. (2001)] there is no primitive element ϵ, for $t \leq 4$, such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = 0$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$, and the cases $t = 5$ and $t = 6$ necessitate substantial computation and appear to demand a different technique.

- For $\omega(p^t - 1) \geq 1547$. By Theorem 3 and Lemma 6, $(p, t) \in A_2$, if $p^{\frac{t}{2}-2} > 5p^{\frac{t}{6}}$. But $t \geq 7$ gives $\frac{3t}{t-6} \leq 21$. Hence $(p, t) \in A_2$, if $p^t > 5^{21}$, which is true for $\omega(p^t - 1) \geq 1547$.
- For $\omega(p^t - 1) \leq 1546$. We use sieve variation (Theorem 4.1) and see that δ assumes its least positive value when $\omega(p^t - 1) \geq 62$.

Calculation for A_2

Calculation is carried for the situation $t \geq 7$, as from [2, Chou, W. S., Cohen, S. D. (2001)] there is no primitive element ϵ, for $t \leq 4$, such that $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = 0$ and $\mathrm{Tr}_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$, and the cases $t = 5$ and $t = 6$ necessitate substantial computation and appear to demand a different technique.

- For $\omega(p^t - 1) \geq 1547$. By Theorem 3 and Lemma 6, $(p, t) \in A_2$, if $p^{\frac{t}{2}-2} > 5p^{\frac{t}{6}}$. But $t \geq 7$ gives $\frac{3t}{t-6} \leq 21$. Hence $(p, t) \in A_2$, if $p^t > 5^{21}$, which is true for $\omega(p^t - 1) \geq 1547$.
- For $\omega(p^t - 1) \leq 1546$. We use sieve variation (Theorem 4.1) and see that δ assumes its least positive value when $\omega(p^t - 1) \geq 62$.
- $(p, t) \in A_2$ if $p^t > 5.834 \times 10^{204}$ or $\omega(p^t - 1) \geq 95$ for $t \geq 7$.

Table

Table 1.

$a \leq \omega \leq b$	$W(k)$	$\delta >$	$\Delta <$	$5\Delta W(k)^2 <$
$a = 13,\ b = 94$	2^{13}	0.04481712	3594.3767988	1.2061×10^{12}
$a = 7,\ b = 34$	2^7	0.04609692	1151.7513186	94,351,469
$a = 6,\ b = 25$	2^6	0.08241088	450.9698124	9,235,862
$a = 6,\ b = 23$	2^6	0.12550135	264.9453729	5,426,082
$a = 6,\ b = 22$	2^6	0.14959773	209.2223842	4,284,875
$a = 5,\ b = 19$	2^5	0.07663431	354.3225878	1,814,132
$a = 5,\ b = 17$	2^5	0.13927194	167.1445296	855,780
$a = 5,\ b = 16$	2^5	0.17317025	123.2679422	631,132
$a = 5,\ b = 15$	2^5	0.21090610	92.0874844	471,488

where $\omega = \omega(p^t - 1)$.

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

- $p^t > 8.8929 \times 10^{30}$ for $t \geq 7$,

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

- $p^t > 8.8929 \times 10^{30}$ for $t \geq 7$,
- $p^t > 1.084 \times 10^{25}$. for $t \geq 8$,

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

- $p^t > 8.8929 \times 10^{30}$ for $t \geq 7$,
- $p^t > 1.084 \times 10^{25}$. for $t \geq 8$,
- $p^t > 2.2725 \times 10^{21}$ for $t \geq 9$ and

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

- $p^t > 8.8929 \times 10^{30}$ for $t \geq 7$,
- $p^t > 1.084 \times 10^{25}$. for $t \geq 8$,
- $p^t > 2.2725 \times 10^{21}$ for $t \geq 9$ and
- $p^t > 8.158 \times 10^{18}$ for $t \geq 10$.

Calculation for A_2

We deduce, utilising Sieve variation repeatedly for values in Table 1 that, $(p, t) \in A_2$ if

- $p^t > 8.8929 \times 10^{30}$ for $t \geq 7$,
- $p^t > 1.084 \times 10^{25}$. for $t \geq 8$,
- $p^t > 2.2725 \times 10^{21}$ for $t \geq 9$ and
- $p^t > 8.158 \times 10^{18}$ for $t \geq 10$.

Hence $(p, t) \in A_2$ unless $t = 7$ and $p < 26382$, $t = 8$ and $p < 1347$, $t = 9$ and $p < 237$, $t = 10$ and $p < 78$, $t = 11$ and $p < 53$, $t = 12$ and $p < 38$, $t = 13$ and $p < 29$, $t = 14$ and $p < 23$, $t = 15$ and $p < 19$, $t = 16$ and $p < 16$, $t = 17$ and $p < 13$, $t = 18$ and $p < 12$, $t = 19$ and $p < 10$, $t = 20$ and $p < 9$, $t = 21, 22$ and $p < 8$, $t = 23, 24$ and $p < 7$, $t = 25, 26, 27$ and $p = 2, 3, 4, 5.$, $28 \leq t \leq 31$ and $p = 2, 3, 4.$, $32 \leq t \leq 39$ and $p = 2, 3.$, $40 \leq t \leq 62$ and $p = 2$.

Calculation for A_2

From the preceding discussion for every (p, t), we validated Theorem 3 and compiled a list of 570 potential exceptions. For these potential exceptions, we discover that sieve variation (Theorem 4.1) is true for the large majority of prime powers with the exception of those mentioned in next Theorem.

Calculation for A_2

From the preceding discussion for every (p, t), we validated Theorem 3 and compiled a list of 570 potential exceptions. For these potential exceptions, we discover that sieve variation (Theorem 4.1) is true for the large majority of prime powers with the exception of those mentioned in next Theorem.

Theorem

Let $t, q, r, p \in \mathbb{N}$ be such that q is a prime number, $t \geq 7$ and $p = q^r$. Suppose p and t assume none of the following values:

1. $2 \leq p \leq 16$ or $p = 19, 23, 25, 27, 31, 37, 43, 49, 61, 67, 79$ and $t = 7$;
2. $2 \leq p \leq 31$ or $p = 32, 37, 41, 43, 47, 83$ and $t = 8$;
3. $2 \leq p \leq 8$ or $p = 11, 16$ and $t = 9$;
4. $p = 2, 3, 4, 5, 7$ and $t = 10, 12$;
5. $p = 2, 3, 4$ and $t = 11$;
6. $p = 2$ and $t = 14, 15, 16, 18, 20, 24$.

Then $(p, t) \in A_2$.

References I

Cao, X., Wang, P. (2014). Primitive elements with prescribed trace. *AAECC* 25(5):339–345.

Chou, W. S., Cohen, S. D. (2001). Primitive elements with zero traces. *Finite Fields Appl.* 7(1):125–141.

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

Cohen, S. D., Presern, M. (2005). Primitive finite field elements with prescribed trace. *Southeast Asian Bull. Math.* 29(2):283–300.

Fan, S., Han, W. (2004). Character sums over galois rings and primitive polynomials over finite fields. *Finite Fields Appl.* 10(1):36–52.

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

References II

Gupta, A., Sharma, R. K., Cohen, S. D. (2018). Primitive element pairs with one prescribed trace over a *finite field. Finite Fields Appl.* 54:1–14.

Jungnickel, D., Vanstone, S. A. (1989). On primitive polynomials over finite fields. *J. Algebra* 124(2):337–353.

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

Sharma, H., Sharma, R.K. (2021). Existence of primitive pairs with prescribed traces over finite fields. *Commun. Algebra* 49(4):1773-1780.

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

Thank You