

# THE WELCH FUNCTION IS NOT THIRD-ORDER SUM-FREE

DEEP BHATTACHARJEE

**ABSTRACT.** Let  $n = 2m + 1$ . Hou and Zhao conjectured that for  $n \geq 7$  the Welch function  $X^{2^m+3}$  on  $\mathbb{F}_{2^n}$  sums to zero over some three-dimensional affine subspace, that is, it is not third-order sum-free. We prove this. The proof counts exactly the elements  $x$  for which some subspace spanned by 1,  $x$  and a third element gives a zero sum: there are  $(2^n + 1 - 3K_n)/4$  of them, where  $K_n$  is a binary Kloosterman sum.

## 1. INTRODUCTION

A function  $f: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$  is *kth order sum-free* if  $\sum_{a \in A} f(a) \neq 0$  for every  $k$ -dimensional affine subspace  $A$  of  $\mathbb{F}_{2^n}$  over  $\mathbb{F}_2$ . Carlet introduced this notion [3, 2]; for  $k = 2$  it is the APN property. Throughout,  $n = 2m + 1$  is odd,  $q = 2^n$ ,  $F = \mathbb{F}_q$  and  $\text{Tr}: F \rightarrow \mathbb{F}_2$  is the absolute trace. The *Welch function* is

$$W_n(X) = X^{2^m+3}.$$

It is APN [5], and decimating a binary  $m$ -sequence by  $2^m + 3$  gives a three-valued cross-correlation, as Welch conjectured [1]. For  $m \geq 2$  it has algebraic degree 3, so the first open question about its higher-order sum-freeness is the third order. For  $m = 2$  the Welch function is  $X^7 = X^{2^3-1}$ , which is third-order sum-free by a result of Carlet [3, Proposition 1]. Hou and Zhao [6] reduced the question to a family of linearized polynomials, computed it for  $7 \leq n \leq 15$ , and proposed the following statement [6, Conjecture 4.10].

**Conjecture 1.** For  $n = 2m + 1 \geq 7$ , the Welch function on  $\mathbb{F}_{2^n}$  is not third-order sum-free.

We prove Conjecture 1. The reduction of Hou and Zhao goes through the polynomial

$$(1.1) \quad g(X, Y) = Y^{2^m}(X^2 + X) + Y^2(X^{2^m} + X) + Y(X^{2^m} + X^2).$$

For  $x \in F$  let  $Z(x) = \{y \in F : g(x, y) = 0\}$ . Since  $g(x, Y)$  is an additive polynomial in  $Y$ ,  $Z(x)$  is a vector space over  $\mathbb{F}_2$ , and it contains 1 and  $x$ . By Lemma 2.3 below,  $W_n$  fails to be third-order sum-free exactly when  $\dim_{\mathbb{F}_2} Z(x) \geq 3$  for some  $x \in F \setminus \mathbb{F}_2$ . Our main result decides this dimension for every  $x$ .

**Theorem 1.1.** Let  $n = 2m + 1 \geq 3$  and  $x \in F \setminus \mathbb{F}_2$ , and put  $u = x^{2^m}$ . Then  $\dim_{\mathbb{F}_2} Z(x) \in \{2, 3\}$ , and  $\dim_{\mathbb{F}_2} Z(x) = 3$  if and only if

$$\text{Tr}\left(\frac{1}{x+u}\right) = 1 \quad \text{and} \quad \text{Tr}\left(\frac{xu}{x+u}\right) = 1.$$

Let

$$K_n = \sum_{z \in F^*} (-1)^{\text{Tr}(z+z^{-1})}$$

2020 *Mathematics Subject Classification.* Primary 11T06; Secondary 11T23, 94A60.

*Key words and phrases.* sum-free functions, Welch function, almost perfect nonlinear functions, Kloosterman sums, linearized polynomials.

Corresponding author: [d.bhattacharjee@erl-forschung.de](mailto:d.bhattacharjee@erl-forschung.de); ORCID [0000-0003-0466-750X](https://orcid.org/0000-0003-0466-750X).

be the Kloosterman sum of  $F$ . The conditions of Theorem 1.1 turn the count of the elements  $x$  with  $\dim Z(x) = 3$  into Kloosterman sums.

