Proofs of two conjectures on ternary weakly regular bent functions

Tor Helleseth[1], *Fellow, IEEE,* Henk D. L. Hollmann, Alexander Kholosha[1], *Member, IEEE,* Zeying Wang, and Qing Xiang[2]

***Abstract*—We study ternary monomial functions of the form $f(x) = \mathrm{Tr}_n(ax^d)$, where $x \in \mathbb{F}_{3^n}$ and $\mathrm{Tr}_n : \mathbb{F}_{3^n} \to \mathbb{F}_3$ is the absolute trace function. Using a lemma of Hou [17], Stickelberger's theorem on Gauss sums, and certain ternary weight inequalities, we show that certain ternary monomial functions arising from [12] are weakly regular bent, settling a conjecture of Helleseth and Kholosha [12]. We also prove that the Coulter-Matthews bent functions are weakly regular.**

***Index Terms*—Bent function, Gauss sum, perfect nonlinear function, planar function, Walsh transform, weakly regular bent function.**

I. Introduction and Summary of results

Let p be a prime, $n \geq 1$ be an integer. We will use $\mathbb{F}_{p^n}$ to denote the finite field of size p^n, and $\mathbb{F}_{p^n}^*$ to denote the set of nonzero elements of $\mathbb{F}_{p^n}$. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a function. The *Walsh (or Fourier) coefficient* of f at $b \in \mathbb{F}_{p^n}$ is defined by

$$S_f(b) \quad = \quad \sum_{x \in \mathbb{F}_{p^n}} \omega^{f(x) - \mathrm{Tr}_n(bx)}$$

where $\mathrm{Tr}_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace function, $\omega = e^{\frac{2\pi i}{p}}$ is a primitive complex pth root of unity, and elements of $\mathbb{F}_p$ are considered as integers modulo p. In the sequel, $S_a(b)$ is also used to denote the Walsh transform coefficient of a function that depends on parameter a when it is clear from the context which function we mean. The function f is said to be a *p-ary bent function* (or a *generalized bent function*) if all its Walsh coefficients satisfy

$$|S_f(b)|^2 = p^n.$$

A p-ary bent function f is said to be *regular* if for every $b \in \mathbb{F}_{p^n}$ the normalized Walsh coefficient $p^{-\frac{n}{2}} S_f(b)$ is equal to a complex pth root of unity, i.e., $p^{-\frac{n}{2}} S_f(b) = \omega^{f^*(b)}$ for some function $f^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$. A bent function f is said to be *weakly regular* if there exists a complex number u with $|u| = 1$ such that $up^{-\frac{n}{2}} S_f(b) = \omega^{f^*(b)}$ for all $b \in \mathbb{F}_{p^n}$, where $f^* : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a function. In such a situation, the function f^* is also a weakly regular bent function and it is called the *dual* of f.

Binary bent functions are usually called *Boolean bent functions*, or simply *bent functions*. These functions were first introduced by Rothaus [24] in 1976. Later Kumar, Scholtz, and Welch [20] generalized the notion of a Boolean bent function to that of a p-ary bent function. All known p-ary bent functions but one are weakly regular. The only example of bent but not weakly regular bent function was constructed by Helleseth and Kholosha [12].

Bent functions, and in general, p-ary bent functions are closely related to other combinatorial and algebraic objects such as Hadamard difference sets in $(\mathbb{F}_{2^n}, +)$ [8], relative difference sets [23], planar functions, and commutative semifields [6], [4], [26]. For future use, we explicitly state the relationship between planar functions and p-ary bent functions here. A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is said to be *planar* if the function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ induced by the polynomial $F(X + a) - F(X) - F(a)$ is bijective for every nonzero $a \in \mathbb{F}_{p^n}$. The following lemma gives the relationship between planar functions and p-ary bent functions.

Lemma 1.1: Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function. Then F is planar if and only if $\mathrm{Tr}_n(aF(x))$ is p-ary bent for all $a \in \mathbb{F}_{p^n}^*$.

The proof of the lemma is fairly straightforward, see [5]. Almost all known planar functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are of Dembowski-Ostrom type, namely the corresponding polynomials $F(X)$ have the form $F(X) = \sum_{i,j} a_{ij} X^{p^i + p^j} \in \mathbb{F}_{p^n}[X]$. The Coulter-Matthews planar functions are special since they are not of Dembowski-Ostrom type. These planar functions can be defined as follows. Let $n, k \geq 1$ be integers such that k is odd and $\gcd(k, n) = 1$. Then the function $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}$ defined by

$$F(x) = x^{\frac{3^k+1}{2}}, \ \forall x \in \mathbb{F}_{3^n}$$

is planar. Thus by Lemma 1.1, $\mathrm{Tr}_n(ax^{\frac{3^k+1}{2}})$ is 3-ary bent for every nonzero $a \in \mathbb{F}_{3^n}$. These bent functions are usually called *the Coulter-Matthews bent functions*. It is conjectured that the Coulter-Matthews bent functions are weakly regular [12], [19]. (Strictly speaking, it was only stated as an open problem in [12] to decide whether the Coulter-Matthews bent functions are weakly regular or not. But most people believed that these functions are weakly regular bent.) In a recent paper [19], it was proved that the Coulter-Matthews bent functions are weakly regular in two special cases. We confirm the conjecture

Tor Helleseth and Alexander Kholosha are with the Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no; Alexander.Kholosha@ii.uib.no).

Henk D. L. Hollmann is with Philips Research Laboratories, High Tech Campus HTC-36, 5656 AE Eindhoven, the Netherlands (e-mail: henk.d.l.hollmann@philips.com).

Zeying Wang and Qing Xiang are with the Department of Mathematical Sciences, University of Delaware, Newark DE 19716 USA (e-mail: xiang@math.udel.edu, wangz@math.udel.edu)

[1] Research supported by the Norwegian Research Council.

[2] Research supported in part by NSF Grant DMS 0701049.

in this paper. Therefore our first result in this paper is

Theorem 1.2: Let $n, k \geq 1$ be integers such that k is odd and $\gcd(k, n) = 1$. Then the bent function $\mathrm{Tr}_n(ax^{\frac{3^k+1}{2}})$, $a \in \mathbb{F}_{3^n}^*$, is weakly regular bent.

Helleseth and Kholosha [12] surveyed all proven and conjectured classes of p-ary monomial bent functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ of the form $f(x) = \mathrm{Tr}_n(ax^d)$, where $a \in \mathbb{F}_{p^n}^*$, d is an integer, and p is odd. (See Table 1 in [12].) In that paper, besides mentioning that it is an open problem to decide whether the Coulter-Matthews bent functions are weakly regular, the authors also made the following conjecture.

Conjecture 1.3: ([12]) Let $n = 2k$ with k odd. Then the ternary function f mapping $\mathbb{F}_{3^n}$ to $\mathbb{F}_3$ and given by

$$f(x) = \mathrm{Tr}_n\left(ax^{\frac{3^n-1}{4}+3^k+1}\right)$$

is a weakly regular bent function if $a = \xi^{\frac{3^k+1}{4}}$ and ξ is a primitive element of $\mathbb{F}_{3^n}$. Moreover, for $b \in \mathbb{F}_{3^n}$ the corresponding Walsh transform coefficient of f is equal to

$$S_f(b) = -3^k \omega^{\pm \mathrm{Tr}_k\left(\frac{b^{3^k+1}}{a(I+1)}\right)}$$

where I is a primitive fourth root of unity in $\mathbb{F}_{3^n}$.

We will show that the ternary functions in the above conjecture are indeed weakly regular bent. It still remains to prove the second part of the conjecture. We state our second result in this paper as

Theorem 1.4: Let k be an odd positive integer, and let $n = 2k$. Then the ternary function $f : \mathbb{F}_{3^n} \to \mathbb{F}_3$ defined by

$$f(x) = \mathrm{Tr}_n(ax^{\frac{3^n-1}{4}+3^k+1}),\ \forall x \in \mathbb{F}_{3^n},$$

is a weakly regular bent function if $a = \xi^{\frac{3^k+1}{4}}$ and ξ is a primitive element of $\mathbb{F}_{3^n}$.

Our proofs of Theorem 1.2 and 1.4 rely on a lemma of Hou [17]. The idea is of a p-adic nature, and it has been used successfully a few times in the literature (see for example, [15], [9]): Given a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, it is usually difficult to compute the Walsh coefficients $S_f(b)$ explicitly; sometimes, even computing the absolute values of $S_f(b)$ is difficult. However, such difficulties can sometimes be bypassed by divisibility considerations. To this end, we first introduce Gauss sums, Stickelberger's theorem on Gauss sums, and Hou's lemma.

II. The Teichmüller character, Gauss sums, Stickelberger's Theorem, and Hou's lemma

Let p be a prime, $q = p^n$, and $n \geq 1$. Let $\omega = e^{\frac{2\pi i}{p}}$ be a primitive complex pth root of unity and let Tr_n be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \omega^{\mathrm{Tr}_n(x)},$$

which is easily seen to be a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*$$

be a character of $\mathbb{F}_q^*$ (the cyclic multiplicative group of $\mathbb{F}_q$). We define the *Gauss sum* by

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

Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0) = -1$. Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi \in X} g(\chi)\chi^{-1}(c), \tag{1}$$

where X denotes the character group of $\mathbb{F}_q^*$.

