Proof of a conjectured three-valued family of Weil sums of binomials

Daniel J. Katz, Philippe Langevin

Proof of a Conjectured Three-Valued Family of Weil Sums of Binomials

Daniel J. Katz[1] and Philippe Langevin[2]

[1] California State University, Northridge,
daniel.katz@csun.edu
[2] Institut de Mathématiques de Toulon, Université de Toulon.
langevin@univ-tln.fr

Abstract. We consider Weil sums of binomials of the form $W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax)$, where F is a finite field, $\psi\colon F \to \mathbb{C}$ is the canonical additive character, $\gcd(d, |F^\times|) = 1$, and $a \in F^\times$. If we fix F and d and examine the values of $W_{F,d}(a)$ as a runs through $F^\times$, we always obtain at least three distinct values unless d is degenerate (a power of the characteristic of F modulo $F^\times$). Choices of F and d for which we obtain only three values are quite rare and desirable in a wide variety of applications. We show that if F is a field of order 3^n with n odd, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $W_{F,d}(a)$ assumes only the three values 0 and $\pm 3^{(n+1)/2}$. This proves the 2001 conjecture of Dobbertin, Helleseth, Kumar, and Martinsen.

1 Introduction

We consider Weil sums of binomials of the form

$$W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax),$$

where F is a finite field of characteristic p and order q, $\psi\colon F \to \mathbb{C}$ is the canonical additive character, d is a positive integer with $\gcd(d, q-1) = 1$, and $a \in F$. These sums and their relatives are much-studied objects in number theory [15, 21, 7, 11, 2, 3, 16, 14, 6, 4, 5], and arise in applications to digital sequence design, cryptography, coding theory, and finite geometry, as detailed in [12, Appendix].

For classical applications in communications like radar or signal synchronization, one fixes F and d and considers the values of $W_{F,d}(a)$ as a runs through $F^\times$; we ignore $W_{F,d}(0)$, which is the Weil sum of the monomial x^d, and is trivially 0. In such situations, it is desirable that all the values of $W_{F,d}$ be as small in magnitude as possible. It is easy to calculate (see [12, Proposition 3.1]) that

$$\sum_{a \in F^\times} W_{F,d}(a)^2 = q^2,$$

which means that some $W_{F,d}(a) > \sqrt{q}$, and it is possible to find F and d such that no $W_{F,d}(a)$ is much larger than $\sqrt{q}$. Some of the best choices of F and d

for this purpose have the property that the number of distinct values, that is, $|\{W_{F,d}(a) : a \in F^\times\}|$ is small. However, we do exclude the case of *degenerate* d, that is, where d is congruent to a power of p modulo $q-1$, for then $\psi(x^d) = \psi(x)$, and our sum degenerates to the Weil sum of the monomial $(1-a)x$, with $W_{F,d}(1) = q$ (the largest possible magnitude for a Weil sum) and $W_{F,d}(a) = 0$ for $a \neq 1$. We say that $W_{F,d}$ is *v-valued* to mean that $|\{W_{F,d}(a) : a \in F^\times\}| = v$. The following fundamental result about how many values $W_{F,d}$ takes is due to Helleseth [9, Theorem 4.1].

Theorem 1. *$W_{F,d}$ is at at least three-valued if d is nondegenerate.*

Thus the smallest number of distinct values for an interesting Weil sum $W_{F,d}$ is three. From 1966 to the present, only ten infinite families of (F, d) pairs that produce three-valued Weil sums $W_{F,d}$ have been discovered; these are listed in [1, Table 1]. This contribution adds an eleventh three-valued infinite family by proving the following conjecture [8, Conjecture B].