**Theorem 1.2.** *Let  $n = 2m+1 \geq 3$ , and let  $N_n$  be the number of  $x \in F \setminus \mathbb{F}_2$  with  $\dim_{\mathbb{F}_2} Z(x) = 3$ . Then*

$$N_n = \frac{2^n + 1 - 3K_n}{4}.$$

By Weil's bound [8] (see also [7, Chapter 5]),  $|K_n| \leq 2 \cdot 2^{n/2}$ . Hence

$$N_n \geq \frac{2^n + 1 - 6 \cdot 2^{n/2}}{4} = \frac{(2^{n/2} - 3)^2 - 8}{4} > 0 \quad \text{for } n \geq 7.$$

**Corollary 1.3.** *Conjecture 1 is true. More precisely, for  $n = 2m+1 \geq 5$  the Welch function sums to zero over exactly*

$$\frac{N_n(2^n - 1)}{42}$$

*three-dimensional linear subspaces of  $F$ , and over exactly  $2^{n-3}$  times as many three-dimensional affine subspaces. This number is positive for every  $n \geq 7$  and is zero for  $n = 5$ .*

By a theorem of Carlitz [4] (see also [7, Chapter 5]),  $K_n = -(\omega^n + \bar{\omega}^n)$  with  $\omega = (-1 + \sqrt{-7})/2$ , because  $K_1 = 1$ . So  $K_0 = -2$ ,  $K_1 = 1$  and  $K_n = -K_{n-1} - 2K_{n-2}$ , which gives Table 1. Hou and Zhao [6, Corollary 4.9] showed that  $\dim Z(x) = 3$  for some  $x \in F \setminus \mathbb{F}_2$  if and only if the polynomial  $\det D^*(X)$  built from a Dickson matrix has more than two roots in  $F$ ; the number of its roots in  $F$  is  $2 + N_n$ . For  $5 \leq n \leq 15$  these are the values Hou and Zhao computed [6, Table 1].

TABLE 1. The Kloosterman sum  $K_n$ , the count  $N_n$  of Theorem 1.2 and the number  $2 + N_n$  of roots of  $\det D^*(X)$  in  $\mathbb{F}_{2^n}$ .

| $n$ | $K_n$ | $N_n$  | $2 + N_n$ |
|-----|-------|--------|-----------|
| 5   | 11    | 0      | 2         |
| 7   | -13   | 42     | 44        |
| 9   | -5    | 132    | 134       |
| 11  | 67    | 462    | 464       |
| 13  | -181  | 2184   | 2186      |
| 15  | 275   | 7986   | 7988      |
| 17  | -101  | 32844  | 32846     |
| 19  | -797  | 131670 | 131672    |
| 21  | 2795  | 522192 | 522194    |

The proof of Theorem 1.1 uses the automorphism  $\rho(z) = z^{2^{m+1}}$  of  $F$ , whose square is the Frobenius map  $z \mapsto z^2$  and whose inverse is  $z \mapsto z^{2^m}$ . Applying  $\rho$  to the equation  $g(x, y) = 0$  and eliminating  $y^{2^m}$  produces an additive polynomial of degree 8 in  $y$ . Its roots form a three-dimensional space  $V$  that always lies in  $F$  and contains  $Z(x)$ , and a linear map built from  $g(x, \cdot)$  moves  $V$  into  $Z(x)$ . Whether  $Z(x) = V$  is then decided by two elements of  $\mathbb{F}_2$ , and both turn out to be traces of explicit rational functions of  $x$  and  $u$ , because an element of  $\mathbb{F}_2$  equals its own trace when  $n$  is odd.

Section 2 collects facts about the trace and the reduction of Hou and Zhao. Section 3 studies a fixed  $x$ , Section 4 proves Theorem 1.1, and Section 5 proves Theorem 1.2 and Corollary 1.3.

## 2. PRELIMINARIES

**Lemma 2.1.** *Let  $\rho(z) = z^{2^{m+1}}$  for  $z \in F$ .*

- (a)  $\rho(z^{2^m}) = z = \rho(z)^{2^m}$  and  $\rho(\rho(z)) = z^2$  for every  $z \in F$ .
- (b) *The elements of  $F$  fixed by  $z \mapsto z^{2^m}$ , and those fixed by  $\rho$ , are 0 and 1.*

*Proof.* (a) holds because  $z^{2^n} = z$ ,  $2^m \cdot 2^{m+1} = 2^n$  and  $2^{m+1} \cdot 2^{m+1} = 2 \cdot 2^n$ . For (b), the fixed field of  $z \mapsto z^{2^k}$  is  $\mathbb{F}_{2^{\gcd(k,n)}}$ , and  $\gcd(m, 2m+1) = \gcd(m+1, 2m+1) = 1$ .  $\square$

Let  $T_0 = \{w \in F : \text{Tr}(w) = 0\}$ , put  $\wp(z) = z^2 + z$ , and for  $z \in F$  let

$$T_m(z) = \sum_{i=0}^{m-1} z^{2^i}.$$

**Lemma 2.2.** (a)  $\text{Tr}(z^{2^k}) = \text{Tr}(z)$  for all  $z \in F$  and  $k \geq 0$ ; in particular  $\text{Tr}(\rho(z)) = \text{Tr}(z)$ .