One of the elementary properties of Gauss sums is [3, Theorem 1.1.4]

$$g(\chi)\overline{g(\chi)} = q, \quad \text{if} \quad \chi \neq \chi_0. \tag{2}$$

A deeper result on Gauss sums is Stickelberger's theorem (Theorem 2.1 below) on the prime ideal factorization of Gauss sums. We first introduce some notation. Let a be any integer not divisible by $q-1$. Then there are *unique* integers $a_0, \ldots, a_{n-1}$ with $0 \leq a_i \leq p-1$ for all i, $0 \leq i \leq n-1$ such that

$$a \equiv a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \bmod q-1.$$

We define the (p-ary) *weight* of a (mod $q-1$), denoted by $w(a)$, as

$$w(a) = a_0 + a_1 + \cdots + a_{n-1}.$$

For integers a divisible by $q-1$, we define $w(a) = 0$.

Next let ξ_{q-1} be a complex primitive $(q-1)$th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let $\omega_\mathfrak{p}$ be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega_\mathfrak{p} : \mathbb{F}_q^* \to \{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\}$$

satisfying

$$\omega_\mathfrak{p}(\alpha) \pmod{\mathfrak{p}} = \alpha, \tag{3}$$

for all α in $\mathbb{F}_q^*$. The Teichmüller character $\omega_\mathfrak{p}$ has order $q-1$; hence it generates all multiplicative characters of $\mathbb{F}_q$.

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{p}$. For an integer a, let $\nu_\mathfrak{P}(g(\omega_\mathfrak{p}^{-a}))$ denote the $\mathfrak{P}$-adic valuation of $g(\omega_\mathfrak{p}^{-a})$. The following classical theorem is due to Stickelberger (see [21, p. 7], [3, p. 344]).

Theorem 2.1: Let p be a prime, and $q = p^n$. Let a be any integer not divisible by $q-1$. Then

$$\nu_\mathfrak{P}(g(\omega_\mathfrak{p}^{-a})) = w(a).$$

Next we state Hou's lemma using the notation developed in this paper.

Lemma 2.2: ([17]) Let $f : \mathbb{F}_{3^n} \to \mathbb{F}_3$ be a function. We have

(i) f is a ternary bent function if and only if $\nu_3(S_f(b)) = \frac{n}{2}$ for all $b \in \mathbb{F}_{3^n}$.

(ii) f is a weakly regular bent function if and only if $\nu_3(S_f(0)) = \frac{n}{2}$ and $\nu_3(S_f(b) - S_f(0)) > \frac{n}{2}$ for all $b \in \mathbb{F}_{3^n}^*$.

III. Proofs of the Main Results

We will first prove Theorem 1.2. The proof is relatively easy since most of the work has been done in [11].

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a function, and $\omega = e^{\frac{2\pi i}{p}}$ be a primitive complex pth root of unity. In [11], the following notation was introduced:

$$S_F(a,b) = \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}_n(aF(x)+bx)},$$

$K = \mathbb{Q}(\omega)$,

$$W_K^+ = \{\omega^i \,|\, 0 \le i \le p-1\}$$

and

$$W_K^- = \{-\omega^i \,|\, 0 \le i \le p-1\}.$$

Note that $W_K = W_K^+ \cup W_K^-$ is the group of roots of unity in K^*. We quote the following theorem from [11].

Theorem 3.1: ([11]) Let q be an odd prime power. Let F be a planar function on $\mathbb{F}_q$ with $F(0) = 0$ and $F(-x) = F(x)$ for all $x \in \mathbb{F}_q$. Then we have

i)

$$\begin{aligned} \sum_{a \in \mathbb{F}_q^*} S_F(a,0) &= 0 \\ \sum_{a,b \in \mathbb{F}_q} S_F(a,b) &= \sum_{a,b \in \mathbb{F}_q} S_F(a,b)^2 = q^2 \end{aligned}$$

ii) For all $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$

$$S_F(a,b) = \varepsilon_{a,b}(\sqrt{p^*})^n, \quad \varepsilon_{a,b} \in W_K,$$

where $p^* = (-1)^{\frac{p-1}{2}}p$. Moreover, if F is of Dembowski-Ostrom type or F is the Coulter-Matthews planar function, then

$$\varepsilon_{a,0} \in \{\pm 1\} \quad \text{and} \quad \varepsilon_{a,b} \cdot \varepsilon_{a,0} \in W_K^+.$$

We are ready to give the proof of Theorem 1.2.

Proof ot Theorem 1.2: Let $F : \mathbb{F}_{3^n} \to \mathbb{F}_{3^n}$ be defined by $F(x) = x^{\frac{3^k+1}{2}}$, $\forall x \in \mathbb{F}_{3^n}$. For any nonzero $a \in \mathbb{F}_{3^n}$, let $f : \mathbb{F}_{3^n} \to \mathbb{F}_3$ be defined by $f(x) = \mathrm{Tr}_n(ax^{\frac{3^k+1}{2}})$, $\forall x \in \mathbb{F}_{3^n}$. By Lemma 2.2, it suffices to show that $\nu_3(S_f(0)) = n/2$, and for every $b \in \mathbb{F}_{3^n}^*$, $\nu_3(S_f(b) - S_f(0)) > \frac{n}{2}$.

As F is a planar function on $\mathbb{F}_{3^n}$, by Theorem 3.1,

$$S_f(0) = S_F(a,0) = \varepsilon_{a,0}(\sqrt{-3})^n.$$

Therefore $\nu_3(S_f(0)) = \frac{n}{2}$.

For any $b \in \mathbb{F}_{3^n}^*$, we have

$$\begin{aligned} &S_f(b) - S_f(0) \\ &\quad = \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}_n(aF(x)-bx)} - \sum_{x \in \mathbb{F}_q} \omega^{\mathrm{Tr}_n(aF(x))} \\ &\quad = S_F(a,-b) - S_F(a,0). \end{aligned}$$

By Theorem 3.1, we have

$$S_F(a,-b) = \varepsilon_{a,-b}(\sqrt{-3})^n, \; S_F(a,0) = \varepsilon_{a,0}(\sqrt{-3})^n,$$

and

$$\varepsilon_{a,0} \in \{\pm 1\} \quad \text{and} \quad \varepsilon_{a,-b} \cdot \varepsilon_{a,0} \in W_K^+.$$

Therefore,

$$\begin{aligned} S_f(b) - S_f(0) &= (\sqrt{-3})^n(\varepsilon_{a,-b} - \varepsilon_{a,0}) \\ &= (\sqrt{-3})^n \varepsilon_{a,0}(\omega^j - 1), \end{aligned}$$

where ω is a complex primitive cubic root of unity, and $j \in \{0, 1, 2\}$.

Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over 3. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \omega]$ lying above $\mathfrak{p}$. Since $\nu_{\mathfrak{P}}(3) = 2$, we see that

$$\nu_3(S_f(b) - S_f(0)) > \frac{n}{2} \iff \nu_{\mathfrak{P}}(S_f(b) - S_f(0)) > n.$$

Note that for $j = 0$, we have $\nu_{\mathfrak{P}}(\omega^j - 1) = \infty$; and for $j = 1$ or 2, we have $\nu_{\mathfrak{P}}(\omega^j - 1) = 1$. As $\nu_{\mathfrak{P}}(\sqrt{-3})^n = n$, we have

$$\nu_{\mathfrak{P}}(S_f(b) - S_f(0)) = \nu_{\mathfrak{P}}(\omega^j - 1) + \nu_{\mathfrak{P}}(\sqrt{-3})^n > n.$$

Hence we have shown that $\nu_3(S_f(b) - S_f(0)) > \frac{n}{2}$. The proof of theorem is now complete. ■

Remark 3.2: It was shown in [17] that if $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a weakly regular bent function and $(p-1)n \ge 4$, then

$$\deg(f) \le \frac{(p-1)n}{2}. \tag{4}$$

In [17], after the proof of the bound in (4), it was mentioned that when p and n are both odd with $n \ge 3$, it is not known if the bound in (4) is attainable. Let $n \ge 3$ be an even integer. Then the Coulter-Matthews bent functions $\mathrm{Tr}_n(ax^{\frac{3^{n-1}+1}{2}})$ are weakly regular (by Theorem 1.2) and have degree n, attaining the bound in (4) in the case where $p = 3$ and n is even. For the case where p and n are both odd, the Coulter-Matthews bent function $\mathrm{Tr}_n(ax^{\frac{3^{n-2}+1}{2}})$ is weakly regular and has degree $n - 1$, which is one less than the bound in (4).

We now make some preparation for the proof of Theorem 1.4. Let C_i $(i = 0, 1, 2, 3)$ denote the *cyclotomic classes* of order four in the multiplicative group of $\mathbb{F}_{p^n}$, i.e., $C_i = \{\xi^{4t+i} \mid t = 0, \ldots, f-1\}$, where ξ is a primitive element of $\mathbb{F}_{p^n}$ and $f = \frac{p^n-1}{4}$. Throughout this section all expressions in the indices numbering the cyclotomic classes are taken modulo 4.

Lemma 3.3: ([13]) Let p be an odd prime with $p \equiv 3 \bmod$ and let $n = 2k$ with k odd. Raising elements of C_i to the $(p^k+1)^{\text{th}}$ power results in a $\frac{p^k+1}{2}$ -to-1 mapping onto the cyclotomic classes of order two in the multiplicative group of $\mathbb{F}_{p^k}$. Moreover, C_0 and C_2 map onto the squares and C_1 and C_3 onto the non-squares in $\mathbb{F}_{p^k}^*$.

Proof: Take the following polynomial over $\mathbb{F}_p$ that factors in $\mathbb{F}_{p^k}$ as

$$p(z) = z^{\frac{p^n-1}{4}} - 1 = (z^t)^{p^k-1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^k}^*} (z^t - \alpha)$$

where $t = \frac{p^k+1}{4}$. The roots of $p(z)$ are exactly all the elements from C_0. Therefore, it can be concluded that raising elements of C_0 to the power of t results in a t-to-1 mapping onto the multiplicative group of $\mathbb{F}_{p^k}$. In general, raising elements of $C_i = \xi^i C_0$ to the t^{th} power results in a t-to-1 mapping onto the coset $\xi^{it}\mathbb{F}_{p^k}^*$.