Conjecture 1 (Dobbertin-Helleseth-Kumar-Martinsen, 2001). If F is a finite field of order $q = 3^n$ with n odd and $n > 1$, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $W_{F,d}$ is three-valued with

$$W_{F,d}(a) = \begin{cases} 0 & \text{for } q - q/3 - 1 \text{ values of } a \in F^\times, \\ \pm\sqrt{3q} & \text{for } (q \pm \sqrt{3q})/6 \text{ values of } a \in F^\times. \end{cases}$$

The original conjecture used the exponent $d_o = 2 \cdot 3^{r_o} + 1$ with $4r_0 \equiv -1 \pmod{n}$ where we use d. But note that our $d \equiv 3^r d_o \pmod{q-1}$, so that the canonical additive character has $\psi(x^d) = \psi(x^{d_0})$ for all $x \in F$, and so $W_{F,d} = W_{F,d_o}$. Also note that the condition $4r \equiv 1 \pmod{n}$ does indeed make $d = 3^r + 2$ coprime to $q - 1 = 3^n - 1$,[3] so that the family of three-valued Weil sums described in the conjecture meets the conditions we set down at the beginning of this section.

The rest of this paper is organized as follows. In Section 2, we show that the proof of Conjecture 1 can be deduced if one knows two things: the sum of fourth powers of the values $W_{F,d}(a)$, and the extent of 3-divisibility of these same values. Accordingly, the sum of fourth powers is determined in Section 3, and the 3-divisibility is determined in Sections 4–5. After some facts from the general theory of divisibility of character sums in Section 4, we present a short computer-assisted proof of the divisibility result that we need in Section 5. A technical computer-free proof is available in the full version of the paper [13].

2 Method of Proof

As in the Introduction, we assume that F is a finite field, that $\psi\colon F \to \mathbb{C}$ is the canonical additive character, that d is a positive integer with $\gcd(d, |F^\times|) = 1$,

[3] For there is some positive integer a with $4r = an + 1$, and then $\gcd(3^r + 2, 3^n - 1)$ is a divisor of $\gcd(3^{4r} - 16, 3^{an+1} - 3) = \gcd(3 - 16, 3^{an+1} - 3)$, which is in turn a divisor of 13. Thus $\gcd(3^r + 2, 3^n - 1) \mid 13$, and yet $3^r + 2 \equiv 3, 5, \text{ or } 11 \pmod{13}$ for every r.

and that

$$W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax)$$

for $a \in F$. Here we show that Conjecture 1 can be deduced from two propositions, whose proofs constitute the remaining sections of this paper. This way to a proof had been proposed in [8, p. 1475] by the authors of Conjecture 1, who noted that they had made some progress with this program, but they did not present details of their partial results. The first proposition we need entails an exact calculation of the fourth power moment of the Weil sum.

Proposition 1. *If F is a finite field of order $q = 3^n$ with n odd, and $d = 3^r + 2$ with $\gcd(d, q-1) = \gcd(r, n) = 1$, then*

$$\sum_{a \in F^\times} W_{F,d}(a)^4 = 3q^3.$$

The second proposition gives the 3-divisibility of the values of the Weil sum.

Proposition 2. *If F is a finite field of order $q = 3^n$ with n odd, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $W_{F,d}(a)$ is a rational integer divisible by $\sqrt{3q}$ for each $a \in F$.*

These combine to give a proof of Conjecture 1 as follows.

Theorem 2. *If F is a finite field of order $q = 3^n$ with n odd $n > 1$, and $d = 3^r + 2$ with $4r \equiv 1 \pmod{n}$, then $W_{F,d}$ is three-valued with*

$$W_{F,d} = \begin{cases} 0 & \text{for } q - q/3 - 1 \text{ values of } a \in F^\times, \\ +\sqrt{3q} & \text{for } (q + \sqrt{3q})/6 \text{ values of } a \in F^\times, \text{ and} \\ -\sqrt{3q} & \text{for } (q - \sqrt{3q})/6 \text{ values of } a \in F^\times. \end{cases}$$

Proof. The first two power moments of the Weil sum are well known (see, e.g., [12, Proposition 3.1]) as

$$\sum_{a \in F^\times} W_{F,d}(a) = q \quad \text{and} \quad \sum_{a \in F^\times} W_{F,d}(a)^2 = q^2. \tag{1}$$