- (b)  $\text{Tr}(1) = 1$ , so  $\text{Tr}(\varepsilon) = \varepsilon$  for  $\varepsilon \in \mathbb{F}_2$ .
- (c) *Each of the maps  $z \mapsto \wp(z)$ ,  $z \mapsto z^{2^m} + z$  and  $z \mapsto \rho(z) + z$  is  $\mathbb{F}_2$ -linear with kernel  $\mathbb{F}_2$  and image  $T_0$ .*
- (d)  $\wp(T_m(z)) = T_m(\wp(z)) = z^{2^m} + z$  for all  $z \in F$ .

*Proof.* (a) is clear and (b) holds because  $n$  is odd. In (c), the kernels are  $\mathbb{F}_2$  by Lemma 2.1(b), so each image has  $q/2$  elements; each image lies in  $T_0$  by (a), and  $|T_0| = q/2$ . For (d), both sides telescope:  $\wp(T_m(z)) = \sum_{i=1}^m z^{2^i} + \sum_{i=0}^{m-1} z^{2^i} = z^{2^m} + z$ , and  $T_m(z^2 + z)$  is the same sum.  $\square$

The next lemma is the reduction of Hou and Zhao [6, Section 4]; we include the short proof.

**Lemma 2.3.** (a) *For  $x, y \in F$ ,*

$$\sum_{a_1, a_2, a_3 \in \mathbb{F}_2} W_n(a_1x + a_2y + a_3) = g(x, y).$$

- (b) *Let  $A = c + A_0$  be a three-dimensional affine subspace of  $F$  with linear part  $A_0$ . Then  $\sum_{a \in A} W_n(a) = \sum_{a \in A_0} W_n(a)$ , and  $\sum_{a \in A_0} W_n(a) = b^{2^m+3} \sum_{a \in b^{-1}A_0} W_n(a)$  for every  $b \in A_0 \setminus \{0\}$ .*
- (c)  *$W_n$  is not third-order sum-free if and only if  $\dim_{\mathbb{F}_2} Z(x) \geq 3$  for some  $x \in F \setminus \mathbb{F}_2$ .*

*Proof.* (a) Since  $a_i^{2^k} = a_i$  for  $a_i \in \mathbb{F}_2$ ,

$$W_n(a_1x + a_2y + a_3) = (a_1x^{2^m} + a_2y^{2^m} + a_3)(a_1x^2 + a_2y^2 + a_3)(a_1x + a_2y + a_3).$$

Expanding, we get a sum of terms  $a_i a_j a_k \alpha \beta \gamma$  with  $\alpha \in \{x^{2^m}, y^{2^m}, 1\}$ ,  $\beta \in \{x^2, y^2, 1\}$  and  $\gamma \in \{x, y, 1\}$ . Summed over  $(a_1, a_2, a_3) \in \mathbb{F}_2^3$ , a monomial in the  $a_i$  gives 0 unless all three of  $a_1, a_2, a_3$  occur in it, because  $\sum_{a \in \mathbb{F}_2} 1 = 0$ . So only the six terms in which  $i, j, k$  are distinct survive, each with sum 1, and they add up to  $g(x, y)$ .

(b) Write the elements of  $A$  as  $c + a$  with  $a \in A_0$  and expand  $W_n(c + a) = (c^{2^m} + a^{2^m})(c^2 + a^2)(c + a)$ . Apart from  $a^{2^m} a^2 a$ , every one of the eight products is a constant times a product of at most two  $\mathbb{F}_2$ -linear functions of  $a$ . In coordinates  $a = a_1 e_1 + a_2 e_2 + a_3 e_3$  with respect to a basis of  $A_0$ , such a product is a combination of monomials in at most two of the  $a_i$ , and its sum over  $A_0$  vanishes as in (a). The second statement holds because  $W_n$  is a power function.

(c) By (b),  $W_n$  is not third-order sum-free if and only if it sums to zero over a three-dimensional linear subspace that contains 1. Such a subspace is  $\langle 1, x, y \rangle$  with  $1, x, y$  linearly independent over  $\mathbb{F}_2$ , and by (a) the sum over it is  $g(x, y)$ . Since  $Z(x)$  always contains  $\langle 1, x \rangle$ , a suitable  $y$  exists if and only if  $\dim Z(x) \geq 3$ .  $\square$

3. A FIXED ELEMENT  $x$ 

In this section and the next,  $x \in F \setminus \mathbb{F}_2$  is fixed and

$$u = x^{2^m}, \quad t = x^2 + x, \quad d = x + u, \quad v = u^2 + u.$$

By Lemma 2.1,  $\rho(x) = u^2$  and  $\rho(u) = x$ , so

$$(3.1) \quad \rho(t) = v^2, \quad \rho(d) = d + v = x + u^2, \quad \rho(d + v) = d^2, \quad \rho(x^2 + u) = u^4 + x, \quad t^{2^m} = v.$$

The elements  $t$ ,  $u^2 + u = v$ ,  $d$  and  $d + v = x + \rho(x)$  are nonzero by Lemma 2.1(b), and

$$(3.2) \quad t = d^2 + d + v.$$

Write  $L(y) = g(x, y)$ , so that

$$L(y) = t y^{2^m} + d y^2 + (x^2 + u) y,$$

an  $\mathbb{F}_2$ -linear map of  $F$  with kernel  $Z(x)$ . One checks directly that  $L(1) = L(x) = 0$ .

