Commun. Math. Res.
doi: 10.4208/cmr.2021-0030

Vol. **38**, No. 2, pp. 184-205
May 2022

A Recursive Formula and an Estimation for a Specific Exponential Sum

Xiwang Cao and Liqin Qian*

School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, P.R. China.

Received 2 March 2021; Accepted 9 July 2021

Abstract. Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^s}$ be an extension of $\mathbb{F}_q$. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree n with $\gcd(n,q)=1$. We present a recursive formula for evaluating the exponential sum $\sum_{c\in\mathbb{F}_{q^s}}\chi^{(s)}(f(x))$. Let a and b be two elements in $\mathbb{F}_q$ with $a\neq 0$, u be a positive integer. We obtain an estimate for the exponential sum $\sum_{c\in\mathbb{F}^*_{q^s}}\chi^{(s)}(ac^u+bc^{-1})$, where $\chi^{(s)}$ is the lifting of an additive character χ of $\mathbb{F}_q$. Some properties of the sequences constructed from these exponential sums are provided too.

AMS subject classifications: 11T23

Key words: Exponential sums, finite fields, Dickson polynomials, sequences.

1 Introduction

Let $\mathbb{F}_q$ denote the finite field of characteristic p with q elements ($q=p^e$, $e\in\mathbb{N}$, the set of positive integers), and $\mathbb{F}_q^*$ be the nonzero elements of $\mathbb{F}_q$. Let $\mathbb{F}_q[x]$ be the polynomial ring with indeterminate x. For every positive integer s and a positive divisor t of s, the relative trace map from $\mathbb{F}_{q^s}$ to $\mathbb{F}_{q^t}$ is defined as

$$\mathrm{Tr}_t^s(c)=c+c^{q^t}+c^{q^{2t}}+\cdots+c^{q^{s-t}},\quad \forall c\in\mathbb{F}_{q^s}. \tag{1.1}$$

*Corresponding author. *Email addresses:* xwcao@nuaa.edu.cn (X. Cao), qianliqin_1108@163.com (L. Qian)

The function maps from $\mathbb{F}_q$ to $\mathcal{C}^*$, the set of nonzero complex numbers, defined by

$$\chi_a(c) = e^{2\pi\sqrt{-1}\mathrm{Tr}(ac)/p}, \quad \forall c \in \mathbb{F}_q$$

is called an additive character of $\mathbb{F}_q$. Let χ be an additive character of $\mathbb{F}_q$, and $f(x) \in \mathbb{F}_q[x]$. The sum

$$\mathcal{S}(f) = \sum_{c \in \mathbb{F}_q} \chi\big(f(c)\big)$$

is called the Weil Sum. Let g be a generator of the cyclic group $\mathbb{F}_q^*$, the function maps from $\mathbb{F}_q$ to $\mathcal{C}^*$ defined by

$$\psi(g^k) = e^{2\pi\sqrt{-1}k/(q-1)}, \quad k = 0,1,\ldots,q-2$$

is called a multiplicative character of $\mathbb{F}_q$. It is easy to see that ψ is a generator of the characteristic group of $\mathbb{F}_q^*$. For every multiplicative character ψ of $\mathbb{F}_q$ and a polynomial $f(x) \in \mathbb{F}_q[x]$, one can also define the following exponential sum:

$$\mathcal{T}(f) = \sum_{c \in \mathbb{F}_q} \psi\big(f(c)\big).$$

Here we extend the definition of ψ to the set $\mathbb{F}_q$ by setting $\psi(0) = 0$.

The problem of explicitly evaluating these sums, $\mathcal{S}(f), \mathcal{T}(f)$, is quite often difficult. On the other hand, the estimates of the absolute values of the sums are often appear in literature. Lidl and Niederreiter gave an overview of this area of research in the concluding remarks of [3, Chapter 5] (see also, [1,4,5,7–10]).

Using the technique of L-functions, one can prove the following results.

Theorem 1.1 ([3, Theorem 5.36]). *Let $f(x) \in \mathbb{F}_q[x]$ be of degree $n \geq 2$ with $\gcd(n,q) = 1$ and let χ be a nontrivial additive character of $\mathbb{F}_q$. Then there exist complex numbers $\omega_1, \omega_2, \ldots, \omega_{n-1}$, only depending on f and χ, such that for any positive integer s we have*

$$\sum_{\gamma \in \mathbb{F}_{q^s}} \chi^{(s)}\big(f(\gamma)\big) = -\omega_1^s - \omega_2^s - \cdots - \omega_{n-1}^s, \tag{1.2}$$

where $\chi^{(s)}(x) = \chi(\mathrm{Tr}_1^s(x))$ for all $x \in \mathbb{F}_{q^s}$ is the lifting of χ from $\mathbb{F}_q$ to $\mathbb{F}_{q^s}$.

Theorem 1.2 ([3, Theorem 5.39]). *Let ψ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$ and $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$ and*