The complete extended differential spectrum of a power map in finite fields of odd characteristics

Constanza Riera[1*], Pantelimon Stănică[2†], Haode Yan[3‡]

[1]Department of Computer Science, Electrical Engineering,
and Mathematical Sciences,
Western Norway University of Applied Sciences,
5020 Bergen, Norway; csr@hvl.no

[2] Department of Applied Mathematics, Naval Postgraduate School,
Monterey, CA 93943-5212, U.S.A.; pstanica@nps.edu

[3] School of Mathematics, Southwest Jiaotong University,
Chengdu 610031, China; hdyan@swjtu.edu.cn

Abstract

The concept of the (scaled) c-differential uniformity found its first application in a paper by Anbar et al. (J. Comb. Des., 2023), where it was shown that the graph of a PcN function corresponds to a difference set in a quasigroup. Further, in a very recent manuscript by Pal and Stănică (Adv. Math. Communic., 2025), a connection was discovered showing that in fact, the boomerang uniformity for an odd APN function in odd characteristic equals its c-differential uniformity when $c = -1$, if the function is a permutation, otherwise it is the maximum of the (-1)-DDT entries, disregarding the first row/column. While we take our inspiration from the extended differentials, our work's goal is to investigate the preimages (these problems tend to be quite difficult, in general) of various polynomials that are obtained via those extended differentials, in odd characteristic. Precisely, in the paper, we concentrate on the map $x \mapsto x^{\frac{p^n+1}{2}}$ on $\mathbb{F}_{p^n}$ and using combinatorial and number theory techniques, we compute its detailed c-differential

*ORCID: 0000-0001-8829-0847
†Corresponding author; ORCID: 0000-0002-8622-7120
‡ORCID: 0000-0001-8144-3433

spectrum for all values of $c \neq 1$ (the spectrum for $c = 1$ is known – see Choi et al. (Finite Fields Appl., 2013)). As a consequence, we find that there are many values of c, where the function has low c-differential uniformity. For example, for $c^2 = -1$, via elliptic curves techniques, we find explicit expressions for the spectrum, and as a consequence, we show that the function is APcN, when n is even and $p \equiv 3, 5, 7 \pmod 8$, or $p \equiv 1 \pmod 8$ (n arbitrary); when $p \equiv 5 \pmod 8$ and n is odd, the c-differential uniformity is 4.

Keywords. differential and c-differential uniformity, cyclotomic numbers, character sums, spectrum, elliptic curves
Mathematics Subject Classification 2020: 11L10, 11T24, 11T71, 12E20, 94A60

1 Introduction and basic definitions

We will introduce here only some basic notations and definitions of Boolean and p-ary functions (where p is an odd prime); the reader can consult [4, 5, 7, 11, 14], for more on these objects and their cryptographic properties.

For a positive integer n and p a prime number, we denote by $\mathbb{F}_p^n$ the n-dimensional vector space over $\mathbb{F}_p$, and by $\mathbb{F}_{p^n}$ the finite field with p^n elements, while $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ will denote the multiplicative group. For $a \neq 0$, we often write $\frac{1}{a}$ to mean the inverse of a in the multiplicative group of the finite field under discussion. We use $\#S$ to denote the cardinality of a set S. We call a function from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ a *p-ary function* on n variables. For positive integers n and m, any map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \to \mathbb{F}_p^m$) is called a *vectorial p-ary function*, or *(n, m)-function*. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i,\ a_i \in \mathbb{F}_{p^n}$, whose *algebraic degree* is then the largest Hamming/p-ary weight of the exponents i with $a_i \neq 0$. To (somewhat) distinguish between the vectorial and single-component output, we shall use upper/lower case to denote the functions.

Throughout, we will use the following notions:

1. The absolute trace Tr_n and the relative trace $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}$ (where $m \,|\, n$), defined as $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^m}}(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$. Whenever clear, we will write q for some power of p.

2. Given a vectorial p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, the derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the p-ary function $D_a f(x) = f(x + a) - f(x),$ for all $x \in \mathbb{F}_{p^n}$.

3. For an (n,m)-function F, and $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, we let $\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - F(x) = b\}$. We call the quantity $\delta_F = \max\{\Delta_F(a,b) : a,b \in \mathbb{F}_{p^n}, a \neq 0\}$ the *differential uniformity* of F. If $\delta_F \leq \delta$, then we say that F is differentially δ-uniform. If $m = n$ and $\delta = 1$, then F is called a *perfect nonlinear* (*PN*) function, or *planar* function. If $m = n$ and $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function. It is well known that PN functions do not exist if $p = 2$.