**Lemma 3.1.**  $L(y) = t T_m(\wp(y)) + d \wp(y)$  for every  $y \in F$ .

*Proof.* By Lemma 2.2(d),  $t T_m(\wp(y)) + d \wp(y) = t(y^{2^m} + y) + d(y^2 + y) = t y^{2^m} + d y^2 + (t + d) y$ , and  $t + d = x^2 + u$ .  $\square$

Let

$$Y(y) = \frac{d y^2 + (x^2 + u) y}{t}, \quad P(y) = v^2 y + (d + v) Y(y)^4 + (u^4 + x) Y(y)^2,$$

and define  $\Phi: F \rightarrow F$  by  $\Phi(y) = \rho(L(y)/t)$ . Then  $Y$ ,  $P$  and  $\Phi$  are  $\mathbb{F}_2$ -linear,  $L(y) = t(y^{2^m} + Y(y))$ , and  $\Phi(y) = 0$  if and only if  $L(y) = 0$ .

**Lemma 3.2.**  $P(y) = \rho(L(\Phi(y)))$  for every  $y \in F$ .

*Proof.* Let  $\ell = L(y)/t$ , so that  $y^{2^m} = Y(y) + \ell$  and, by Lemma 2.1(a),  $\rho(y) = (y^{2^m})^2 = (Y(y) + \ell)^2$ . Applying  $\rho$  to  $L(y)$  and using (3.1),

$$\rho(L(y)) = v^2 y + (d + v) \rho(y)^2 + (u^4 + x) \rho(y) = P(y) + (d + v) \ell^4 + (u^4 + x) \ell^2.$$

On the other hand  $\rho(L(y)) = \rho(t\ell) = v^2 \rho(\ell)$ . Hence  $P(y) = v^2 \rho(\ell) + (d + v) \ell^4 + (u^4 + x) \ell^2$ . Now put  $\ell' = \Phi(y) = \rho(\ell)$ . By Lemma 2.1(a),  $\ell'^{2^m} = \ell$  and  $\rho(\ell') = \ell^2$ , so

$$\rho(L(\ell')) = \rho(t\ell + d\ell'^2 + (x^2 + u)\ell') = v^2 \ell' + (d + v) \ell^4 + (u^4 + x) \ell^2 = P(y). \quad \square$$

Let  $\Pi(y) = y(y+1)(y+x)(y+x+1) = \wp(y)(\wp(y)+t) = y^4 + (t+1)y^2 + ty$ . It is an additive polynomial whose roots are the elements of  $\langle 1, x \rangle$ . Put

$$\lambda = \frac{(d+v)d^4}{t^4}, \quad c = \frac{t^3 v^2}{d^4(d+v)}, \quad a = \frac{c}{t^2} = \frac{t v^2}{d^4(d+v)}.$$

**Lemma 3.3.** As polynomials in  $y$  over  $F$ ,  $P(y) = \lambda \Pi(y)(\Pi(y) + c)$ . The roots of  $P$  in an algebraic closure of  $F$  form a three-dimensional  $\mathbb{F}_2$ -space  $V$  that contains  $\langle 1, x \rangle$ , and  $V \setminus \langle 1, x \rangle = \{y : \Pi(y) = c\}$ .

*Proof.*  $P$  is an additive polynomial. Its coefficient of  $y^8$  is  $\lambda \neq 0$  and its coefficient of  $y$  is  $v^2 \neq 0$ , since  $Y(y)^4$  and  $Y(y)^2$  contain only  $y^8$ ,  $y^4$  and  $y^2$ . So  $P$  has 8 distinct roots, and they form a three-dimensional  $\mathbb{F}_2$ -space  $V$ . Since  $Y(1) = 1$  and  $Y(x) = u$ ,

$$P(1) = v^2 + (d + v) + (u^4 + x) = 0, \quad P(x) = v^2 x + (d + v)u^4 + (u^4 + x)u^2 = 0,$$

so  $\langle 1, x \rangle \subseteq V$ . Choose  $y_0 \in V \setminus \langle 1, x \rangle$ . Then  $V = \langle 1, x \rangle \cup (y_0 + \langle 1, x \rangle)$  and, since  $\Pi$  is additive,

$$P(y) = \lambda \Pi(y) \Pi(y + y_0) = \lambda \Pi(y) (\Pi(y) + \Pi(y_0)).$$

The coefficient of  $y$  on the right is  $\lambda t \Pi(y_0)$ , because  $\Pi(y)^2$  has only even powers of  $y$ . Comparing with  $v^2$  gives  $\Pi(y_0) = v^2/(\lambda t) = c$ . Finally  $c \neq 0$ , so the roots of  $\Pi(y) + c$  are exactly the four elements of  $V$  outside  $\langle 1, x \rangle$ .  $\square$