Let $\eta = \xi^{p^k+1}$ be a primitive element of $\mathbb{F}_{p^k}$. When k is odd, the cyclic subgroups generated by η^2 and by η^4 are equal since they have the same multiplicative order equal to

$$\mathrm{ord}\,(\eta^4) = \frac{p^k-1}{\gcd(p^k-1,4)} = \frac{p^k-1}{2} = \mathrm{ord}\,(\eta^2)\ .$$

Thus, raising elements of $\mathbb{F}^*_{p^k}$ to the fourth power is a mapping onto the subgroup generated by η^2 and since both α and $-\alpha$ produce the same image for any $\alpha \in \mathbb{F}^*_{p^k}$, this is a 2-to-1 mapping.

Also note that $\xi^{4it} = \xi^{i(p^k+1)} = \eta^i$. Therefore, combination of these two mappings that is equivalent to raising elements of C_i to the power of $4t = p^k+1$, results in a $\frac{p^k+1}{2}$ -to-1 mapping onto the cyclotomic classes of order two in $\mathbb{F}^*_{p^k}$. Moreover, C_0 and C_2 map onto the squares and C_1 and C_3 onto the non-squares in $\mathbb{F}^*_{p^k}$. ■

Lemma 3.4: ([13]) Let p be an odd prime with $p \equiv 3 \bmod 8$ and let $n = 2k$ with k odd. Then for any $c \in \mathbb{F}^*_{p^k}$ and $z \in \mathbb{F}^*_{p^n}$, and any cyclotomic class C_j $(j = 0,1,2,3)$, we have

$$\sum_{y\in C_j} \omega^{\mathrm{Tr}_n(cz^{p^k}y)} = \begin{cases} \frac{3p^k-1}{4}, & \text{if } z \in C_{j+2};\\ -\frac{p^k+1}{4}, & \text{otherwise.}\end{cases}$$

This lemma is a direct consequence of part (1) of the following general theorem [22] on uniform cyclotomy. See also [2].

Theorem 3.5: ([22]) Let $q = p^n$ be a prime power, let $e > 1$ be a divisor of $q-1$ and let C_i, $0 \le i \le e-1$, be the cyclotomic classes of order e. Assume there exists a positive integer j such that $p^j \equiv -1$ $(mod\ e)$, and assume j is the smallest such integer. Moreover assume that $n = 2j\gamma$. Then the cyclotomic periods $\eta_i = \sum_{x\in C_i} \omega^{\mathrm{Tr}_n(x)}$ are given as follows:

(1) If $\gamma, p, \frac{p^j+1}{e}$ are all odd, then

$$\eta_{\frac{e}{2}} = \frac{(e-1)p^{j\gamma}-1}{e}, \qquad \eta_i = \frac{-1-p^{j\gamma}}{e}, (i \neq e/2).$$

(2) In all other cases,

$$\eta_0 = \frac{-1-(-1)^{\gamma}(e-1)p^{j\gamma}}{e}, \quad \eta_i = \frac{(-1)^{\gamma}p^{j\gamma}-1}{e}, (i \neq 0).$$

Lemma 3.6: ([13]) Let p be an odd prime with $p \equiv 3 \bmod 8$ and let $n = 2k$ with k odd. For any $c \in \mathbb{F}_{p^k}$ and $j = 0,1,2,3$ denote

$$T_j = \sum_{x\in C_j} \omega^{\mathrm{Tr}_k\left(c(x+1)^{p^k+1}-c\right)}\ .$$

Then for any j

$$-\overline{T_j} = \omega^{\mathrm{Tr}_k(c)} T_{j+2} + \frac{p^k+1}{4}\left(\omega^{\mathrm{Tr}_k(c)}+1\right)$$

where the bar over a complex value denotes the complex conjugate and the indices are taken modulo 4.

Proof: First, it is easy to see that for any nonzero $c \in \mathbb{F}_{p^k}$

$$\begin{aligned} &1 + T_0 + T_1 + T_2 + T_3\\ &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_k i\left(c(x+1)^{p^k+1}-c\right)}\\ &= \omega^{-\mathrm{Tr}_k(c)} \sum_{y\in\mathbb{F}_{p^n}} \omega^{\mathrm{Tr}_k\left(cy^{p^k+1}\right)} \qquad (5)\\ &\overset{(*)}{=} \omega^{-\mathrm{Tr}_k(c)}\left((p^k+1)\sum_{z\in\mathbb{F}^*_{p^k}} i\omega^{\mathrm{Tr}_k(cz)}+1\right)\\ &= -p^k\omega^{-\mathrm{Tr}_k(c)}\end{aligned}$$

where $(*)$ holds since raising elements of $\mathbb{F}^*_{p^n}$ to the $(p^k+1)^{\mathrm{th}}$ power is a (p^k+1)-to-1 mapping onto $\mathbb{F}^*_{p^k}$ as proved in [7, Lemma 1].

Let $C_i \cdot C_j$ denote the *strong union* of C_i and C_j, i.e., the set of elements of $\mathbb{F}_{p^n}$ that can be represented as a sum of two addends from C_i and C_j, respectively, and counting the multiplicity of such a representation. Thus, $C_i \cdot C_j$ consists of the elements $\xi^{4t+i} + \xi^{4d+j} = \xi^{4d+j}(1+\xi^{4(t-d)+i-j})$ for all $t, d = 0, \ldots, f-1$. Therefore,

$$\begin{aligned} C_i \cdot C_j &= C_j(1 + C_{i-j})\\ &= (i-j,0)C_j \cup (i-j,1)C_{j+1}\\ &\quad \cup (i-j,2)C_{j+2} \cup (i-j,3)C_{j+3}\\ &= (i-j,-j)C_0 \cup (i-j,1-j)C_1\\ &\quad \cup (i-j,2-j)C_2 \cup (i-j,3-j)C_3 \qquad (6)\end{aligned}$$

if $i \neq j$ and otherwise, since $-1 \in C_0$,

$$\begin{aligned} C_i \cdot C_i &= (0,-i)C_0 \cup (0,1-i)C_1\\ &\quad \cup (0,2-i)C_2 \cup (0,3-i)C_3 \cup f\{0\} \qquad (7)\end{aligned}$$

where (i,j) denotes the *cyclotomic number* that is equal to the number of elements $x \in C_i$ such that $x+1 \in C_j$ and $f\{0\}$ denotes the zero-element of $\mathbb{F}_{p^n}$ taken with multiplicity f. The components i, j in cyclotomic numbers are taken modulo 4.

Also denote $C_i^j = \{x \in C_i \mid 1+x \in C_j\}$ (obviously, $|C_i^j| = (i,j)$). In our case $-1 \in C_0$ and we can prove that $(i,j) = (j,i)$. Indeed, the elements of C_i^j correspond to the pairs (t,d) with $t,d \in \{0,\ldots,f-1\}$ that satisfy the equation $\xi^{4t+i}+1 = \xi^{4d+j}$. Multiplying both sides of the equation by $-1 = \xi^{4l}$ we get the equivalent equation $\xi^{4(d+l)+j}+1 = \xi^{4(t+l)+i}$ whose solutions give the elements of C_j^i. Therefore, for any $i \in \{0,1,2,3\}$ we have

$$\begin{aligned}\sum_{j=0}^{3}(j,i) = \sum_{j=0}^{3}(i,j) &= |C_i^0 \cup C_i^1 \cup C_i^2 \cup C_i^3|\\ &= \begin{cases} |C_i| = f, & \text{if } i \neq 0;\\ |C_0\backslash\{-1\}| = f-1, & \text{otherwise}\end{cases}\end{aligned}$$

since $-1+1 = 0$ that does not belong to any C_i. A good introduction into this subject can be found in [25]. Now for

$i, j \in \{0,1,2,3\}$ and $i \neq j$ we evaluate the product

$$\begin{aligned} T_i\overline{T_j} &= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k(c(x+1)^{p^k+1}-c-c(y+1)^{p^k+1}+c)} \\ &= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k(c[x^{p^k+1}-y^{p^k+1}+(x-y)^{p^k}+(x-y)])} \\ &= \sum_{x\in C_i,\, y\in C_j} \omega^{\mathrm{Tr}_k(c[x^{p^k+1}-y^{p^k+1}+(x+y)^{p^k}+(x+y)])}, \end{aligned}$$

where in the last line we used that $C_j = -C_j$. Hence

$$\begin{aligned} T_i\overline{T_j} &= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k(c[(z-y)^{p^k+1}-y^{p^k+1}+z^{p^k}+z])} \\ &= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)}\, \omega^{-\mathrm{Tr}_k(c[zy^{p^k}+z^{p^k}y])} \\ &= \sum_{z\in C_i\cdot C_j} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)}\, \omega^{-\mathrm{Tr}_n(cz^{p^k}y)} \\ &= \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)} \sum_{r\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n(cz^{p^k}\frac{z}{1+r})}, \end{aligned} \tag{8}$$

where $z = x + y \in C_i \cdot C_j$ and the value of y is uniquely defined by z. Therefore, if $z = x + y \in C_t$ with $x \in C_i$ and $y \in C_j$ then $z = y(1 + xy^{-1})$ with $xy^{-1} \in C_{i-j}^{t-j}$. By (6), the multiplicity of $z \in C_t$ in $C_i \cdot C_j$ is equal to $(i-j, t-j) = \left|C_{i-j}^{t-j}\right|$. Thus, for a fixed $z \in C_t$ the set $\left\{\frac{z}{1+r} \mid r \in C_{i-j}^{t-j}\right\}$ contains all $(i-j, t-j)$ values for $y \in C_j$ that correspond to this z taken with the appropriate multiplicity $(i-j, t-j)$ as a member of $C_i \cdot C_j$. For $i = j$ we just have additionally to consider the zero-element of $\mathbb{F}_{p^n}$ that is found in $C_i \cdot C_i$ with the multiplicity f (see (7)). Then

$$T_i\overline{T_i} = \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)} \sum_{r\in C_0^{t-i}} \omega^{-\mathrm{Tr}_n(cz^{p^k}z/(1+r))} + f. \tag{9}$$