4. As defined in [8], for an (n,m)-function F, $a \in \mathbb{F}_{p^n}$ and $c \in \mathbb{F}_{p^m}$, the (*multiplicative*) *c-derivative* of F with respect to $a \in \mathbb{F}_{p^n}$ is the function

$$ {}_cD_aF(x) = F(x+a) - cF(x), \text{ for all } x \in \mathbb{F}_{p^n}. $$

   We let the entries of the c-Difference Distribution Table (c-DDT) be defined by ${}_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - cF(x) = b\}$. We call the quantity

$$ {}_c\Delta_F = \max\{{}_c\Delta_F(a,b) \,|\, a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m} \text{ and } a \neq 0 \text{ if } c = 1\} $$

   the *c-differential uniformity* of F.

5. If ${}_c\Delta_F = \delta$, then we say that F is differentially (c,δ)-uniform (or that F has c-uniformity δ, or that F *is δ-uniform c-DDT*). If $\delta = 1$, then F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as shown in [8], there exist PcN functions for $p = 2$, for all $c \neq 1$). If $\delta = 2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function. When we need to specify the constant c for which the function is PcN or APcN, then we may use the notation c-PN, or c-APN. Note that if F is an (n,n)-function, then F is c-PN if and only if ${}_cD_aF$ is a permutation polynomial.

6. As in [17], let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a power function $F(x) = x^d$ with c-differential uniformity ${}_c\Delta_F$. Denote by ${}_c\omega_i = \#\{b \in \mathbb{F}_{p^n} : {}_c\delta_F(1,b) = i\}$. We define the *c-differential spectrum* of F as the multiset $\mathbb{S} = \{{}_c\omega_i : 0 \leq i \leq {}_c\Delta_F \text{ and } {}_c\omega_i > 0\}$.

   NB: Note that, for $a = 0$, for a power function $F(x) = x^d$, where $k = \gcd(d, p^n - 1)$, the equation $F(x+a) - cF(x) = b$ becomes $(1-c)x^d = b$. If $k = 1$, the equation has a unique solution. If $k > 1$, and $b/(1-c) = g^s$, for some s, where g is a primitive element of the field, the equation has solutions (namely k of them) if and only if $k \,|\, s$.

In the computation of the differential or c-differential uniformity for a power function, for $a \neq 0$, we can assume without loss of generality that $a = 1$, since an equation of the form $(x+a)^d - cx^d = b$ is equivalent to $(y+1)^d - c'y^d = b'$, where $y = x/a$, $b' = b/a^d, c' = c/a^d$.

In [17, Theorem 4], it was proved that for any monomial function x^d, for $c \neq 1$, $q = p^n$,

$$\sum_{i=0}^{{}_c\Delta_F} {}_c\omega_i = \sum_{i=0}^{{}_c\Delta_F} (i \cdot {}_c\omega_i) = p^n$$

and

$$\sum_{i=0}^{{}_c\Delta_F} (i^2 \cdot_c \omega_i) = \frac{{}_cN_4 - 1}{p^n - 1} - \gcd(d, p^n - 1),$$

where

$${}_cN_4 = \# \left\{ (x_1, x_2, x_3, x_4) \in (\mathbb{F}_q)^4 : \begin{cases} x_1 - x_2 + x_3 - x_4 = 0 \\ x_1^d - cx_2^d + cx_3^d - x_4^d = 0 \end{cases} \right\}.$$

This gives the relationship between the c-differential spectrum and the number of solutions of a certain system of equations.

7. We will denote by $\eta(\alpha)$ the quadratic character of α (that is, $\eta(\alpha) = 0$ if $\alpha = 0$, $\eta(\alpha) = 1$ if $0 \neq \alpha$ is a square, $\eta(\alpha) = -1$ if α is not a square).

In this paper we are computing precisely the c-differential spectrum of the function $F(x) = x^{\frac{p^n+1}{2}}$ over $\mathbb{F}_{p^n}$. Since some of the proofs are rather long, we will split the analysis in three results, treating the cases $c = 0$, $c = -1$ and $c \neq 0, \pm 1$, separately. We also provide a more explicit result for the particular case $c^2 = -1$. Recall that the spectrum (and differential uniformity) for $c = 1$ is known for this map [6]. As a byproduct, several character sums are explicitly found. We point to [16], where the spectrum for $x^{\frac{p^n-3}{2}}$ was also found.

We include in Appendix A (Table 1) a table of known PcN and APcN monomial functions.

The concept of the c-differential uniformity found its first application in the paper [1], where it was shown that the graph of a PcN function corresponds to a difference set in a quasigroup. Further, in a very recent manuscript by Pal and Stănică [13], a connection was discovered showing that, in fact, the boomerang uniformity for an odd APN function (odd characteristic) equals its c-differential uniformity when $c = -1$, if the function

is a permutation, otherwise it is the maximum of the (-1)-DDT entries disregarding the first row/column.