**Lemma 3.4.**  $\text{Tr}(a) = 0$ . If  $z \in F$  satisfies  $\wp(z) = a$ , then  $\text{Tr}(tz) = 0$ . Consequently  $V \subseteq F$ .

*Proof.* From (3.2) one checks the identity

$$(3.3) \quad a = \wp\left(\frac{v}{d^2}\right) + \frac{1}{d} + \frac{1}{d+v};$$

multiplied by  $d^4(d+v)$  it reads  $tv^2 = v^2(d+v) + vd^2(d+v) + d^3(d+v) + d^4$ , and the right side equals  $v^2(d^2 + d + v)$ . By (3.1),  $1/(d+v) = \rho(1/d)$ , so  $\text{Tr}(1/(d+v)) = \text{Tr}(1/d)$  and  $\text{Tr}(a) = 0$ . By Lemma 2.2(c) there are exactly two elements  $z \in F$  with  $\wp(z) = a$ , and they differ by 1; since  $\text{Tr}(t) = \text{Tr}(\wp(x)) = 0$ , the value  $\text{Tr}(tz)$  does not depend on the choice.

Let  $h = 1/d$ . Since  $\text{Tr}(h + \text{Tr}(h)) = 0$  by Lemma 2.2(b), Lemma 2.2(c) gives  $z_2 \in F$  with  $\rho(z_2) + z_2 = h + \text{Tr}(h)$ . By Lemma 2.1(a),

$$\wp(z_2) = \rho(\rho(z_2)) + z_2 = \rho(\rho(z_2) + z_2) + (\rho(z_2) + z_2) = \rho(h) + h = \frac{1}{d+v} + \frac{1}{d},$$

so by (3.3) we may take  $z = v/d^2 + z_2$ . First, by (3.2),

$$\frac{tv}{d^2} = v + \frac{v}{d} + \frac{v^2}{d^2} = \wp(u) + \wp\left(\frac{v}{d}\right),$$

which has trace 0. Second, let  $e = d + v = x + \rho(x)$ . Then  $\rho(e) = d^2$  by (3.1), and  $\rho(e) + e = x^2 + x = t$ . Using Lemma 2.2(a) and Lemma 2.1(a) to move  $z \mapsto z^{2^m}$  and  $\rho$  through the trace,

$$\begin{aligned} \text{Tr}(tz_2) &= \text{Tr}(\rho(e)z_2) + \text{Tr}(ez_2) = \text{Tr}(e z_2^{2^m}) + \text{Tr}(ez_2) = \text{Tr}(e(\rho(z_2) + z_2)^{2^m}) \\ &= \text{Tr}(\rho(e)(\rho(z_2) + z_2)) = \text{Tr}(d^2(h + \text{Tr}(h))) = \text{Tr}(d) + \text{Tr}(h) \text{Tr}(d^2) = 0, \end{aligned}$$

since  $\text{Tr}(d) = \text{Tr}(x + x^{2^m}) = 0$ . Hence  $\text{Tr}(tz) = 0$ .

Now Lemma 2.2(c) gives  $y \in F$  with  $\wp(y) = tz$ . Then  $\Pi(y) = tz(tz + t) = t^2\wp(z) = c$ , so  $y \in V \setminus \langle 1, x \rangle$  by Lemma 3.3, and  $V = \langle 1, x, y \rangle \subseteq F$ .  $\square$

**Lemma 3.5.**  $V = \{y \in F : L(\Phi(y)) = 0\}$ ,  $Z(x) \subseteq V$  and  $\Phi(V) \subseteq Z(x)$ . The element  $\delta(x) = \Phi(y_0)$  is the same for all  $y_0 \in V \setminus \langle 1, x \rangle$  and lies in  $\langle 1, x \rangle$ . If  $\delta(x) = 0$  then  $Z(x) = V$ ; otherwise  $Z(x) = \langle 1, x \rangle$ .

