Journal of Number Theory 154 (2015) 160–178

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Cyclotomy of Weil sums of binomials

Yves Aubry [a,b], Daniel J. Katz [c,*], Philippe Langevin [a]

[a] *Institut de Mathématiques de Toulon, Université de Toulon, 83957 La Garde Cedex, France*
[b] *Institut de Mathématiques de Marseille, CNRS-UMR 7373, Aix-Marseille Université, 13288 Marseille Cedex 9, France*
[c] *Department of Mathematics, California State University, Northridge, CA 91330, United States*

ARTICLE INFO

Article history:
Received 7 January 2014
Received in revised form 21 February 2015
Accepted 23 February 2015
Available online 3 April 2015
Communicated by D. Wan

MSC:
11T23
11L05
11T22

Keywords:
Weil sum
Character sum
Finite field
Cyclotomy

ABSTRACT

The Weil sum $W_{K,d}(a) = \sum_{x \in K} \psi(x^d + ax)$ where K is a finite field, ψ is an additive character of K, d is coprime to $|K^\times|$, and $a \in K^\times$ arises often in number-theoretic calculations, and in applications to finite geometry, cryptography, digital sequence design, and coding theory. Researchers are especially interested in the case where $W_{K,d}(a)$ assumes three distinct values as a runs through $K^\times$. A Galois-theoretic approach, combined with p-divisibility results on Gauss sums, is used here to prove a variety of new results that constrain which fields K and exponents d support three-valued Weil sums, and restrict the values that such Weil sums may assume.

* Corresponding author.
E-mail addresses: yves.aubry@univ-tln.fr (Y. Aubry), daniel.katz@csun.edu (D.J. Katz), langevin@univ-tln.fr (P. Langevin).

http://dx.doi.org/10.1016/j.jnt.2015.02.011
0022-314X/

1. Introduction

Let K be a finite field of characteristic p. Let ψ_K be the canonical additive character of K, that is, $\psi_K(x) = \exp(2i\pi \operatorname{Tr}_{K/\mathbb{F}_p}(x)/p)$ where $\operatorname{Tr}_{K/\mathbb{F}_p}$ is the absolute trace. *Weil sums* with ψ_K applied to binomials, that is, sums of the form $\sum_{x\in K} \psi_K(bx^j + cx^k)$, have been studied extensively from the early twentieth century to present [32,37,41,14,1,23,6,7,33,31,11,9,10]. We are interested in such sums when j and k are coprime to $|K^\times|$, in which case we reparameterize them to obtain sums of the form

$$\mathrm{W}_{K,d}(a) = \sum_{x\in K} \psi_K(x^d + ax) \tag{1}$$

with $\gcd(d, |K^\times|) = 1$ and $a \in K$. This definition will remain in force throughout the paper, and we shall always insist that $\gcd(d, |K^\times|) = 1$ whenever we write $\mathrm{W}_{K,d}$. The sums $\mathrm{W}_{K,d}(a)$ are always real algebraic integers [20, Theorem 3.1(a)], and furthermore, are all rational integers if and only if $d \equiv 1 \pmod{p-1}$ [20, Theorem 4.2]. Apart from arising often in number-theoretic calculations, these sums are also the key to problems in finite geometry, cryptography, digital sequence design, and coding theory, as discussed in [27, Appendix].

For a fixed K and d, we consider $\mathrm{W}_{K,d}(a)$ as a function of $a \in K^\times$, and are interested in how many different values it assumes as a runs through $K^\times$. $\mathrm{W}_{K,d}(a)$ with $a = 0$ is passed over, as it is the Weil sum of the monomial x^d, and since $x \mapsto x^d$ is a permutation of K, we always have $\mathrm{W}_{K,d}(0) = 0$. We call $\{\mathrm{W}_{K,d}(a) : a \in K^\times\}$ the *value set* of $\mathrm{W}_{K,d}$, and say that $\mathrm{W}_{K,d}$ is *v-valued* over K to mean that this set is of cardinality v.

If $d \equiv p^j \pmod{|K^\times|}$ for some j, we say that d is *degenerate over* K, because $\operatorname{Tr}_{K/\mathbb{F}_p}(x^d + ax) = \operatorname{Tr}_{K/\mathbb{F}_p}((1+a)x)$, and so the binomial effectively becomes zero (if $a = -1$) or a nonvanishing linear form (if $a \neq -1$). Thus if d is degenerate over K, one readily obtains for $a \in K$ that

$$\mathrm{W}_{K,d}(a) = \begin{cases} |K| & \text{if } a = -1, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

Helleseth [20, Theorem 4.1] shows that one always obtains a richer value set in the nondegenerate case.

Theorem 1.1. *(See Helleseth, 1976.) If d is nondegenerate over K, then $\mathrm{W}_{K,d}(a)$ takes at least three values as a runs through $K^\times$.*

Here we want to know when Weil sums of this form can be three-valued, and if so, what are the three values they may take. We indicate all known infinite families of three-valued examples, arranged according to analogy, in Table 1 below.

In several entries, we make use of the *p-adic valuation* of an integer a, denoted $\mathrm{val}_p(a)$, which is the maximum k such that $p^k \mid a$ (or ∞ if $a = 0$). We write "nondegenerate" in