2 The spectrum of $x^{\frac{p^n+1}{2}}$, p odd prime

Since the case of $c = 1$ was treated in [6], for this function, we assume below that $c \neq 1$. We include here the c-differential uniformity for this function, and we give in the proof a complete characterization of the conditions on b to have any number of solutions for the equation $(x+1)^{\frac{p^n+1}{2}} - cx^{\frac{p^n+1}{2}} = b$, where c varies through the field. We note that this case is not included in [17], who treated the (-1)-spectrum for the function $x^{\frac{p^k+1}{2}}$, under the assumption $\gcd(n,k) = 1$ and $\frac{2n}{\gcd(2n,k)}$ being even.

We will use the following result (see [6]) about the cyclotomic numbers: Let $S_{i,j} = \{0, -1 \neq x \in \mathbb{F}_{p^n} : \eta(x+1) = i, \eta(x) = j\}$, where $i, j \in \{\pm 1\}$. Then, if $\eta(-1) = 1$ (which happens if $p^n \equiv 1 \mod 4$), then $\#S_{1,1} = \frac{p^n-5}{4}$ and $\#S_{-1,1} = \#S_{1,-1} = \#S_{-1,-1} = \frac{p^n-1}{4}$. If $\eta(-1) = -1$ (which happens if $p^n \equiv 3 \mod 4$), then $\#S_{-1,1} = \frac{p^n+1}{4}$ and $\#S_{1,1} = \#S_{1,-1} = \#S_{-1,-1} = \frac{p^n-3}{4}$.

We start with the easy case of $c = 0$.

Theorem 2.1. *Let $F(x) = x^d$, where $d = \frac{p^n+1}{2}$ (for p odd) on $\mathbb{F}_{p^n}$. If $c = 0$, then the function is PcN if $\eta(-1) = 1$, and APcN if $\eta(-1) = -1$, with c-differential spectrum $\left\{ {}_0\omega_0 = \frac{p^n-1}{2}, {}_0\omega_1 = 1, {}_0\omega_2 = \frac{p^n-1}{2} \right\}$.*

Proof. Let $d = \frac{p^n+1}{2} = \frac{p^n-1}{2} + 1$. We look at the equation

$$F(x+1) - cF(x) = b,$$

and so,

$$\begin{aligned} (x+1)^{\frac{p^n+1}{2}} - cx^{\frac{p^n+1}{2}} &= (x+1)^{\frac{p^n-1}{2}+1} - cx^{\frac{p^n-1}{2}+1} \\ &= \eta(x+1)(x+1) - c\eta(x)x = b. \end{aligned} \tag{1}$$

When $c = 0$, Equation (1) becomes $\eta(x+1)(x+1) = b$.

- If $x = -1$, then, $b = 0$.
- Let $\eta(x+1) = 1$. Then, the equation becomes $x + 1 = b$, so $x = b - 1$. This solution is valid if and only if $\eta(b) = 1$.

- Let $\eta(x+1) = -1$. Then, the equation becomes $-x - 1 = b$, so $x = -b - 1$. This solution is valid if and only if $\eta(-b) = -1$.

Therefore, if $\eta(-1) = 1$, then we have a unique solution for every b. The function is then 0-PN (that is, a permutation), so its spectrum is, naturally,

$$\{{}_0\omega_1 = p^n\}.$$

If $\eta(-1) = -1$, then we have a single solution for $b = 0$, two solutions for b such that $\eta(b) = 1$, and no solution otherwise. The function is then 0-APN, with spectrum

$$\left\{{}_0\omega_0 = \frac{p^n - 1}{2},\ {}_0\omega_1 = 1,\ {}_0\omega_2 = \frac{p^n - 1}{2}\right\}.$$

The claim is therefore shown. □

We continue with the more complicated case of $c = -1$.

Theorem 2.2. *Let $F(x) = x^d$, where $d = \frac{p^n+1}{2}$ (for p odd), over $\mathbb{F}_{p^n}, n \geq 1$. If $c = -1$, then the c-differential spectrum is $\left\{{}_{-1}\omega_0 = \frac{p^n-1}{2},\ {}_{-1}\omega_1 = \frac{p^n-3}{2},\ {}_{-1}\omega_{\frac{p^n+3}{4}} = 2\right\}$ if $\eta(-1) = 1$, and $\left\{{}_{-1}\omega_0 = \frac{3p^n-5}{4},\ {}_{-1}\omega_2 = \frac{p^n-3}{4},\ {}_{-1}\omega_{\frac{p^n-3}{4}} = 1,\ {}_{-1}\omega_{\frac{p^n+1}{4}} = 1\right\}$, if $\eta(-1) = -1$.*

Proof. When $c = -1$, Equation (1) becomes

$$\eta(x+1)(x+1) + \eta(x)x = b. \tag{2}$$

Assuming $\eta(-1) = 1$, we get the solutions:

- for $b = 1$, $x = 0$ and all elements $x \in \mathbb{F}_{p^n}$ such that $\eta(x+1) = 1 = -\eta(x)$ (that is, $\#S_{1,-1} = \frac{p^n-2+\eta(-1)}{4} = \frac{p^n-1}{4}$);
- for $b = -1$, $x = -1$ and all elements $x \in \mathbb{F}_{p^n}$ such that $\eta(x+1) = -1 = -\eta(x)$ (that is, $\#S_{-1,1} = \frac{p^n-\eta(-1)}{4} = \frac{p^n-1}{4}$);
- one solution if $\eta(b+1) = \eta(b-1)$, and no solution otherwise.

We get then, for $b = \pm 1$, $\frac{p^n+3}{4}$ solutions for (2).

The spectrum is therefore

$$\begin{aligned} {}_c\omega_0 &= \#\{b \neq \pm 1 : \eta(b+1) \neq \eta(b-1)\} \\ {}_c\omega_1 &= \#\{b \neq \pm 1 : \eta(b+1) = \eta(b-1)\| \end{aligned}$$

$$_c\omega_{\frac{p^n+3}{4}} = \#\{b = \pm 1\} = 2.$$

The c-differential uniformity is then $\frac{p^n+3}{4}$, achieved only in two points. We want to compute the cardinality of $T_{i,j} = \{b \neq \pm 1 : \eta(b-1) = i, \eta(b+1) = j\}$, $i, j \in \{\pm 1\}$. We have that

$$\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1)) = 4\#T_{i,j} + 2 + j\eta(2) + i\eta(-2).$$

On the other hand,

$$\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1)) = p^n + ij \sum_{b \in \mathbb{F}_{p^n}} \eta((b-1)(b+1)).$$

We know [10] that if $f(x) = a_2x^2 + a_1x + a_0$ is a polynomial in a finite field $\mathbb{F}_q$ of odd characteristic, $a_2 \neq 0, d = a_1^2 - 4a_0a_2$, and η is the quadratic character on $\mathbb{F}_q$, then the Jacobsthal sum of f is

$$\sum_{x \in \mathbb{F}_q} \eta(f(x)) = \begin{cases} -\eta(a_2) & \text{if } d \neq 0 \\ (q-1)\eta(a_2) & \text{if } d = 0. \end{cases} \tag{3}$$

To compute $\sum_{b \in \mathbb{F}_{p^n}} \eta((b-1)(b+1))$, we apply (3) and take $f(x) = x^2 - 1$, $d = 4 \neq 0$, and so, the Jacobsthal sum becomes $\sum_{x \in \mathbb{F}_{p^n}} \eta(x^2-1) = -\eta(1) = -1$. Therefore

$$\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1)) = p^n - ij,$$

so

$$\#T_{i,j} = \frac{1}{4}\left(p^n - ij - 2 - j\eta(2) - i\eta(-2)\right).$$

If $\eta(-1) = 1$, then $\#T_{1,1} = \frac{1}{4}(p^n - 3 - 2\eta(2))$, $\#T_{1,-1} = \frac{1}{4}(p^n - 1) = \#T_{-1,1}$, and $\#T_{-1,-1} = \frac{1}{4}(p^n - 3 + 2\eta(2))$ (recall that 2 is a quadratic residue if and only if $p \equiv \pm 1 \pmod 8$, or, $p \equiv \pm 3 \pmod 8$ and n even).

Thus,

$$_c\omega_0 = \#\{b \neq \pm 1 : \eta(b+1) \neq \eta(b-1)\} = \#T_{1,-1} + \#T_{-1,1} = \frac{p^n - 1}{2},$$
$$_c\omega_1 = \#\{b \neq \pm 1 : \eta(b+1) = \eta(b-1)\} = \#T_{1,1} + \#T_{-1,-1} = \frac{p^n - 3}{2},$$

and thus, the spectrum becomes

$$\left\{ {}_c\omega_0 = \frac{p^n-1}{2},\ {}_c\omega_1 = \frac{p^n-3}{2},\ {}_c\omega_{\frac{p^n+3}{4}} = 2 \right\}. \tag{4}$$