Now note that Proposition 1 applies since the condition $4r \equiv 1 \pmod{n}$ clearly makes $\gcd(r, n) = 1$ and also makes $\gcd(d, q-1) = 1$ by footnote 1 in the Introduction. Then (1) and Proposition 1 show that

$$\sum_{a \in F^\times} W_{F,d}(a)^2 (W_{F,d}^2 - 3q) = 0,$$

and Proposition 2 shows that the individual terms of this sum are nonnegative. Thus all terms must be zero, and so $W_{F,d}(a) \in \{0, \pm\sqrt{3q}\}$ for all $a \in F^\times$. If we let N_0, N_+, and N_- denote the number of $a \in F^\times$ such that $W_{F,d}(a)$ equals 0, $+\sqrt{3}$, and $-\sqrt{3}$, respectively, then the total count of $F^\times$, along with (1), gives the three equations $N_0 + N_+ + N_- = q - 1$, $\sqrt{3q}N_+ - \sqrt{3q}N_- = q$, and $3qN_+ + 3qN_- = q^2$, whence we deduce the claimed frequencies.

3 Fourth Power Moment

The purpose of this section is to prove Proposition 1, which requires us to compute precisely the fourth power moment of our Weil sum. Throughout this section, we assume that F is a finite field of characteristic p and order $q = p^n$, and that $\mathrm{Tr}\colon F \to \mathbb{F}_p$ is the absolute trace. We let $\epsilon\colon \mathbb{F}_p \to \mathbb{C}$ be the canonical additive character of $\mathbb{F}_p$, that is, $\epsilon(x) = \exp(2\pi i x/p)$, and we let $\psi\colon F \to \mathbb{C}$ be the canonical additive character of F, that is, $\psi(x) = \epsilon(\mathrm{Tr}(x))$. We also assume that $d = 2 + p^r$ for some nonnegative integer r such that $\gcd(d, q-1) = 1$, and define the Weil sum as usual:

$$W_{F,d}(a) = \sum_{x \in F} \psi(x^d - ax).$$

We use the abbreviation $\bar{x}$ for x^{p^r}, so that $x^d = \bar{x}x^2$.

If we consider F as a $\mathbb{F}_p$-vector space with $\mathbb{F}_p$-basis $\beta_1, \ldots, \beta_n$, and expand $x \in F$ as $x = x_1\beta_1 + \cdots + x_n\beta_n$ with $x_1, \ldots, x_n \in \mathbb{F}_p$, then $\mathrm{Tr}(x^d)$ is a cubic form in $x_1, \ldots, x_n$ over $\mathbb{F}_p$. This kind of object is considered in [18], which inspired the method we use here.

We define a symmetric $\mathbb{F}_p$-trilinear form on F,

$$\langle x, y, z\rangle = \mathrm{Tr}(\bar{x}yz + x\bar{y}z + xy\bar{z}), \tag{2}$$

and we express the fourth power of our Weil sum in terms of this form.

Lemma 1. *We have*

$$\sum_{a \in F^\times} W_{F,d}(a)^4 = q \sum_{x,y,z} \epsilon(\langle x, y, x\rangle + \langle x, y, y\rangle + 2\langle x, y, z\rangle).$$

Proof. Since $W_{F,d}(0) = 0$, we change nothing by summing $W_{F,d}(a)$ over all $a \in F$, so

$$\begin{aligned}
\sum_{a \in F^\times} W_{F,d}(a)^4 &= \sum_{a,t,u,v,w \in F} \psi(t^d + u^d + v^d + w^d - a(t+u+v+w)) \\
&= q \sum_{\substack{t,u,v,w \in F \\ t+u+v+w=0}} \psi(t^d + u^d + v^d + w^d) \\
&= q \sum_{x,y,z \in F} \psi((x+y+z)^d - (x+z)^d - (y+z)^d + z^d),
\end{aligned}$$

where we have reparameterized with $t = x+y+z$, $u = -(x+z)$, $v = -(y+z)$, and $w = z$ in the last step, and used the fact that our condition $\gcd(d, q-1) = 1$ makes d odd when we are in odd characteristic. Now use the fact that $s^d = s^2\bar{s}$ to expand out $(x+y+z)^d - (x+z)^d - (y+z)^d + z^d$ to obtain

$$2x\bar{x}y + x^2\bar{y} + 2xy\bar{y} + \bar{x}y^2 + 2\bar{x}yz + 2x\bar{y}z + 2xy\bar{z},$$

so that the trace of this quantity is $\langle x, y, x\rangle + \langle x, y, y\rangle + 2\langle x, y, z\rangle$, which completes the proof, since $\psi = \epsilon \circ \mathrm{Tr}$.