Let $t, j \in \{0,1,2,3\}$ and $z \in C_t$ be fixed. Then for any $i \in \{0,1,2,3\}$ and $r \in C_{i-j}^{t-j}$ we have $\frac{z}{1+r} \in C_j$. Further, $\sum_{i=0}^{3}\left|C_{i-j}^{t-j}\right| = \sum_{i=0}^{3}(i, t-j)$ is equal to $|C_{t-j}| = f$ if $t \neq j$ and is equal to $|C_0| - 1 = f - 1$ otherwise. Since the cardinality of C_j is f, we have proven that

$$\{z/(1+r) \mid r \in C_{i-j}^{t-j},\, i = 0,1,2,3\} = \begin{cases} C_j, & \text{if } t \neq j; \\ C_j \setminus \{z\}, & \text{otherwise} \end{cases}$$

since $r \neq 0$. Therefore, for any $t, j \in \{0,1,2,3\}$ and $z \in C_t$

$$\sum_{i=0}^{3}\sum_{r\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n(cz^{p^k+1}/(1+r))} = \begin{cases} \sum_{y\in C_j} \omega^{-\mathrm{Tr}_n(cz^{p^k}y)}, & \text{if } t \neq j; \\ \sum_{y\in C_j\setminus\{z\}} \omega^{-\mathrm{Tr}_n(cz^{p^k}y)}, & \text{otherwise.} \end{cases} \tag{10}$$

Note that since $n = 2k$ and $p \equiv 3 \bmod 8$ then $(p^n-1)/2 \equiv 0 \bmod 4$ and $-1 = \xi^{\frac{p^n-1}{2}} \in C_0$. Therefore, $-C_j = C_j$ and

$$\begin{aligned} \overline{T_j} &= \sum_{z\in C_j} \omega^{\mathrm{Tr}_k(c[-z^{p^k+1}-z^{p^k}-z])} \\ &= \sum_{z\in C_j} \omega^{\mathrm{Tr}_k(c[-z^{p^k+1}+z^{p^k}+z])}. \end{aligned} \tag{11}$$

Making use of Lemma 3.4 we get that

$$\begin{aligned} &(T_0+T_1+T_2+T_3)\overline{T_j} \\ &\overset{(8,9)}{=} \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)} \\ &\times \quad \sum_{i=0}^{3}\sum_{r\in C_{i-j}^{t-j}} \omega^{-\mathrm{Tr}_n(cz^{p^k}\frac{z}{1+r})} + f \\ &\overset{(10)}{=} \sum_{t=0}^{3}\sum_{z\in C_t} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)} \sum_{y\in C_j} \omega^{-\mathrm{Tr}_n(cz^{p^k}y)} \\ &\quad - \sum_{z\in C_j} \omega^{\mathrm{Tr}_k(c(z+1)^{p^k+1}-c)} \omega^{-\mathrm{Tr}_n(cz^{p^k+1})} + f \\ &= -\frac{p^k+1}{4}\sum_{t\neq j+2} T_t + \frac{3p^k-1}{4}T_{j+2} \\ &\quad - \sum_{z\in C_j} \omega^{\mathrm{Tr}_k(c(-z^{p^k+1}+z^{p^k}+z))} + f \\ &\overset{(11)}{=} -\frac{p^k+1}{4}(T_0+T_1+T_2+T_3) + p^kT_{j+2} - \overline{T_j} + f. \end{aligned}$$

Now, using (5), we get

$$\begin{aligned} -p^k\omega^{-\mathrm{Tr}_k(c)}\overline{T_j} = (p^k\omega^{-\mathrm{Tr}_k(c)}+1)&\frac{p^k+1}{4} \\ &+ p^kT_{j+2} + \frac{p^n-1}{4}, \end{aligned}$$

and hence

$$-\overline{T_j} = \omega^{\mathrm{Tr}_k(c)}T_{j+2} + \frac{p^k+1}{4}(\omega^{\mathrm{Tr}_k(c)}+1),$$

as was claimed. ■

Lemma 3.7: ([12], [14]) Let $n = 2k$ and $a \in \mathbb{F}_{p^n}$ for an odd prime p. Then the function f defined by $f(x) = \mathrm{Tr}_n\left(ax^{p^k+1}\right)$ $\forall x \in \mathbb{F}_{p^n}$ is bent if and only if $a + a^{p^k} \neq 0$. Moreover, if the latter condition holds then f is weakly regular and, for $b \in \mathbb{F}_{p^n}$, the corresponding Walsh transform coefficient of f is equal to

$$S_a(b) = -p^k\omega^{-\mathrm{Tr}_k\left(\frac{b^{p^k+1}}{a+a^{p^k}}\right)}.$$

For the proof of this lemma, we refer the reader to ([12], [14]).

Proof ot Theorem 1.4: By Lemma 2.2, it suffices to show that $\nu_3(S_a(0)) = k$, and for every $b \in \mathbb{F}_{3^n}^*$, $\nu_3(S_a(b) - S_a(0)) > \frac{n}{2}$. First we will compute $S_a(0)$ and $S_a(b) - S_a(0)$.

Let $I = \xi^{\frac{3^n-1}{4}}$, where I is a primitive 4th root of unity in $\mathbb{F}_{3^n}$ (obviously $I^2 = -1$). As before, let C_i, $0 \leq i \leq 3$, be the cyclotomic classes of order 4 of $\mathbb{F}_{3^n}$. Then any $x \in C_i$

satisfies $x^{\frac{3^n-1}{4}} = \xi^{\frac{i(3^n-1)}{4}} = I^i$. Also $a^{3^k} = aI$ and $\mathrm{Tr}_k^n(a) = a + a^{3^k} = a(I+1)$. On the other hand, $\mathrm{Tr}_k^n(aI) = aI - a^{3^k}I = aI + a = a(I+1) = \mathrm{Tr}_k^n(a)$ since $3^k \equiv 3 \pmod 4$ for odd k. Therefore,

$$\begin{aligned}
S_a(b) - 1 &= \sum_{x\in\mathbb{F}_{3^n}} \omega^{\mathrm{Tr}_n(ax^{\frac{3^n-1}{4}+3^k+1}-bx)} - 1 \\
&= \sum_{i=0}^{3}\sum_{x\in C_i} \omega^{\mathrm{Tr}_n(aI^i x^{3^k+1}-bx)} \\
&= \sum_{x\in C_0\cup C_1} \omega^{\mathrm{Tr}_k(a_1x^{3^k+1}-bx-b^{3^k}x^{3^k})} \\
&\quad + \sum_{x\in C_2\cup C_3} \omega^{\mathrm{Tr}_k(-a_1x^{3^k+1}-bx-b^{3^k}x^{3^k})} \\
&= \sum_{x\in C_0\cup C_1} \omega^{\mathrm{Tr}_k(a_1(x-\beta)^{3^k+1}-a_1\beta^{3^k+1})} \\
&\quad + \sum_{x\in C_2\cup C_3} \omega^{-\mathrm{Tr}_k(a_1(x+\beta)^{3^k+1}-a_1\beta^{3^k+1})}, \quad (12)
\end{aligned}$$

where $a_1 = a(I+1) \neq 0$ belongs to $\mathbb{F}_{3^k}$ and $b = a_1\beta^{3^k}$.

If $b = 0$, then $\beta = 0$. Using Lemma 3.3, we have

$$\begin{aligned}
S_a(0) &= 1 + \sum_{x\in C_0\cup C_1} \omega^{\mathrm{Tr}_k(a_1x^{3^k+1})} \\
&\quad + \sum_{x\in C_2\cup C_3} \omega^{-\mathrm{Tr}_k(a_1x^{3^k+1})} \\
&= 1 + \frac{3^k+1}{2}\sum_{y\in\mathbb{F}_{3^k}^*}\left(\omega^{\mathrm{Tr}_k(a_1y)} + \omega^{-\mathrm{Tr}_k(a_1y)}\right) \\
&= -3^k.
\end{aligned}$$

Therefore $\nu_3(S_a(0)) = k = n/2$.