*Proof.* Since  $V \subseteq F$  (Lemma 3.4) and  $\rho$  is injective, Lemma 3.2 shows that  $V = \{y \in F : L(\Phi(y)) = 0\}$ . If  $L(y) = 0$  then  $\Phi(y) = 0$  and  $y \in V$ , so  $Z(x) \subseteq V$ ; and  $\Phi(V) \subseteq Z(x)$  by the same description of  $V$ . Two choices of  $y_0$  differ by an element of  $\langle 1, x \rangle \subseteq Z(x)$ , on which  $\Phi$  vanishes. As  $\langle 1, x \rangle \subseteq Z(x) \subseteq V$  and  $\dim V = 3$ , either  $Z(x) = V$  or  $Z(x) = \langle 1, x \rangle$ . In the first case  $\delta(x) = 0$ . In the second case  $\delta(x) \in \Phi(V) \subseteq \langle 1, x \rangle$ , and  $\delta(x) \neq 0$  because  $y_0 \notin Z(x)$ .  $\square$

**Lemma 3.6.**  $\delta(x) \in \{0, 1\}$  if and only if  $\text{Tr}(1/d) = 1$ .

*Proof.* Take  $y_0 \in V \setminus \langle 1, x \rangle$  and let  $z = \wp(y_0)/t$ . By Lemma 3.3,  $t^2\wp(z) = \wp(y_0)(\wp(y_0) + t) = c$ , so  $\wp(z) = a$ . Let  $\ell_0 = L(y_0)/t$ , so that  $\delta(x) = \rho(\ell_0)$ , and  $\delta(x) \in \{0, 1\}$  if and only if  $\ell_0 \in \{0, 1\}$ , that is,  $\wp(\ell_0) = 0$ . By Lemma 3.1,  $\ell_0 = T_m(tz) + dz$ . By Lemma 2.2(d), (3.1) and (3.2),

$$\wp(\ell_0) = (tz)^{2^m} + tz + d^2 z^2 + dz = v z^{2^m} + (t + d^2 + d)z + d^2 a = v(z^{2^m} + z) + d^2 a = v T_m(a) + d^2 a.$$

Put  $\gamma = d^2a/v$ , so that  $\wp(\ell_0) = v(T_m(a) + \gamma)$ . On the other hand  $\delta(x) \in \langle 1, x \rangle$  by Lemma 3.5, so  $\ell_0 = \delta(x)^{2^m} \in \{0, 1, u, u+1\}$  and  $\wp(\ell_0) \in \{0, v\}$ . Therefore  $\varepsilon = T_m(a) + \gamma$  lies in  $\mathbb{F}_2$ , and  $\varepsilon = 0$  exactly when  $\delta(x) \in \{0, 1\}$ . By Lemma 2.2(b) and (a),

$$\varepsilon = \text{Tr}(\varepsilon) = \sum_{i=0}^{m-1} \text{Tr}(a^{2^i}) + \text{Tr}(\gamma) = m \text{Tr}(a) + \text{Tr}(\gamma) = \text{Tr}(\gamma),$$

using  $\text{Tr}(a) = 0$  from Lemma 3.4. By (3.2),  $\gamma = tv/(d^2(d+v)) = v/d^2 + v/(d+v)$ . By (3.1),  $\rho(t/d^2) = v^2/(d+v)^2$ , so  $\text{Tr}(v/(d+v)) = \text{Tr}(t/d^2)$ . Since  $v+t = d^2+d$ ,

$$\text{Tr}(\gamma) = \text{Tr}\left(\frac{v+t}{d^2}\right) = \text{Tr}(1) + \text{Tr}\left(\frac{1}{d}\right) = 1 + \text{Tr}\left(\frac{1}{d}\right).$$

So  $\delta(x) \in \{0, 1\}$  if and only if  $\text{Tr}(1/d) = 1$ .  $\square$

#### 4. PROOF OF THEOREM 1.1

The objects of Section 3 depend on  $x$ ; we write  $L_x$ ,  $t_x$ ,  $\Phi_x$ ,  $V_x$  and  $d_x = x + x^{2^m}$  when the dependence matters. The second condition of Theorem 1.1 comes from the substitution  $x \mapsto 1/x$ .

**Lemma 4.1.** *For  $x \in F \setminus \mathbb{F}_2$  and  $y \in F$ ,  $g(1/x, y/x) = x^{-(2^m+3)}g(x, y)$ . Moreover  $\Phi_{1/x}(y) = x^{-1}\Phi_x(xy)$ ,  $V_{1/x} = x^{-1}V_x$  and  $\delta(1/x) = x^{-1}\delta(x)$ .*

*Proof.* With  $u = x^{2^m}$ ,

$$u x^3 g(1/x, y/x) = u x^3 \left( \frac{y^{2^m}}{u} \cdot \frac{1+x}{x^2} + \frac{y^2}{x^2} \cdot \frac{x+u}{xu} + \frac{y}{x} \cdot \frac{u+x^2}{x^2u} \right) = g(x, y).$$