If we fix x and y, then $z \mapsto \langle x, y, z\rangle$ is an $\mathbb{F}_p$-linear form. Let the kernel K be the set of $(x, y) \in F^2$ that make this the zero functional:

$$K = \{(x, y) \in F^2 : \langle x, y, z\rangle = 0 \text{ for every } z \in F\}.$$

Then a consequence of our previous result is that the fourth power moment is related to $|K|$.

Corollary 1. *We have*

$$\sum_{a\in F^\times} W_{F,d}(a)^4 = q^2 \,|K|\,.$$

Proof. From Lemma 1, we have

$$\sum_{a\in F^\times} W_{F,d}(a)^4 = q \sum_{(x,y)\in F^2} \epsilon(\langle x, y, x\rangle + \langle x, y, y\rangle) \sum_{z\in F} \epsilon(\langle x, y, z\rangle).$$

If $(x, y) \notin K$, then $z \mapsto \langle x, y, z\rangle$ is a nontrivial $\mathbb{F}_p$-linear functional, so as z runs through F, the value of $\langle x, y, z\rangle$ runs through $\mathbb{F}_p$, taking each value equally often, thus making the sum over z vanish. So we can restrict our sum over (x, y) to K to get

$$\begin{aligned}\sum_{a\in F^\times} W_{F,d}(a)^4 &= q \sum_{(x,y)\in K} \epsilon(\langle x, y, x\rangle + \langle x, y, y\rangle) \sum_{z\in F} \epsilon(\langle x, y, z\rangle) \\ &= q \sum_{(x,y)\in K} \epsilon(0 + 0) \sum_{z\in F} \epsilon(0) \\ &= q^2 \,|K|\,,\end{aligned}$$

where we use the definition of K in the middle step.

Now it remains to compute the size of K. First we find a useful characterization of K.

Lemma 2. *We have* $K = \{(x, y) \in F^2 : \bar{\bar{x}}\bar{y} + \bar{x}\bar{\bar{y}} + xy = 0\}$.

Proof. We note that $\mathrm{Tr}(\bar{s}) = \mathrm{Tr}(s)$ for any $s \in F$, because $\mathrm{Tr}(s^p) = \mathrm{Tr}(s)$, which means that the definition (2) of our trilinear form is equivalent to

$$\begin{aligned}\langle x, y, z\rangle &= \mathrm{Tr}(\overline{\bar{x}yz} + \overline{x\bar{y}z} + xy\bar{z}) \\ &= \mathrm{Tr}((\bar{\bar{x}}\bar{y} + \bar{x}\bar{\bar{y}} + xy)\bar{z}),\end{aligned}$$

and since Tr is a nonzero $\mathbb{F}_p$-functional of F and $z \mapsto \bar{z}$ is an automorphism of F, our kernel K is the set of (x, y) that make $\bar{\bar{x}}\bar{y} + \bar{x}\bar{\bar{y}} + xy = 0$.

Lemma 3. *If our field F is of characteristic $p = 3$ and order $q = 3^n$ with n odd, and if our exponent $d = 2 + 3^r$ has $\gcd(r, n) = 1$, then $|K| = 3q$.*

Proof. From the expression for K in Lemma 2, it is clear that all $(x, 0)$ and $(0, y) \in F^2$ lie in K, thus accounting for $2q - 1$ points. So it remains to show that there are $q + 1$ points $(x, y) \in K$ with $x, y \neq 0$, and we reparameterize the condition in Lemma 2 using $x = wy$ to obtain

$$(\bar{w} + \bar{w})(\bar{y}\bar{y}) + wy^2 = 0,$$

and so we want to show that $q + 1$ points (w, y) with $w, y \neq 0$ satisfy this equation, or equivalently, we want to show that