For $\eta(-1) = -1$, we get, for $b = 1$, $x = 0$, $x = -1$, and all elements $x \in \mathbb{F}_{p^n}$ such that $\eta(x+1) = 1 = -\eta(x)$ (that is, $\#S_{1,-1} = \frac{p^n-2+\eta(-1)}{4} = \frac{p^n-3}{4}$); for $b = -1$, all elements $x \in \mathbb{F}_{p^n}$ such that $\eta(x+1) = -1 = -\eta(x)$ (that is, $\#S_{-1,1} = \frac{p^n-\eta(-1)}{4} = \frac{p^n+1}{4}$); two solutions if $\eta(b+1) = \eta(b-1) = \eta(2)$, and no solution, otherwise. The spectrum is then:

$$\begin{aligned}
{}_c\omega_2 &= \#\{b \neq \pm 1 : \eta(b+1) = \eta(b-1) = \eta(2)\} \\
{}_c\omega_0 &= \#\{b \neq \pm 1 : b \notin c_{\omega_2}\} \\
{}_c\omega_{\frac{p^n-3}{4}} &= \#\{b = 1\} = 1 \\
{}_c\omega_{\frac{p^n+1}{4}} &= \#\{b = -1\} = 1.
\end{aligned}$$

If $\eta(-1) = -1$, then $\#T_{1,1} = \frac{1}{4}(p^n - 3) = \#T_{-1,-1}$, $\#T_{1,-1} = \frac{1}{4}(p^n - 1 + 2\eta(2))$ and $\#T_{-1,1} = \frac{1}{4}(p^n - 1 - 2\eta(2))$. Then:

$$\begin{aligned}
{}_c\omega_2 &= \#\{b \neq \pm 1 : \eta(b+1) = \eta(b-1) = \eta(2)\} = \frac{1}{4}(p^n - 3), \\
{}_c\omega_0 &= \#\{b \neq \pm 1 : b \notin c_{\omega_2}\} = p^n - 2 - \frac{1}{4}(p^n - 3) = \frac{3p^n - 5}{4}.
\end{aligned}$$

The c-differential uniformity is then $\frac{p^n+1}{4}$, achieved only in one point, and the spectrum is then

$$\left\{ {}_c\omega_0 = \frac{3p^n-5}{4},\ {}_c\omega_2 = \frac{p^n-3}{4},\ {}_c\omega_{\frac{p^n-3}{4}} = 1,\ {}_c\omega_{\frac{p^n+1}{4}} = 1 \right\}. \tag{5}$$

The theorem is therefore shown. □

Using our above counts and [17, Theorem 4], we have the following corollary:

Corollary 2.1. *The number of solutions $(x_1, x_2, x_3, x_4) \in (\mathbb{F}_{p^n})^4$ of the following system of equations*

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0 \\ x_1^d + x_2^d - x_3^d - x_4^d = 0 \end{cases}$$

for $d = \frac{p^n+1}{2}$ is $\frac{1}{8}(p^{3n} + 9p^{2n} - 5p^n + 3)$ when $\eta(-1) = 1$, and is $\frac{1}{8}(p^{3n} + 5p^{2n} - 17p^n + 19)$ when $\eta(-1) = -1$.

We continue with the $c \neq 0, \pm 1$ cases under $\eta(-1) = 1$ (that is, $p \equiv 1 \pmod 4$, or $p \equiv 3 \pmod 4$ and n even). For $c \in \mathbb{F}_{p^n}$ fixed, we will need the following elliptic curve $E(\mathbb{F}_{p^n}) : y^2 = x(x-1)(x-c^2)$ over the field $\mathbb{F}_{p^n}$. We shall be using the standard notations for elliptic curves, which the readers can find in their favorite books on the subject, such as [15]. By the Hasse-Weil inequality [15, Corollary 4.15], we know that $|\#E(\mathbb{F}_{p^n}) - (p^n + 1)| \leq 2\sqrt{p^n}$.

We denote by $a_{p^n}^{(c)} = \#E(\mathbb{F}_{p^n}) - (p^n + 1)$ the Frobenius trace (as it can be interpreted as the trace of the Frobenius endomorphism of the elliptic curve), and use this notation in the following theorem:

Theorem 2.3. *Let $F(x) = x^d$, where $d = \frac{p^n+1}{2}$, over $\mathbb{F}_{p^n}, n \geq 1$, p odd prime. If $c \neq 0, \pm 1$ and $\eta(-1) = 1$, then the c-differential spectrum of F is the following*:

(*i*) *If $\eta(1 - c^2) = 1$, then*

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}\left(p^n + a_{p^n}^{(c)} + 5\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(3p^n - a_{p^n}^{(c)} - 5\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(p^n + a_{p^n}^{(c)} + 5\right).
\end{aligned}
$$

Note that this implies that the function is APcN for those values of c.