Next suppose $b \neq 0$. Then $\beta \neq 0$. Let $c = a_1\beta^{3^k+1}$. We have $c \in \mathbb{F}_{3^k}^*$. Assuming that $\beta^{-1} \in C_j$ (i.e., ind(β^{-1})$\equiv j \pmod 4$), we have $\beta^{-1}C_i = C_{i+j}$ for any $i \in \{0,1,2,3\}$. Now making the substitution $x = \beta y$ in (12), we have

$$\begin{aligned}
S_a(b) - 1 &= \sum_{y\in C_j\cup C_{j+1}} \omega^{\mathrm{Tr}_k(c(y-1)^{3^k+1}-c)} \\
&\qquad + \sum_{y\in C_{j+2}\cup C_{j+3}} \omega^{-\mathrm{Tr}_k(c(y+1)^{3^k+1}-c)}.
\end{aligned}$$

Since $n = 2k$, $(3^n-1)/2 \equiv 0 \pmod 4$ and $-1 = \xi^{\frac{3^n-1}{2}} \in C_0$. Therefore, $-C_i = C_i$ and

$$\sum_{y\in C_i} \omega^{\mathrm{Tr}_k(c(y-1)^{3^k+1})} = \sum_{y\in C_i} \omega^{\mathrm{Tr}_k(c(y+1)^{3^k+1})}.$$

Let T_i $(i = 0,1,2,3)$ be defined as in Lemma 3.6. Then we have

$$S_a(b) = 1 + T_j + T_{j+1} + \overline{T_{j+2}} + \overline{T_{j+3}},$$

where the bars denote complex conjugation. By Lemma 3.6 we have

$$\begin{aligned}
S_a(b) &= 1 + T_j + T_{j+1} + \overline{T_{j+2}} + \overline{T_{j+3}} \\
&= \left(1 - \omega^{\mathrm{Tr}_k(c)}\right)\left(T_j + T_{j+1} + \frac{3^k+1}{2}\right) - 3^k, \quad (13)
\end{aligned}$$

where

$$\begin{aligned}
T_j &= \sum_{x\in C_j} \omega^{\mathrm{Tr}_k(c(x+1)^{3^k+1}-c)} = \sum_{x\in C_j} \omega^{\mathrm{Tr}_n(2cx^{3^k+1}+cx)} \\
&= \sum_{x\in C_j} \omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)},
\end{aligned}$$

for $j = 0,1,2,3$. Let η be a multiplicative character of $\mathbb{F}_{3^n}$ of order 4 such that $\eta(\xi) = i$. Then

$$T_0 = \frac{1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\left(1 + \eta(x) + \eta^2(x) + \eta^3(x)\right)\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)};$$

$$T_1 = \frac{1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}(1 - i\eta(x) - \eta^2(x) + i\eta^3(x))\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)};$$

$$T_2 = \frac{1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\left(1 - \eta(x) + \eta^2(x) - \eta^3(x)\right)\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)};$$

$$T_3 = \frac{1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}(1 + i\eta(x) - \eta^2(x) - i\eta^3(x))\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}.$$

So

$$\begin{aligned}
T_0 + T_1 &= \frac{1}{2}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)} \\
&\quad + \frac{1-i}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\
&\qquad + \frac{1+i}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x); \quad (14)
\end{aligned}$$

$$\begin{aligned}
T_1 + T_2 &= \frac{1}{2}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)} \\
&\quad + \frac{-i-1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\
&\qquad + \frac{i-1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x); \quad (15)
\end{aligned}$$

$$\begin{aligned}
T_2 + T_3 &= \frac{1}{2}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)} \\
&\quad + \frac{-1+i}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\
&\qquad + \frac{-i-1}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x); \quad (16)
\end{aligned}$$

$$\begin{aligned} T_3+T_0 = &\frac{1}{2}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)} \\ &+\frac{1+i}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\ &+\frac{1-i}{4}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x). \quad (17)\end{aligned}$$

In the following, we will compute the three sums

$$\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}, \qquad \sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x),$$

and

$$\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x).$$

First, by Lemma 3.7 we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)} &= \sum_{x\in\mathbb{F}_{3^n}}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}-\omega^{\mathrm{Tr}_n(0)} \\ &= -3^k\omega^{-\mathrm{Tr}_k(c)}-1 \\ &= -3^k\omega^{\mathrm{Tr}_n(c)}-1. \quad (18)\end{aligned}$$

Next we will compute $\sum_{x\in\mathbb{F}_{3^n}^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x)$.

To simplify notation we write $L=\mathbb{F}_{3^n}$, and $g_L(\chi)=\sum_{x\in\mathbb{F}_{3^n}^*}\chi(x)\omega^{\mathrm{Tr}_n(x)}$. Then

$$\omega^{\mathrm{Tr}_n(x)}=\frac{1}{3^n-1}\sum_{\chi\in\widehat{L^*}}g_L(\chi)\overline{\chi}(x).$$

With this notation, we have

$$\begin{aligned}&\sum_{x\in L^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\ &=\sum_{x\in L^*}\eta(x)\omega^{\mathrm{Tr}_n(-cx^{3^k+1})}\omega^{\mathrm{Tr}_n(cx)} \\ &=\sum_{x\in L^*}\eta(x) \\ &\quad\times\frac{1}{3^n-1}\sum_{\chi_1\in\widehat{L^*}}g_L(\chi_1)\overline{\chi_1}(-cx^{3^k+1}) \\ &\quad\times\frac{1}{3^n-1}\sum_{\chi_2\in\widehat{L^*}}g_L(\chi_2)\overline{\chi_2}(cx) \\ &=\frac{1}{(3^n-1)^2}\sum_{\chi_1}\sum_{\chi_2}g_L(\chi_1)g_L(\chi_2)\overline{\chi_1}(-c)\overline{\chi_2}(c) \\ &\quad\times\sum_{x\in L^*}\eta(x)\overline{\chi_1}(x^{3^k+1})\overline{\chi_2}(x) \\ &=\frac{1}{(3^n-1)^2}\sum_{\chi_1}\sum_{\chi_2}g_L(\chi_1)g_L(\chi_2)\overline{\chi_1}(-c)\overline{\chi_2}(c) \\ &\quad\times\sum_{x\in L^*}\overline{\chi_1}^{3^k+1}(x)\overline{\chi_2}(x)\eta(x).\end{aligned}$$

If $\chi_2=\overline{\chi_1}^{3^k+1}\eta$, then $\overline{\chi_1}^{3^k+1}(x)\overline{\chi_2}(x)\eta(x)=1$ holds for all $x\in L^*$. Otherwise

$$\sum_{x\in L^*}\overline{\chi_1}^{3^k+1}(x)\overline{\chi_2}(x)\eta(x)=0.$$

Thus,

$$\begin{aligned}&\sum_{x\in L^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\ &=\frac{1}{3^n-1}\sum_{\chi_1}g_L(\chi_1)g_L(\overline{\chi_1}^{3^k+1}\eta)\overline{\chi_1}(-c)\chi_1^{3^k+1}(c)\overline{\eta}(c) \\ &=\frac{\overline{\eta}(c)}{3^n-1}\sum_{\chi_1}g_L(\chi_1)g_L(\overline{\chi_1}^{3^k+1}\eta)\chi_1(-c).\end{aligned}$$

So

$$\begin{aligned}&\sum_{x\in L^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta(x) \\ &=\frac{\overline{\eta}(c)}{3^n-1}\sum_{b=0}^{3^n-2}g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3^{2k}-1}{4}})\omega_{\mathfrak{p}}^{-b}(-c), \quad (19)\end{aligned}$$

where $\mathfrak{p}$ is a prime ideal in $\mathbb{Z}[\xi_{q-1}]$ lying above 3 and $\omega_{\mathfrak{p}}$ is the Teichmüller character of L.

Similarly, we can compute $\sum_{x\in L^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x)$ as follows:

$$\begin{aligned}&\sum_{x\in L^*}\omega^{\mathrm{Tr}_n(-cx^{3^k+1}+cx)}\eta^3(x) \\ &=\frac{1}{(3^n-1)^2}\sum_{\chi_1}\sum_{\chi_2}g_L(\chi_1)g_L(\chi_2)\overline{\chi_1}(-c)\overline{\chi_2}(c) \\ &\quad\times\sum_{x\in L^*}\overline{\chi_1}^{3^k+1}(x)\overline{\chi_2}(x)\eta^3(x) \\ &=\frac{\overline{\eta^3}(c)}{3^n-1}\sum_{\chi_1}g_L(\chi_1)g_L(\overline{\chi_1}^{3^k+1}\eta^3)\chi_1(-c) \\ &=\frac{\overline{\eta^3}(c)}{3^n-1}\sum_{b=0}^{3^n-2}g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3(3^{2k}-1)}{4}})\omega_{\mathfrak{p}}^{-b}(-c). \\ &\qquad (20)\end{aligned}$$

In what follows, we will use (19) and (20) to express all relevant quantities in terms of the two sums

$$E_1=\sum_{b=0}^{3^n-2}g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3^{2k}-1}{4}})\omega_{\mathfrak{p}}^{-b}(-c)$$

and

$$E_3=\sum_{b=0}^{3^n-2}g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3(3^{2k}-1)}{4}})\omega_{\mathfrak{p}}^{-b}(-c).$$

If $\beta^{-1}\in C_0$, then by (13), (14), (18), (19) and (20), we have

$$\begin{aligned}S_a(b)&=(1-\omega^{\mathrm{Tr}_k(c)})(T_0+T_1+\frac{3^k+1}{2})-3^k \\ &=(1-\omega^{\mathrm{Tr}_k(c)})[-\frac{1}{2}3^k\omega^{\mathrm{Tr}_n(c)}+\frac{3^k}{2} \\ &\quad+\frac{1-i}{4}\frac{\overline{\eta}(c)}{3^n-1}E_1+\frac{1+i}{4}\frac{\overline{\eta^3}(c)}{3^n-1}E_3]-3^k. \quad (21)\end{aligned}$$

Since $S_a(0) = -3^k$, we have

$$\begin{aligned} &S_a(b) - S_a(0) \\ &\quad = (1-\omega^{\mathrm{Tr}_k(c)})[-\frac{1}{2}3^k\omega^{\mathrm{Tr}_n(c)} + \frac{3^k}{2} \\ &\quad\quad + \frac{1-i}{4}\frac{\overline{\eta}(c)}{3^n-1}E_1 + \frac{1+i}{4}\frac{\overline{\eta^3}(c)}{3^n-1}E_3]. \end{aligned} \tag{22}$$