$$S = \{(w, y) \in (F^\times)^2 : y^{2-3^r-3^{2r}} = -w^{3^r-1}(w^{3^{2r}-3^r} + 1)\},$$

has $q+1$ elements. Note that $\gcd(2-3^r-3^{2r}, q-1) = \gcd((1-3^r)(2+3^r), 3^n-1) = \gcd((3^r-1)d, 3^n-1)$, and recall that d is coprime to $3^n - 1$, so that our greatest common divisor is $3^{\gcd(r,n)} - 1 = 2$. Thus $|S| = |T|$, where

$$T = \{(v, w) \in (F^\times)^2 : v^2 = -w^{3^r-1}(w^{3^{2r}-3^r} + 1)\},$$

so it suffices to show that $|T| = q + 1$. Note that $w^{3^{2r}-3^r} + 1$ is never 0, because this would imply that -1 is a quadratic residue in F, which is it not, since $[F : \mathbb{F}_3] = n$ is odd. We compute $|T|$ using the quadratic character η of F.

$$|T| = \sum_{w \in F^*} \Big(1 + \eta(-w^{3^r-1}(w^{3^{2r}-3^r} + 1))\Big) = (q-1) - \sum_{w \in F^*} \eta(w^{3^{2r}-3^r} + 1),$$

and then note that $\gcd(3^{2r}-3^r, q-1) = \gcd(3^r(3^r-1), 3^n-1) = 3^{\gcd(r,n)}-1 = 2$, so that

$$|T| = (q-1) - \sum_{u \in F^*} \eta(u^2 + 1) = q - \sum_{u \in F} \eta(u^2 + 1) = q + 1,$$

where we use the well known [20, Theorem 5.48] evaluation of the last character sum.

Corollary 1 and Lemma 3 together immediately prove Proposition 1: the fourth power moment of our Weil sum is $3q^3$.

4 Divisibility: General Remarks

It only remains to prove Proposition 2. The fact that the Weil sums are in $\mathbb{Z}$ follows from a result of Helleseth [9, Theorem 4.2]. To prove the result on divisibility, we use a well known technique that relies on Stickelberger's Theorem (or alternatively, one can use McEliece's Theorem). To state the principle, we use the p-adic valuation, written v_p, for a prime $p \in \mathbb{Z}$, and we extend v_p to $\mathbb{Q}(e^{2\pi i/p})$ so that $v_p(e^{2\pi i/p} - 1) = 1/(p-1)$. Also, for b and n positive integers, we use the b-ary weight function $w_{b,n} \colon \mathbb{Z}/(b^n - 1)\mathbb{Z} \to \mathbb{Z}$, which computes the sum of the digits in the b-ary expansion of an $a \in \mathbb{Z}/(b^n - 1)\mathbb{Z}$. That is, if we write an element $a \in \mathbb{Z}/(b^n - 1)\mathbb{Z}$ as $a = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} a_i b^i$ with the elements b^i in the group $\mathbb{Z}/(b^n - 1)\mathbb{Z}$ and each coefficient $a_i \in \{0, 1, \ldots, b-1\} \subseteq \mathbb{Z}$ with at least one $a_i < b - 1$, then $w_{b,n}(a) = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} a_i$.

Proposition 3. *Let F be of characteristic p and order p^n, and let*

$$m = (p-1)n + \min_{\substack{j \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ j \neq 0}} w_{p,n}(dj) - w_{p,n}(j).$$

Then $v_p(W_{F,d}(a)) \geq m/(p-1)$ for all $a \in F$, with equality for some $a \in F$.