So  $L_{1/x}(y) = x^{-(2^m+3)}L_x(xy)$ . Since  $t_{1/x} = x^{-2} + x^{-1} = t_x/x^3$ ,

$$\Phi_{1/x}(y) = \rho\left(\frac{L_x(xy)}{u t_x}\right) = \rho(u^{-1}) \Phi_x(xy) = x^{-1} \Phi_x(xy).$$

By the first statement of Lemma 3.5, applied to  $x$  and to  $1/x$ ,  $V_{1/x} = \{y \in F : L_{1/x}(\Phi_{1/x}(y)) = 0\} = \{y \in F : L_x(\Phi_x(xy)) = 0\} = x^{-1}V_x$ . If  $y_0 \in V_x \setminus \langle 1, x \rangle$ , then  $y_0/x \in V_{1/x} \setminus \langle 1, 1/x \rangle$ , and  $\delta(1/x) = \Phi_{1/x}(y_0/x) = x^{-1}\Phi_x(y_0) = x^{-1}\delta(x)$ .  $\square$

*Proof of Theorem 1.1.* By Lemma 3.5,  $\dim Z(x) \in \{2, 3\}$ , and  $\dim Z(x) = 3$  if and only if  $\delta(x) = 0$ . Since  $\delta(x) \in \langle 1, x \rangle$  and  $x \neq 1$ ,  $\delta(x) = 0$  if and only if  $\delta(x) \in \{0, 1\}$  and  $\delta(x) \in \{0, x\}$ . By Lemma 3.6, the first condition is  $\text{Tr}(1/d_x) = 1$ . By Lemma 4.1,  $\delta(x) \in \{0, x\}$  if and only if  $\delta(1/x) \in \{0, 1\}$ , which by Lemma 3.6 applied to  $1/x$  means  $\text{Tr}(1/d_{1/x}) = 1$ . Finally  $d_{1/x} = 1/x + 1/u = (x+u)/(xu)$ .  $\square$

#### 5. COUNTING

*Proof of Theorem 1.2.* For  $x \in F \setminus \mathbb{F}_2$  let  $d = x + x^{2^m}$ ,  $u = x^{2^m}$ ,  $\alpha(x) = (-1)^{\text{Tr}(1/d)}$  and  $\beta(x) = (-1)^{\text{Tr}(xu/d)}$ . By Theorem 1.1,

$$N_n = \frac{1}{4} \sum_{x \in F \setminus \mathbb{F}_2} (1 - \alpha(x))(1 - \beta(x)) = \frac{1}{4} \left( q - 2 - \sum \alpha - \sum \beta + \sum \alpha\beta \right),$$

all sums over  $x \in F \setminus \mathbb{F}_2$ . By Lemma 2.2(c),  $x \mapsto x + x^{2^m}$  maps  $F \setminus \mathbb{F}_2$  two-to-one onto  $T_0 \setminus \{0\}$ . Hence

$$\sum \alpha = 2 \sum_{w \in T_0 \setminus \{0\}} (-1)^{\text{Tr}(1/w)} = \sum_{w \in F^*} (1 + (-1)^{\text{Tr}(w)}) (-1)^{\text{Tr}(1/w)} = -1 + K_n,$$

because  $w \mapsto 1/w$  permutes  $F^*$  and  $\sum_{w \in F^*} (-1)^{\text{Tr}(w)} = -1$ . The map  $x \mapsto 1/x$  permutes  $F \setminus \mathbb{F}_2$ , and  $\beta(x) = \alpha(1/x)$  because  $d_{1/x} = d/(xu)$ ; so  $\sum \beta = K_n - 1$ . Finally,  $x \mapsto x + 1$  permutes  $F \setminus \mathbb{F}_2$ , leaves  $d$  unchanged and sends  $xu$  to  $(x + 1)(u + 1) = xu + d + 1$ ; since  $\text{Tr}(1) = 1$ ,

$$\beta(x + 1) = (-1)^{\text{Tr}((xu+1)/d)+1} = -\alpha(x)\beta(x).$$

So  $\sum \alpha\beta = -\sum \beta = 1 - K_n$ , and

$$N_n = \frac{1}{4}(q - 2 - 2(K_n - 1) + 1 - K_n) = \frac{q + 1 - 3K_n}{4}. \quad \square$$

*Proof of Corollary 1.3.* If  $\dim Z(x) = 3$ , then  $A = Z(x)$  is a three-dimensional subspace containing 1 over which  $W_n$  sums to zero, by Lemma 2.3(a). Conversely, let  $A \ni 1$  be such a subspace and  $x' \in A \setminus \mathbb{F}_2$ . Writing  $A = \langle 1, x', y' \rangle$ , Lemma 2.3(a) gives  $g(x', y') = 0$ , so  $A \subseteq Z(x')$ , and  $Z(x') = A$  by Theorem 1.1. Hence the subspaces containing 1 with zero sum correspond to the elements  $x$  with  $\dim Z(x) = 3$ , six elements to each subspace, and there are  $N_n/6$  of them.