(*ii*) *If $\eta(1 - c) = 1, \eta(1 + c) = -1$, then*

$$
\begin{aligned}
{}_c\omega_1 &= \frac{1}{4}\left(p^n + a_{p^n}^{(c)} + 1\right) + \begin{cases} 2, & \eta(2) = 1, \eta(c) = 1 \\ 1, & \eta(c) = -1 \\ 0, & \eta(2) = -1, \eta(c) = 1, \end{cases} \\
{}_c\omega_2 &= \frac{1}{4}\left(p^n - a_{p^n}^{(c)} - 7\right), \\
{}_c\omega_3 &= \begin{cases} 1, & \eta(c) = -1 \\ 0, & \eta(c) = 1, \end{cases} \\
{}_c\omega_4 &= \frac{1}{16}\left(p^n + a_{p^n}^{(c)} - 3 - 4\eta(2)(1 + \eta(c))\right), \\
{}_c\omega_0 &= p^n - ({}_c\omega_1 +_c \omega_2 +_c \omega_3 +_c \omega_4).
\end{aligned}
$$

(*iii*) *If $\eta(1 - c) = -1, \eta(1 + c) = 1$, then*

$$
{}_c\omega_1 = \frac{1}{4}\left(p^n + a_{p^n}^{(c)} + 1\right) + \begin{cases} 0, & \eta(2) = 1, \eta(c) = 1 \\ 1, & \eta(c) = -1 \\ 2, & \eta(2) = -1, \eta(c) = 1, \end{cases}
$$

$$
\begin{aligned}
{}_c\omega_2 &= \frac{1}{4}\left(p^n - a_{p^n}^{(c)} - 7\right), \\
{}_c\omega_3 &= \begin{cases} 2, & \eta(2) = 1, \eta(c) = 1 \\ 1, & \eta(c) = -1 \\ 0, & \eta(2) = -1, \eta(c) = 1, \end{cases} \\
{}_c\omega_4 &= \frac{1}{16}\left(p^n + a_{p^n}^{(c)} - 3 + 4\eta(2)(1+\eta(c))\right), \\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

Proof. When $c \neq 0, \pm 1$, we analyze the possible solutions for (1):

- If $x_1 = 0$ is a solution, then $b = 1$, otherwise, 0 is not a solution.
- If $x_2 = -1$ is a solution, then $b/c = \eta(-1) = 1$, otherwise -1 is not a solution.
- Let $\eta(x+1) = 1 = \eta(x)$. Then:

$$
\begin{aligned}
(1-c)x + 1 = b, \text{ and so, } x_3 = \frac{b-1}{1-c}, \text{ thus,} \\
\eta(x_3) = \eta(b-1)\eta(1-c), \\
\eta(x_3+1) = \eta(b-c)\eta(1-c).
\end{aligned}
$$

- Let $\eta(x+1) = -1 = \eta(x)$. Then:

$$
\begin{aligned}
-(1-c)x - 1 = b, \text{ and so, } x_4 = -\frac{b+1}{1-c} \\
\eta(x_4) = \eta(-1)\eta(b+1)\eta(1-c), \\
\eta(x_4+1) = \eta(-1)\eta(b+c)\eta(1-c).
\end{aligned}
$$

- Let $\eta(x+1) = 1 = -\eta(x)$. Then:

$$
\begin{aligned}
(1+c)x + 1 = b, \text{ and so, } x_5 = \frac{b-1}{1+c}, \\
\eta(x_5) = \eta(b-1)\eta(1+c), \\
\eta(x_5+1) = \eta(b+c)\eta(1+c).
\end{aligned}
$$

- Let $\eta(x+1) = -1 = -\eta(x)$. Then:

$$
\begin{aligned}
(-1-c)x - 1 = b, \text{ and so, } x_6 = \frac{b+1}{-1-c}, \\
\eta(x_6) = \eta(-1)\eta(b+1)\eta(1+c), \\
\eta(x_6+1) = \eta(-1)\eta(b-c)\eta(1+c).
\end{aligned}
$$

Case A. $\eta(1-c) = 1 = \eta(1+c)$ $(c \neq 0, \pm 1)$. Then:

$$\begin{aligned}
&\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1,\\
&\eta(x_4) = \eta(-1)\eta(b+1) = -1, \eta(x_4+1) = \eta(-1)\eta(b+c) = -1,\\
&\eta(x_5) = \eta(b-1) = -1, \eta(x_5+1) = \eta(b+c) = 1,\\
&\eta(x_6) = \eta(-1)\eta(b+1) = 1, \eta(x_6+1) = \eta(-1)\eta(b-c) = -1.
\end{aligned}$$

Case A1. $\eta(-1) = 1$. Then:

$$\begin{aligned}
&\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1,\\
&\eta(x_4) = \eta(b+1) = -1, \eta(x_4+1) = \eta(b+c) = -1,\\
&\eta(x_5) = \eta(b-1) = -1, \eta(x_5+1) = \eta(b+c) = 1,\\
&\eta(x_6) = \eta(b+1) = 1, \eta(x_6+1) = \eta(b-c) = -1.
\end{aligned}$$

We see that, for a fixed b, if x_3 exists, then x_5 and x_6 cannot exist, and vice-versa. Also, if x_4 exists, then x_5 and x_6 cannot exist, and vice-versa. We can therefore have at most two solutions, namely x_3 and x_4 or x_5 and x_6.