Proof. Lemma 4.1 of [1] tells us that

$$\min_{a \in F^*} v_p(W_{F,d}(a)) = \min_{\substack{\chi \in \widehat{F^*} \\ \chi \neq 1}} v_p(\tau(\chi)\tau(\bar{\chi}^d)), \tag{3}$$

where $\widehat{F^*}$ is the group of multiplicative characters of F, with the principal character denoted by 1, and for any $\chi \in \widehat{F^*}$, we have the Gauss sum

$$\tau(\chi) = \sum_{a \in F^*} \psi(a)\chi(a).$$

If we let $\omega \colon F^* \to \mathbb{C}$ be the Teichmüller character, then Stickelberger's Theorem [17, Theorem 2.1] tells us that for $j \in \mathbb{Z}/(p^n-1)\mathbb{Z}$, we have $v_p(\tau(\omega^j)) = w_{p,n}(-j)/(p-1)$. Thus, if we express the nontrivial multiplicative characters of F as powers of the Teichmüller character, i.e., $\chi = \omega^j$ for $j \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ with $j \neq 0$, then equation (3) becomes $\min_{a \in F^*} v_p(W_{F,d}(a)) = m/(p-1)$, where

$$m = \min_{\substack{j \in \mathbb{Z}/(p^n-1)\mathbb{Z} \\ j \neq 0}} w_{p,n}(-j) + w_{p,n}(dj)m,$$

and we get the formula for m in the statement of this proposition by using the fact that if a nonzero $j \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ has p-ary expansion $\sum_{i \in \mathbb{Z}/n\mathbb{Z}} j_i p^i$, then the element $-j$ has p-ary expansion $\sum_{i \in \mathbb{Z}/n\mathbb{Z}} (p-1-j_i)p^i$, so that $w_{p,n}(-j) = (p-1)n - w_{p,n}(j)$.

Given $j \in \mathbb{Z}/(p^n-1)\mathbb{Z}$, we use a modular add-and-carry method inspired by [10] to help compute the weight dj that appear in the formula in Proposition 3. The basic result we need is a technical result related to [10, Lemma 3].

Lemma 4. *Let b and n be positive integers with $b > 1$. Suppose that we have $s_i, t_i \in \mathbb{Z}$ for every $i \in \mathbb{Z}/n\mathbb{Z}$, such that $\sum_{i \in \mathbb{Z}/n\mathbb{Z}} s_i b^i \equiv \sum_{i \in \mathbb{Z}/n\mathbb{Z}} t_i b^i \pmod{b^n - 1}$. Then there is a unique collection of integers $\{c_i\}_{i \in \mathbb{Z}/n\mathbb{Z}}$ such that*

$$s_i + c_{i-1} = t_i + bc_i, \tag{4}$$

for all $i \in \mathbb{Z}/n\mathbb{Z}$: these are in fact

$$c_i = \frac{1}{b^n - 1} \sum_{j=0}^{n-1} (s_{j+i+1} - t_{j+i+1})b^j. \tag{5}$$

for $i \in \mathbb{Z}/n\mathbb{Z}$. Furthermore

$$\sum_{i \in \mathbb{Z}/n\mathbb{Z}} c_i = \frac{1}{b-1} \sum_{i \in \mathbb{Z}/n\mathbb{Z}} (s_i - t_i). \tag{6}$$

Proof. The c_i defined in (5) are indeed integers, because the sum is congruent modulo $b^n - 1$ to $b^{-(i+1)} \sum_{j \in \mathbb{Z}/n\mathbb{Z}} (s_j - t_j) b^i$, which vanishes modulo $b^n - 1$ by assumption. Replace i in (4) with $j + i + 1$, multiply both sides by b^j, and then sum this for j from 0 to $n - 1$, then rearrange and divide by $b^n - 1$ to obtain (5). Conversely, replace i with $i - 1$ in (5), and subtract from this b times (5) (with i unchanged) to obtain (4). Finally, sum (4) for all $i \in \mathbb{Z}/n\mathbb{Z}$, rearrange, and divide by $b - 1$ to obtain (6).

For the rest of this paper, we assume that n is odd and $d = 2 + 3^r$ where $4r \equiv 1 \pmod{n}$, and we write w for $w_{3,n}$. By Proposition 3, we will complete our proof of Proposition 2 if we show that

$$n + w(dx) - w(x) > 0, \tag{7}$$

for all nonzero $x \in \mathbb{Z}/(3^n - 1)\mathbb{Z}$.