Let  $\mathcal{S}$  be the set of three-dimensional linear subspaces with zero sum. By Lemma 2.3(b),  $A \in \mathcal{S}$  and  $b \in F^*$  imply  $bA \in \mathcal{S}$ . The pairs  $(A, b)$  with  $A \in \mathcal{S}$  and  $b \in A \setminus \{0\}$  number  $7|\mathcal{S}|$ , and  $(A, b) \mapsto (b^{-1}A, b)$  maps them bijectively to the pairs  $(B, b)$  with  $B \in \mathcal{S}$ ,  $1 \in B$  and  $b \in F^*$ , which number  $(q - 1)N_n/6$ . So  $|\mathcal{S}| = N_n(q - 1)/42$ . By Lemma 2.3(b), an affine subspace has zero sum exactly when its linear part does, and each linear part has  $2^{n-3}$  cosets. The numbers are positive for  $n \geq 7$  by the bound after Theorem 1.2, and  $N_5 = 0$  because  $K_5 = 11$ .  $\square$

*Remark 5.1.* For  $n = 5$ , Corollary 1.3 gives a second proof that  $W_5 = X^7$  is third-order sum-free. For  $n = 3$  the polynomial  $g(x, Y)$  vanishes identically, and indeed  $N_3 = 6 = 2^3 - 2$  since  $K_3 = -5$ .

## DECLARATIONS

**Funding.** No funding was received for conducting this study.

**Competing interests.** The author has no competing interests to declare that are relevant to the content of this article.

**Data availability.** The proofs in this article are complete by hand. The source of the article and the programs that check its statements (the criterion of Theorem 1.1 and every lemma at every element of  $\mathbb{F}_{2^n}$  in C and Python, the zero-sum subspaces counted from the definition in C++, Theorem 1.2 and Table 1 in Julia and Bash, a Lean 4 kernel certificate for  $n = 5$  and  $n = 7$ , and Lean 4 with Mathlib for the algebraic identities of the proof) are in release v1.1.0 of the repository <https://github.com/creelie/eConjectureWelchSumFree>, <https://github.com/creelie/eConjectureWelchSumFree/releases/tag/v1.1.0>.

**Use of generative AI.** During the preparation of this work the author used Claude (Anthropic) to search the literature, to find and check the proofs, and to draft the text. The author checked every step of the proofs and every reference, and takes full responsibility for the content.

## REFERENCES

- [1] A. Canteaut, P. Charpin and H. Dobbertin, *Binary  $m$ -sequences with three-valued crosscorrelation: a proof of Welch's conjecture*, IEEE Trans. Inform. Theory **46** (2000), 4–8. <https://doi.org/10.1109/18.817504>
- [2] C. Carlet, *On the vector subspaces of  $\mathbb{F}_{2^n}$  over which the multiplicative inverse function sums to zero*, Des. Codes Cryptogr. **93** (2025), 1237–1254. <https://doi.org/10.1007/s10623-024-01531-6>

- [3] C. Carlet, *Two generalizations of almost perfect nonlinearity*, J. Cryptology **38** (2025), Paper No. 20. <https://doi.org/10.1007/s00145-025-09538-5>
- [4] L. Carlitz, *Kloosterman sums and finite field extensions*, Acta Arith. **16** (1969), 179–194. <https://doi.org/10.4064/aa-16-2-179-194>
- [5] H. Dobbertin, *Almost perfect nonlinear power functions on  $GF(2^n)$ : the Welch case*, IEEE Trans. Inform. Theory **45** (1999), 1271–1275. <https://doi.org/10.1109/18.761283>
- [6] X. Hou and S. Zhao, *Further results on sum-freedom of binary and  $q$ -ary functions*, preprint, 2026. [arXiv:2609.31489](https://arxiv.org/abs/2609.31489)
- [7] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. **20**, Cambridge University Press, Cambridge, 1997. <https://doi.org/10.1017/CB09780511525926>
- [8] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207. <https://doi.org/10.1073/pnas.34.5.204>

FORMERLY, ELECTRO-GRAVITATIONAL SPACE PROPULSION LABORATORY (EGSPL),  
BHUBANESWAR, ODISHA 751030, INDIA  
*Email address:* [d.bhattacharjee@erl-forschung.de](mailto:d.bhattacharjee@erl-forschung.de)  
*Email address:* [itsdeep@live.com](mailto:itsdeep@live.com)  
*URL:* <https://orcid.org/0000-0003-0466-750X>