Similarly, when $\beta^{-1} \in C_1$, we have

$$\begin{aligned} &S_a(b) - S_a(0) \\ &\quad = (1-\omega^{\mathrm{Tr}_k(c)})[-\frac{1}{2}3^k\omega^{\mathrm{Tr}_n(c)} + \frac{3^k}{2} \\ &\quad\quad + \frac{-i-1}{4}\frac{\overline{\eta}(c)}{3^n-1}E_1 + \frac{i-1}{4}\frac{\overline{\eta^3}(c)}{3^n-1}E_3], \end{aligned} \tag{23}$$

when $\beta^{-1} \in C_2$, we have

$$\begin{aligned} &S_a(b) - S_a(0) \\ &\quad = (1-\omega^{\mathrm{Tr}_k(c)})[-\frac{1}{2}3^k\omega^{\mathrm{Tr}_n(c)} + \frac{3^k}{2} \\ &\quad\quad + \frac{-1+i}{4}\frac{\overline{\eta}(c)}{3^n-1}E_1 + \frac{-i-1}{4}\frac{\overline{\eta^3}(c)}{3^n-1}E_3], \end{aligned} \tag{24}$$

and when $\beta^{-1} \in C_3$, we have

$$\begin{aligned} &S_a(b) - S_a(0) \\ &\quad = (1-\omega^{\mathrm{Tr}_k(c)})[-\frac{1}{2}3^k\omega^{\mathrm{Tr}_n(c)} + \frac{3^k}{2} \\ &\quad\quad + \frac{1+i}{4}\frac{\overline{\eta}(c)}{3^n-1}E_1 + \frac{1-i}{4}\frac{\overline{\eta^3}(c)}{3^n-1}E_3]. \end{aligned} \tag{25}$$

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_3]$ lying above $\mathfrak{p}$. Since $\nu_{\mathfrak{P}}(3) = 2$, we see that

$$\nu_3(S_a(b) - S_a(0) > \frac{n}{2} \iff \nu_{\mathfrak{P}}(S_a(b) - S_a(0)) > n = 2k.$$

Note that $\omega^{\mathrm{Tr}_k(c)} = 1$, ω or ω^2. Hence $\nu_{\mathfrak{P}}(1-\omega^{\mathrm{Tr}_k(c)}) = \infty$ or 1. Using the expressions of $S_a(b) - S_a(0)$ in (22), (23), (24), and (25), we see that $\nu_{\mathfrak{P}}(S_a(b) - S_a(0)) > n$ if

$$\begin{aligned} &\nu_{\mathfrak{P}}(E_1) = \\ &\nu_{\mathfrak{P}}\left(\sum_{b=0}^{3^n-2} g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3^{2k}-1}{4}})\omega_{\mathfrak{p}}^{-b}(-c)\right) \geq 2k \end{aligned} \tag{26}$$

and

$$\begin{aligned} &\nu_{\mathfrak{P}}(E_3) = \\ &\nu_{\mathfrak{P}}\left(\sum_{b=0}^{3^n-2} g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3(3^{2k}-1)}{4}})\omega_{\mathfrak{p}}^{-b}(-c)\right) \geq 2k. \end{aligned} \tag{27}$$

By Theorem 2.1 and the fact that $g_L(\chi_0) = -1$, where χ_0 is the trivial multiplicative character of $\mathbb{F}_{3^n}$, we have for any b, $0 \leq b \leq 3^n - 2$ that

$$\begin{aligned} &\nu_{\mathfrak{P}}\left(g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3^{2k}-1}{4}})\omega_{\mathfrak{p}}^{-b}(-c)\right) \\ &\qquad\qquad = w(b) + w\left(-(3^k+1)b - \frac{3^{2k}-1}{4}\right) \end{aligned}$$

and

$$\begin{aligned} &\nu_{\mathfrak{P}}\left(g_L(\omega_{\mathfrak{p}}^{-b})g_L(\omega_{\mathfrak{p}}^{(3^k+1)b+\frac{3(3^{2k}-1)}{4}})\omega_{\mathfrak{p}}^{-b}(-c)\right) \\ &\qquad\qquad = w(b) + w\left(-(3^k+1)b - \frac{3\left(3^{2k}-1\right)}{4}\right). \end{aligned}$$

Therefore if we can prove that for each b, $0 \leq b \leq q-2$,

$$w(b) + w\left(-(3^k+1)b - \frac{3^{2k}-1}{4}\right) \geq 2k \tag{28}$$

and

$$w(b) + w\left(-(3^k+1)b - \frac{3\left(3^{2k}-1\right)}{4}\right) \geq 2k, \tag{29}$$

then $\nu_3(S_a(b) - S_a(0)) > n/2$; and it follows that f is weakly regular bent by Lemma 2.2. We will give proofs of (28) and (29) in the next two sections, which will complete the proof of Theorem 1.4 ■

IV. THE p-ARY MODULAR ADD-WITH-CARRY ALGORITHM

In a sequence of papers [10] [15] [16] [1] a systematic method has been developed to derive binary weight inequalities. Here we generalize this approach to p-ary weight inequalities. As in the binary case, the idea is to analyze the digit-wise contributions to the weights in the inequality using the carries generated by a modular add-with-carry algorithm for the p-ary numbers involved. Essentially, this approach enables the analysis of the *global* properties of the weights in terms of *local*, digit-wise contributions.

Then, these local contributions can be analyzed *for all word lengths simultaneously* in a *finite* weighted directed graph that models these local contributions. This graph has the property that valid modular add-with-carry computations are in one-to-one correspondence with directed closed walks in the graph. In this way, the original weight inequality gets transformed into a bound on the sum of the arc-weights of directed closed walks in this graph as a function of the length of the walk. In principle, such a bound can then be verified by inspection, either directly (if the graph is sufficiently small) or with the aid of a computer. Alternatively, a detailed analysis of the properties of the graph, possibly with the aid of a computer, can be used to devise a mathematical proof (although such proofs can be quite tedious, see e.g. [18]).

We start with the derivation of the p-ary modular add-with-carry algorithm. Our aim is to prove the following theorem.

Theorem 4.1 (Modular p-ary add-with-carry algorithm): Let $a^{(1)}, \ldots, a^{(m)}$ be m integers, and let the integer s satisfy

$$s \equiv t_1 a^{(1)} + t_2 a^{(2)} + \cdots + t_m a^{(m)} \bmod p^n - 1.$$

for some nonzero integers $t_1, t_2, \ldots, t_m$. Suppose that s and $a^{(1)}, \ldots, a^{(m)}$ have p-ary representations $s = \sum_{i=0}^{n-1} s_i p^i$ and

$a^{(j)}=\sum_{i=0}^{n-1} a_i^{(j)}p^i$ for $j=1,\ldots,m$, where the p-ary digits s_i and $a_i^{(j)}$ are integers in $\{0,1,\ldots,p-1\}$. Then there exists a *unique* integer sequence $c=c_{-1},c_0,\ldots,c_{n-1}$ with $c_{-1}=c_{n-1}$ such that

$$pc_i+s_i=c_{i-1}+\sum_{j=1}^{m} t_j a_i^{(j)} \quad (0\le i\le n-1). \tag{30}$$

Moreover, if we define

$$t_+=\sum_{\substack{j=1\\ t_j>0}}^{m} t_j, \qquad t_-=\sum_{\substack{j=1\\ t_j<0}}^{m} t_j,$$

then $t_- -1\le c_i\le t_+$, and furthermore

$$t_-\le c_i\le t_+-1 \tag{31}$$

for $i=0,\ldots,n-1$ provided that $a^{(j)}\not\equiv 0 \bmod p^n-1$ for some $j=1,\ldots,m$. As a consequence, the value $w(c)=c_0+\cdots+c_{n-1}$, the weight $w(s)=s_0+\cdots+s_{n-1}$ of s, and the weights $w(a^{(j)})=a_0^{(j)}+\cdots+a_{n-1}^{(j)}$ of the $a^{(j)}$ satisfy

$$(p-1)w(c)=\sum_{j=1}^{m} t_j w(a^{(j)})-w(s). \tag{32}$$

We will usually refer to the s_i and c_i as the (p-ary) *digits* and *carries* for the computation modulo p^n-1 of the number s. We emphasize that the non-obvious part of Theorem 4.1 is the existence of a carry sequence with $c_{n-1}=c_{-1}$: otherwise (30) represents the ordinary p-ary add-with-carry algorithm. To stress the periodic nature of this *modular* add-with-carry algorithm, we will often consider all indices modulo n.

There are various ways to prove this theorem. Here we will derive it from the following simple technical lemma.

Lemma 4.2: Let $r_0,r_1,\ldots,r_{n-1}$ be an integer sequence. For all j, write

$$r(j)=\sum_{i=0}^{n-1} r_{i+j}p^i,$$

where the indices are to be interpreted modulo n. Then there exists an integer sequence $c=c_{-1},c_0,c_1,\ldots,c_{n-1}$ with $c_{-1}=c_{n-1}$ such that

$$pc_i=r_i+c_{i-1} \tag{33}$$

for $i=0,\ldots,n-1$ if and only if $r(0)\equiv 0 \bmod p^n-1$. In that case, we have

$$c_{j-1}=r(j)/(p^n-1) \tag{34}$$

for $j=0,\ldots,n-1$; in particular, the solution is *unique*. Moreover, the "weights" $w(r)=r_0+\cdots+r_{n-1}$ and $w(c)=c_0+\cdots+c_{n-1}$ of r and c satisfy

$$(p-1)w(c)=w(r). \tag{35}$$

Proof: Suppose that (33) holds for $i=0,\ldots,n-1$, with $c_{-1}=c_{n-1}$. Write

$$c(j)=\sum_{i=0}^{n-1} c_{i+j}p^i,$$

where the indices of c are to be interpreted modulo n. Then

$$\begin{aligned} pc(j) &= r(j)+\sum_{i=0}^{n-1} c_{i-1+j}p^i\\ &= r(j)+pc(j)+c_{j-1}-p^n c_{j+n-1}\\ &= r(j)+pc(j)-c_{j-1}(p^n-1), \end{aligned}$$

hence $r(j)=c_{j-1}(p^n-1)$ for all j. So $r(j)\equiv 0 \bmod p^n-1$ and $c_{j-1}=r(j)/(p^n-1)$ for all j; in particular, we have that $r(0)\equiv 0 \bmod p^n-1$.