5 Computer-Assisted Proof of Divisibility

In this section, we use a graph-theoretic formulation as in [19] to provide a computational verification of (7) (which then secures Proposition 2) by means of the algorithms of Tarjan and Bellman-Ford. We continue to assume that n is odd, that $d = 2 + 3^r$ with $4r \equiv 1 \pmod{n}$, and we use $w(a)$ to denote the sum of the digits in the ternary expansion of $a \in \mathbb{Z}/(3^n - 1)\mathbb{Z}$. (Thus $w(a)$ here is $w_{3,n}(a)$ per the definition given just before Proposition 3.)

To verify (7), we let x be a given nonzero element of $\mathbb{Z}/(3^n - 1)\mathbb{Z}$, and set $y = dx$, and then our goal is to show

$$n + w(y) - w(x) > 0. \tag{8}$$

For each $i \in \mathbb{Z}/n\mathbb{Z}$, we let $x_i, y_i \in \{0, 1, 2\} \subseteq \mathbb{Z}$ such that $x = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} x_i 3^i$ and $y = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} y_i 3^i$. Since $y = dx$ with $d = 2 + 3^r$, we can also write $y = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} (2x_i + x_{i-r}) 3^i$. Then by Lemma 4, there are integers c_i for $i \in \mathbb{Z}/n\mathbb{Z}$ such that

$$y_i + 3c_i = 2x_i + x_{i-r} + c_{i-1} \tag{9}$$

for every $i \in \mathbb{Z}/n\mathbb{Z}$.

We now set $X_i = x_{ri}$, $Y_i = y_{ri}$, and $C_i = c_{ri}$ for each $i \in \mathbb{Z}/n\mathbb{Z}$, and use the fact that $4r \equiv 1 \pmod{n}$ to reparameterize (9) with $i = rj$ to obtain

$$Y_j + 3C_j = 2X_j + X_{j-1} + C_{j-4}. \tag{10}$$

Note that r no longer explicitly appears in our formula. Since $Y_j \in \{0, 1, 2\}$ for every j, we see that

$$C_j = \left\lfloor \frac{2X_j + X_{j-1} + C_{j-4}}{3} \right\rfloor. \tag{11}$$

We sum (10) over all $j \in \mathbb{Z}/n\mathbb{Z}$ to obtain

$$\sum_{j\in\mathbb{Z}/n\mathbb{Z}} Y_j + 2\sum_{j\in\mathbb{Z}/n\mathbb{Z}} C_j = 3\sum_{j\in\mathbb{Z}/n\mathbb{Z}} X_j, \tag{12}$$

and then note that $\sum_{j\in\mathbb{Z}/n\mathbb{Z}} X_j = \sum_{i\in\mathbb{Z}/n\mathbb{Z}} x_i = w(x)$ and $\sum_{j\in\mathbb{Z}/n\mathbb{Z}} Y_j = w(y)$ to get

$$\sum_{j\in\mathbb{Z}/n\mathbb{Z}} C_j = \frac{3w(x) - w(y)}{2}.$$

Since $0 \le w(x), w(y) < 2n$, we see that there are $k, \ell \in \mathbb{Z}/n\mathbb{Z}$ with $C_k \ge 0$ and $C_\ell \le 2$. Then one can use (11) and the fact that $X_i \in \{0,1,2\}$ for all $i \in \mathbb{Z}/n\mathbb{Z}$ to see that $C_{k+4} \ge 0$ and $C_{\ell+4} \le 2$. Continuing in this fashion (and recalling that $4r \equiv 1 \pmod{n}$), we see that $C_j \in \{0,1,2\}$ for every $j \in \mathbb{Z}/n\mathbb{Z}$.

We again note that $w(x) = \sum_{j\in\mathbb{Z}/n\mathbb{Z}} X_j$ and $w(y) = \sum_{j\in\mathbb{Z}/n\mathbb{Z}} Y_j$, and employ (12) to see that (8) (which is our goal) is equivalent to

$$\sum_{j\in\mathbb{Z}/n\mathbb{Z}} (1 + 2(X_j - C_j)) \ge 0, \tag{13}$$

where the strict inequality has been replaced by a non-strict one inasmuch as the left hand side is always odd (since n is odd). Now our goal is to prove (13).