NB: For $b = -1$, if $\eta(2) = 1$ (that is, $p \equiv \pm 1 \pmod 8$, or, $p \equiv \pm 3 \pmod 8$ and n even), we get a solution x_3. If $\eta(2) = -1$ (that is, $p \equiv \pm 1 \pmod 8$ or n odd), we get a solution x_5. Regardless, we can see that $b = -1$ gives one solution. For $b = -c$, if $\eta(2c) = 1$, we get a solution x_3. If $\eta(2c) = -1$, we get a solution x_6. Regardless, we can see that $b = -c$ gives one solution.

For c fixed, and $i, j, u, v \in \{\pm 1\}$, we define the following intersection of cyclotomic sets,

$$S^c_{i,j,u,v} = \{b \neq \pm 1, \pm c : (\eta(b-1), \eta(b+1), \eta(b-c), \eta(b+c)) = (i, j, u, v)\}.$$

We note the following distribution, which depends on the existence of such a b for each fixed c:

$$\begin{aligned}
{}_c\omega_0 &= \#(S^c_{1,-1,-1,1} \cup S^c_{-1,1,1,-1}),\\
{}_c\omega_2 &= \#(S^c_{1,-1,1,-1} \cup S^c_{-1,1,-1,1}),\\
{}_c\omega_1 &= p^n - ({}_c\omega_0 + {}_c\omega_2).
\end{aligned}$$

Case B. $\eta(1-c) = -1 = \eta(1+c)$ (thus, $c \neq \pm 1$). In this case, all the above equations change sign, which implies the same compatibilities. The distribution is then given as above, with the values of $\eta(b-1), \eta(b+1), \eta(b-c), \eta(b+c)$ of opposite sign, giving:

Case B1. $\eta(-1) = 1$:

$$
\begin{aligned}
{}_c\omega_0 &= \#(S^c_{1,-1,-1,1} \cup S^c_{-1,1,1,-1}),\\
{}_c\omega_2 &= \#(S^c_{1,-1,1,-1} \cup S^c_{-1,1,-1,1}),\\
{}_c\omega_1 &= p^n - ({}_c\omega_0 + {}_c\omega_2).
\end{aligned}
$$

Case C. $\eta(1-c) = 1 = -\eta(1+c)$ (thus, $c \neq \pm 1$):

$$
\begin{aligned}
&\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1,\\
&\eta(x_4) = \eta(-1)\eta(b+1) = -1, \eta(x_4+1) = \eta(-1)\eta(b+c) = -1,\\
&\eta(x_5) = -\eta(b-1) = -1, \eta(x_5+1) = -\eta(b+c) = 1,\\
&\eta(x_6) = -\eta(-1)\eta(b+1) = 1, \eta(x_6+1) = -\eta(-1)\eta(b-c) = -1.
\end{aligned}
$$

Case C1. $\eta(-1) = 1$:

$$
\begin{aligned}
\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1,\\
\eta(x_4) = \eta(b+1) = -1, \eta(x_4+1) = \eta(b+c) = -1,\\
\eta(x_5) = -\eta(b-1) = -1 \Rightarrow \eta(b-1) = 1,\\
\eta(x_5+1) = -\eta(b+c) = 1 \Rightarrow \eta(b+c) = -1,\\
\eta(x_6) = -\eta(b+1) = 1 \Rightarrow \eta(b+1) = -1,\\
\eta(x_6+1) = -\eta(b-c) = -1 \Rightarrow \eta(b-c) = 1.
\end{aligned}
$$

We see that, for a fixed $b \neq \pm 1, \pm c$, all four solutions are a priori possible.

NB: For $b = 1$, if $\eta(2) = -1$, we get the distinct solutions $x_4 \neq 0$ and $x_6 \neq 0$. In this case, we can see that $b = 1$ gives three distinct solutions. For $b = c$, we get the distinct solutions x_4, x_5 if $\eta(2c) = -1$, and the solution x_2, giving three distinct solutions in that case.