Conversely, suppose that $r(0)\equiv 0 \bmod p^n-1$. Then obviously $p^j r(j)\equiv r(0)\equiv 0 \bmod p^n-1$, so that $r(j)\equiv 0 \bmod p^n-1$ for all j. Hence the sequence $c_{-1},c_0,\ldots,c_{n-1}$ defined by (34) is an integer sequence, with $c_{-1}=c_{n-1}$ by definition, and it is easily verified that this sequence indeed satisfies (33) for $i=0,\ldots,n-1$. Finally, the equation (35) follows directly from (33) by summing (33) for $i=0,\ldots,n-1$. ■

Remark 4.3: If we associate polynomials $r(x)=r_0+r_1x+\cdots+r_{n-1}x^{n-1}$ and $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ with the sequences r and c, then (33) can be read as

$$r(x)+(x-p)c(x)\equiv 0 \bmod x^n-1.$$

If p is not a zero of x^n-1, that is, if $p^n\ne 1$, then for each r there is a unique solution c. Since $\gamma(x)=(p^{n-1}+p^{n-2}x+\cdots+px^{n-2}+x^{n-1})/(p^n-1)$ satisfies

$$(p-x)\gamma(x)\equiv 1 \bmod x^n-1,$$

the solution c is given by

$$c(x)=\sum_{i=0}^{n-1} r_i\gamma(x)x^i.$$

This approach provides an alternative proof of the lemma.

Proof ot Theorem 4.1: Define $r_i=-s_i+\sum_{j=1}^{k} t_j a_i^{(j)}$ for $i=0,\ldots,n-1$. Since

$$r(0)=-s+\sum_{j=1}^{k} t_j a^{(j)}\equiv 0 \bmod p^n-1,$$

both the existence and uniqueness of the carry sequence $c_{-1},\ldots,c_{n-1}$ satisfying (30), as well as the relation (32), follows from Lemma 4.2. To obtain the bounds on the carries c_i, simply note that

$$(p^n-1)t_- -(p^n-1)\le r(j)\le (p^n-1)t_+$$

holds for all j. Moreover, since all t_j are assumed to be nonzero, if equality holds in either of these bounds then s and each $a^{(j)}$ is congruent to 0 modulo p^n-1. ■

V. The weight inequalities

We will now use Theorem 4.1 for a local analysis of the weight inequalities (28) and (29). We begin by analyzing the ternary representations of the two constants

$$u=(3^{2k}-1)/4, \qquad v=3(3^{2k}-1)/4 \tag{36}$$

occurring in (28) and (29). Write

$$z=(3^{2k}-1)/8.$$

Lemma 5.1: The numbers z, u, v are all integers, with $0 \leq z, u, v < 3^{2k}-1$, and $u = 2z$, $v = 3u$, and $3u \equiv -u \equiv v \bmod 3^{2k}-1$. Moreover, if $z = z_{2k-1}\cdots z_0$, $u = u_{2k-1}\cdots u_0$, and $v = v_{2k-1}\cdots v_0$ are the (unique) 3-ary representations of z, u, and v, respectively, then

$$z_{2i} = 1, \qquad z_{2i-1} = 0, \qquad u_i = 2z_i, \qquad v_i = u_{i-1}.$$

In particular, $w(u) = w(v) = 2w(z) = 2k$. Finally, if k is odd, then $3^k u \equiv v$ and $3^k v \equiv u$ modulo $3^{2k}-1$.

Proof: By definition, $z = (3^{2k}-1)/8 = 1 + 3^2 + \cdots + 3^{2k-2}$, so z is integer, and hence $u = 2z$ and $v = 3u$ are also integers. Since also $0 < z < u < v < 3^{2k}-1$, their 3-ary representations are unique and as described in the lemma. This immediately implies that $w(u) = w(v) = 2w(z) = 2k$. Next note that $4u = u + v = 3^{2k}-1 \equiv 0 \bmod 3^{2k}-1$; hence $3u \equiv -u \equiv v$ and $3v \equiv -v \equiv u$ modulo $3^{2k}-1$. As a consequence, if k is odd, then $3^k u \equiv 3u \equiv -u \equiv v \bmod 3^{2k}-1$ and $3^k v \equiv u \bmod 3^{2k}-1$. ■

Now let b be any integer. Suppose that k is odd. Then $3^k u \equiv v \bmod 3^{2k}-1$ by Lemma 5.1. Hence if s satisfies

$$s \equiv -(3^k+1)b - u \bmod 3^{2k}-1,$$

then $t = 3^k s$ satisfies

$$t \equiv -(3^k+1)b - v \bmod 3^{2k}-1.$$

Now the ternary representation of t is just a cyclic shift of that of s, hence $w(s) = w(t)$ (this is also correct if $s \equiv t \equiv 0 \bmod 3^{2k}-1$), and so the two weight inequalities (28) and (29) are in fact equivalent.

We want to prove these two weight inequalities by analyzing the contribution to the weights from individual ternary digits of b. To this end, we will apply Theorem 4.1 to the addition $s \equiv -b - a + v \bmod 3^{2k}-1$, where $a = 3^k b$, with the aim to prove the weight inequality $w(b) + w(s) \geq 2k$. (For technical reasons, we will prefer this form of the addition, which has the same outcome s as the earlier one since $-u \equiv v \bmod 3^{2k}-1$). However, the i^{th} digit $a_i = b_{i+k}$ (indices modulo $2k$) of a and the i^{th} digit b_i of b are entirely unrelated, so a straightforward local analysis is doomed to fail. This is a standard problem when investigating p-ary weight inequalities, see for example several cases in [15]. Fortunately, there is a standard solution. First, use the relations between the numbers involved to derive other, equivalent weight inequalities, typically by multiplying the relevant addition by a suitable power of p. Then forget the relation between the numbers, but analyze the resulting weight inequalities (in fact, their addition) *simultaneously*. This approach in general results in a *generalisation* of the original weight inequality.

For the case at hand, the generalization suggested by this approach turns out to be the following.

Theorem 5.2: Let k be any positive integer, and let u and v be defined as in (36). For any integers a and b, if s and t satisfy

$$s \equiv -a - b + v, \qquad t \equiv -a - b + u \bmod 3^{2k}-1,$$

then $w(a) + w(b) + w(s) + w(t) \geq 4k$.
We first show that the original weight inequalities (28) and (29) indeed follow from this result.

Corollary 5.3: Let b be an integer, and let k be odd. Then

$$\begin{aligned} &w(b) + w(-(3^k+1)b - (3^{2k}-1)/4) \\ &\qquad = w(b) + w(-(3^k+1)b - 3(3^{2k}-1)/4) \geq 2k. \end{aligned}$$

Proof: Apply Theorem 5.2 with $a = 3^k b$. Then $w(a) = w(b)$. Also, since k is odd, $3^k u \equiv v \bmod 3^{2k}-1$ by Lemma 5.1; hence

$$3^k s \equiv -3^k(3^k+1)b + 3^k v \equiv -(3^k+1)b + u \equiv t \bmod 3^{2k}-1,$$

so that $w(t) = w(s)$. From the theorem, we now conclude that $w(b) + w(s) = w(b) + w(t) \geq 2k$, as claimed. ■

Proof ot Theorem 5.2: Let s and t be defined as in the theorem, and write $n = 2k$. Assume that a, b, u, v, s, and t have ternary digits a_i, b_i, u_i, v_i, s_i, and t_i, for $i = 0, \ldots, n-1$. According to Lemma 5.1, we have that $u_i = v_{i-1}$ (indices modulo n) and $v_{2i} = 0$, $v_{2i-1} = 2$, for all i. Now apply Theorem 4.1 to the defining additions for s and t. In both cases, $t_+ = 1$ and $t_- = -2$, hence there are carry sequences $c_0, \ldots, c_{n-1}$ and $d_0, \ldots, d_{n-1}$ with $c_{-1} = c_{n-1}$, $d_{-1} = d_{n-1}$, and $-2 \leq c_i, d_i \leq 0$ for all i such that

$$3c_i + s_i \;=\; -a_i - b_i + v_i + c_{i-1} \qquad (37)$$

$$3d_i + t_i \;=\; -a_i - b_i + v_{i-1} + d_{i-1} \qquad (38)$$

for all $i = 0, \ldots, n-1$. Moreover, $2w(c) + w(s) = 2w(d) + w(t) = -w(a) - w(b) + w(v) = -w(a) - w(b) + 2k$. Using these relations, we see that the weight inequality in the theorem is equivalent to

$$w(a) + w(b) + 2w(c) + 2w(d) \leq 0. \qquad (39)$$

In order to analyze the contribution of the individual ternary digits a_i, b_i to the sum of the weights in the left hand side of (39), we construct the following labeled directed graph G.