We consider a directed graph with 3^6 vertices,

$$(\xi, \gamma) = (\xi_0, \xi_1, \gamma_0, \gamma_1, \gamma_2, \gamma_3) \in \{0,1,2\}^6,$$

with an edge $(\xi, \gamma) \to (\xi', \gamma')$ if and only if

$$\xi_0' = \xi_1, \qquad \gamma_0' = \gamma_1, \quad \gamma_1' = \gamma_2, \quad \gamma_2' = \gamma_3, \quad \text{and} \qquad \gamma_3' = \left\lfloor \frac{\xi_0 + 2\xi_1 + \gamma_0}{3} \right\rfloor.$$

If we write the sextuple $T_j = (X_{j-1}, X_j, C_{j-4}, C_{j-3}, C_{j-2}, C_{j-1})$ for each $j \in \mathbb{Z}/n\mathbb{Z}$, then the sequence $T_0, T_1, \ldots, T_{n-1}, T_0$ traces a directed cycle of length n in our directed graph: the first four conditions for an edge are immediately satisfied by the structure of T_j and T_{j+1}, while the last condition is satisfied because of (11). Furthermore, if we attach to each directed edge a cost

$$\kappa((\xi, \gamma), (\xi', \gamma')) = 1 + 2(\xi_1 - \gamma_0),$$

then the total cost for our directed cycle is equal to $\sum_{j\in\mathbb{Z}/n\mathbb{Z}}(1 + 2(X_j - C_j))$. Thus to verify (13) (which secures Proposition 2), it suffices to show that the graph does not contain any *absorbent circuit*, that is, a circuit of strictly negative cost. The graph is of order 729, with 2187 edges. We apply Tarjan's algorithm to split the graph in 258 strongly connected components. Each is trivial (singleton without circuit) except two components having orders 2 and 471. We apply the Bellman-Ford algorithm to prove the non-existence of an absorbent circuit.

References

1. Y. Aubry, D. J. Katz, and P. Langevin. Cyclotomy of Weil sums of binomials. *arXiv*, 1312.3889 [math.NT], 2013.
2. L. Carlitz. A note on exponential sums. *Math. Scand.*, 42(1):39–48, 1978.
3. L. Carlitz. Explicit evaluation of certain exponential sums. *Math. Scand.*, 44(1):5–16, 1979.
4. T. Cochrane and C. Pinner. Stepanov's method applied to binomial exponential sums. *Q. J. Math.*, 54(3):243–255, 2003.
5. T. Cochrane and C. Pinner. Explicit bounds on monomial and binomial exponential sums. *Q. J. Math.*, 62(2):323–349, 2011.
6. R. S. Coulter. Further evaluations of Weil sums. *Acta Arith.*, 86(3):217–226, 1998.
7. H. Davenport and H. Heilbronn. On an exponential sum. *Proc. London Math. Soc. (2)*, 41(6):449–453, 1936.
8. H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen. Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inform. Theory*, 47(4):1473–1481, 2001.
9. T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.
10. H. D. L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields Appl.*, 7(2):253–286, 2001.
11. A. A. Karatsuba. On estimates of complete trigonometric sums. *Mat. Zametki*, 1:199–208, 1967. trans. in *Math. Notes* **1** (1967), no. 2, 133–139.
12. D. J. Katz. Weil sums of binomials, three-level cross-correlation, and a conjecture of Helleseth. *J. Combin. Theory Ser. A*, 119(8):1644–1659, 2012.
13. D. J. Katz and P. Langevin. Proof of a conjectured three-valued family of weil sums of binomials. *arXiv*, 1409.2459 [math.NT], 2014.
14. N. Katz and R. Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.
15. H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.
16. G. Lachaud and J. Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987.
17. S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.
18. P. Langevin and P. Solé. Kernels and defaults. In *Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997)*, volume 225 of *Contemp. Math.*, pages 77–85. Amer. Math. Soc., Providence, RI, 1999.
19. G. Leander and P. Langevin. On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 410–418. World Sci. Publ., Hackensack, NJ, 2008.
20. R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
21. I. M. Vinogradov. Some trigonometrical polynomials and their applications. *C. R. Acad. Sci. URSS*, (6):249–254, 1933.