The graph G will have a vertex (a', b', c', d', v') whenever $a', b' \in \{0,1,2\}$, $c', d' \in \{-2,-1,0\}$, and $v' \in \{0,2\}$, and a weighted directed arc

$$(a', b', c', d', v') \xrightarrow{a'+b'+2c''+2d''} (a'', b'', c'', d'', v'')$$

whenever $v'' = 2 - v'$,

$$s' = -a' - b' + v' + c' - 3c'' \in \{0,1,2\},$$

and

$$t' = -a' - b' + v'' + d' - 3d'' \in \{0,1,2\}.$$

Note that, according to these definitions, whenever (37) holds there is an arc

$$(a_i, b_i, c_{i-1}, d_{i-1}, v_{i-1}) \xrightarrow{a_i+b_i+2c_i+2d_i} (a_{i+1}, b_{i+1}, c_i, d_i, v_i)$$

in the graph. Moreover, since $c_{-1} = c_{n-1}$ and $d_{-1} = d_{n-1}$, there is a one-to-one correspondence between sets of relations (37) for $i = 0, \ldots, n-1$ with corresponding sum of weights $w = w(a) + w(b) + 2w(c) + 2w(d)$ and directed walks of length n in the graph for which the sum of the weights of the arcs equals w.

So we are done if we can show that the weight of each directed walk in the graph G is non-positive. We will show that in fact *all* arc-weights are non-positive. To this end, consider an arc

$$(a',b',c',d',v') \xrightarrow{a'+b'+2c''+2d''} (a'',b'',c'',d'',v''),$$

where $a',b' \in \{0,1,2\}$, $c',d',c'',d'' \in \{-2,-1,0\}$, $v' \in \{0,2\}$, $v''=2-v'$,

$$s' = v' - (a'+b') - 3c'' + c' \in \{0,1,2\},$$

and

$$t' = v'' - (a'+b') - 3d'' + d' \in \{0,1,2\}.$$

Since $s',t' \geq 0$ and $c',d' \leq 0$, we conclude that

$$3c'' \leq v' - (a'+b'), \qquad 3d'' \leq v'' - (a'+b'). \qquad (40)$$

Now consider the arc weight $w = (a'+b') + 2(c''+d'')$. We have that $0 \leq a'+b' \leq 4$. Obviously, if $a'+b'=0$, then $w \leq 0$. If $1 \leq a'+b' \leq 2$, then since $v'=0$ or $v''=0$, at least one of c'' or d'' is negative, and $w \leq 0$ again. Finally, if $3 \leq a'+b' \leq 4$, then both $c'',d'' \leq -1$, and again $w \leq 0$. ■

A close inspection of this proof reveals that in the same way, we can prove the following somewhat stronger result.

Theorem 5.4: Let n be any positive integer. Let u and v be numbers with 3-ary representation $u = u_{n-1}\cdots u_0$ and $v = v_{n-1}\cdots v_0$, respectively, for which $u_i = 0$ or $v_i = 0$ holds for each $i = 0,\ldots,n-1$. If a, b are integers, and s and t satisfy

$$s \equiv -a-b+v, \qquad t \equiv -a-b+u \bmod 3^n-1,$$

then $w(a)+w(b)+w(s)+w(t) \geq w(u)+w(v)$.

References

[1] K.T. Arasu, Henk D.L. Hollmann, Kevin Player, Qing Xiang, On the p-ranks of GMW difference sets, In *Codes and Designs*, Proceedings of the Dijen Ray-Chaudhuri 65th birthday conference, A. Seress and K.T. Arasu (Eds), de Gruyter, 2002, 9–35.

[2] L. D. Baumert, W. H. Mills, R. L. Ward, Uniform Cyclotomy, J. Number Theory **14** (1982), 67-82.

[3] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley Interscience, 1998.

[4] C. Carlet, C. S. Ding, Highly nonlinear mappings, *J. Complexity* **20** (2004), 205–244.

[5] C. Carlet, S. Dubuc, On generalized bent and q-ary perfect nonlinear functions, Finite fields and applications (Augsburg, 1999), 81–94, Springer, Berlin, 2001.

[6] R. S. Coulter, R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.* **10** (1997), 167–184.

[7] P. Delsarte, J. M. Goethals, Tri-weight codes and generalized Hadamard matrices. *Information and Control* **15** (1969), 196–206.

[8] J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D. dissertation, University of Maryland, College Park, 1974.

[9] Cunsheng Ding, Zeying Wang, and Qing Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3,3^{2h+1})$, *J. Combin. Theory* (A) **114** (2007), 867–887.

[10] R. Evans, Henk D.L. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory* (A) **87** (1999), 74–119.

[11] Keqin Feng, Jinquan Luo, Value distributions of exponential sums from perfect nonlinear functions and their applications, *IEEE Trans. Inform. Theory* **53** (2007), 3035-3041.

[12] Tor Helleseth and Alexander Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Transactions on Information Theory* **52** (2006), 2018–2032.

[13] Tor Helleseth and Alexander Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, Report NO 310, Reports in Informatics. Department of Informatics, University of Bergen, Bergen, Norway.

[14] Tor Helleseth and Alexander Kholosha, On the dual of monomial quadratic p-ary bent functions, In *Sequences, Subsequences, and Consequences*, ser. Lecture Notes in Computer Science, S. Golomb, G. Gong, T. Helleseth, and H.-Y. Song, Eds., vol. 4893. Berlin: Springer-Verlag, 2007, 50–61.

[15] Henk D. L. Hollmann, Qing Xiang, A proof of the Welch and Niho conjectures on crosscorrelation of binary m-sequences, *Finite Fields Appl.* **7** (2001), 253–286.

[16] Henk D.L. Hollmann, Qing Xiang, On binary cyclic codes with few weights, Finite fields and applications (Augsburg, 1999), 251–275, Springer, Berlin, 2001.

[17] Xiang-Dong Hou, p-Ary and q-ary versions of certain results about bent functions and resilient functions, *Finite Fields Appl.* **10** (2004), 566-582.

[18] Xiang-dong Hou, A note on the proof of Niho's conjecture, *SIAM J. Discrete Math.*, **18** (2005), 313–319.

[19] Xiang-Dong Hou, On the dual of a Coulter-Matthews bent function, *Finite Fields Appl.*, in press.

[20] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *J. Comb. Theory, Ser. A* **40** (1985), 90-107,.

[21] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

[22] G. Myerson, Period polynomials and Gauss sums, *Acta Arithmetica* **39** (1981), 251-264.

[23] A. Pott, Nonlinear functions in abelian groups and relative difference sets. Optimal discrete structures and algorithms (ODSA 2000). *Discrete Appl. Math.* **138** (2004), no. 1-2, 177–193.

[24] O. S. Rothaus, On "bent" functions, *J. Comb. Theory* (A) **20** (1976), 300–305.

[25] T. Storer, Cyclotomy and Difference Sets. Lectures in Advanced Mathematics. Markham Publishing Company, Chicago 1967.

[26] G. B. Weng, W. S. Qiu, Z. Y. Wang, and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.* **44** (2007), 49–62.

Tor Helleseth (M'89–SM'96–F'97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973 to 1980, he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984, he was at the Chief Headquarters of Defense in Norway. Since 1984, he has been a Professor in the Department of Informatics at the University of Bergen. During the academic years 1977–1978 and 1992–1993, he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979–1980, he was a Research Fellow at the Eindhoven University of Technology, Eindhoven, The Netherlands. His research interests include coding theory and cryptology.

From 1991 to 1993, Prof. Helleseth served as an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY. He was a Program Chairman for Eurocrypt'93 and for the Information Theory Workshops in 1997 in Longyearbyen and in 2007 in Solstrand, Norway. He was also a Program Co-Chairman for SETA conferences. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography. He is currently serving on the Board of Governors for the IEEE Information Theory Society.

Henk D. L. Hollmann was born in Utrecht, the Netherlands, on March 10, 1954. He received the Masters degree in mathematics in 1982, with a thesis on association schemes, and the Ph.D. degree in 1996, with a thesis on modulation codes, both from Eindhoven University of Technology. He was awarded the SNS bank prize 1996/1997 for the best Ph.D. thesis in fundamental research at this university.

In 1982 he joined CNET, Issy-les-Moulineaux, France, where he worked mainly on Number Theoretic Transforms. Since 1985 he is with Philips Research Laboratories, Eindhoven, the Netherlands, currently in the rank of Principal Scientist.

His research interests include discrete mathematics and combinatorics, information theory, cryptography, and digital signal processing.

Alexander Kholosha received the Ph.D. degree in mathematics from the Eindhoven University of Technology, Eindhoven, The Netherlands, in 2003.

He is a Postdoctoral Fellow in the Department of Informatics at the University of Bergen, Bergen, Norway. His research interests lie in the area of cryptology in general and he is particularly interested in cryptographic properties of Boolean and pseudo-Boolean functions, sequences, and key-stream generation for stream ciphers, cryptanalysis. He was a Program Co-Chairman for the International Workshop on Coding and Cryptography 2009 in Ullensvang, Norway.

Zeying Wang received the Ph.D. degree in mathematics from University of Delaware, Newark, Delaware, in 2008. She is currently a Postdoctoral Fellow in the Department of Mathematics at Ohio University, Athens, Ohio. Her research interests lie in the areas of combinatorial designs and coding theory.

Qing Xiang received the Ph.D. degree in mathematics from the Ohio State University, Columbus, Ohio, in 1995. From 1995 to 1997, he was a Bateman Research Instructor in the Department of Mathematics of Caltech. Since 1997, he has been with Department of Mathematical Sciences of University of Delaware, where he was promoted to Professor of Mathematics in 2006.

Qing Xiang was awarded the Kirkman Medal of the Institute of Combinatorics and its Applications in 1999. Since 2006, Professor Xiang has been an Editor-in-Chief of THE ELECTRONIC JOURNAL OF COMBINATORICS. He is also on the editorial board of DESIGNS, CODES AND CRYPTOGRAPHY and JOURNAL OF COMBINATORIAL DESIGNS.