The distribution in this case is:

- If $\eta(2) = 1$ and $\eta(2c) = 1$ (thus, $\eta(c) = 1$):

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{1,1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1-1,-1,-1} \cup \{b = 1, c\}),\\
{}_c\omega_2 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,-1,1,-1}),\\
{}_c\omega_4 &= \#S^c_{1,-1,1,-1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = 1$ and $\eta(2c) = -1$ (thus, $\eta(c) = -1$):

$$
{}_c\omega_1 = \#(S^c_{1,1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1-1,-1,-1} \cup \{b = 1\}),
$$

$$
\begin{aligned}
{}_c\omega_2 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,-1,1,-1}),\\
{}_c\omega_3 &= \#\{b = c\},\\
{}_c\omega_4 &= \#S^c_{1,-1,1,-1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = -1$ and $\eta(2c) = 1$ (thus, $\eta(c) = -1$):

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{1,1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1-1,-1,-1} \cup \{b = c\}),\\
{}_c\omega_2 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,-1,1,-1}),\\
{}_c\omega_3 &= \#\{b = 1\},\\
{}_c\omega_4 &= \#S^c_{1,-1,1,-1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = -1$ and $\eta(2c) = -1$ (thus, $\eta(c) = 1$):

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{1,1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1-1,-1,-1}),\\
{}_c\omega_2 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,-1,1,-1}),\\
{}_c\omega_3 &= \#\{b = 1, c\},\\
{}_c\omega_4 &= \#S^c_{1,-1,1,-1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

Case D. $\eta(1-c) = -1 = -\eta(1+c) (\Rightarrow c \neq \pm 1)$: In this case, all above equations change sign, which implies the same compatibilities.
Case D1. $\eta(-1) = 1$:

- If $\eta(2) = 1$ and $\eta(2c) = \eta(c) = 1$:

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{1,1,1,1}),\\
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{1,1,-1,1}),\\
{}_c\omega_3 &= \#\{b = 1, c\},\\
{}_c\omega_4 &= \#S^c_{-1,1,-1,1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = 1$ and $\eta(2c) = \eta(c) = -1$:

$$
{}_c\omega_1 = \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{1,1,1,1} \cup \{b = c\}),
$$

$$
\begin{aligned}
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{1,1,-1,1}),\\
{}_c\omega_3 &= \#\{b = 1\},\\
{}_c\omega_4 &= \#S^c_{-1,1,-1,1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = -1$ and $\eta(2c) = -\eta(c) = 1$:

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{1,1,1,1} \cup \{b = 1\}),\\
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{1,1,-1,1}),\\
{}_c\omega_3 &= \#\{b = c\},\\
{}_c\omega_4 &= \#S^c_{-1,1,-1,1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_4).
\end{aligned}
$$

- If $\eta(2) = -1$ and $\eta(2c) = -\eta(c) = -1$:

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{1,1,1,1} \cup \{b = 1, c\}),\\
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{1,1,-1,1}),\\
{}_c\omega_4 &= \#S^c_{-1,1,-1,1},\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
\end{aligned}
$$

For fixed $i, j, u, v \in \{\pm 1\}$, we will now compute the cardinalities of the cyclotomic sets $S^c_{i,j,u,v}$, which, we recall are defined by

$$S^c_{i,j,u,v} = \{b \neq \pm 1, \pm c : (\eta(b-1), \eta(b+1), \eta(b-c), \eta(b+c)) = (i, j, u, v)\}.$$

For fixed (i, j, u, v), we have

$$
\begin{aligned}
&\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1))(1 + u\eta(b-c))(1 + v\eta(b+c))\\
=&16|S^c_{i,j,u,v}| + (1 + j\eta(2))(1 + u\eta(1-c))(1 + v\eta(1+c))\\
&+ (1 + i\eta(-2))(1 + u\eta(-1-c))(1 + v\eta(-1+c))\\
&+ (1 + i\eta(c-1))(1 + j\eta(c+1))(1 + v\eta(2c))\\
&+ (1 + i\eta(-c-1))(1 + j\eta(-c+1))(1 + u\eta(-2c)).
\end{aligned}
$$

On the other hand,

$$\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1))(1 + u\eta(b-c))(1 + v\eta(b+c))$$

$$
\begin{aligned}
=&\sum_{b\in\mathbb{F}_{p^n}} 1+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)+\sum_{b\in\mathbb{F}_{p^n}} j\eta(b+1)+\sum_{b\in\mathbb{F}_{p^n}} u\eta(b-c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} v\eta(b+c)+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)j\eta(b+1)+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)u\eta(b-c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)v\eta(b+c)+\sum_{b\in\mathbb{F}_{p^n}} j\eta(b+1)u\eta(b-c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} j\eta(b+1)v\eta(b+c)+\sum_{b\in\mathbb{F}_{p^n}} u\eta(b-c)v\eta(b+c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)j\eta(b+1)u\eta(b-c)+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)j\eta(b+1)v\eta(b+c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)u\eta(b-c)v\eta(b+c)+\sum_{b\in\mathbb{F}_{p^n}} j\eta(b+1)u\eta(b-c)v\eta(b+c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} i\eta(b-1)j\eta(b+1)u\eta(b-c)v\eta(b+c)\\
=&p^n+\sum_{b\in\mathbb{F}_{p^n}} ij\eta(b^2-1)+\sum_{b\in\mathbb{F}_{p^n}} iu\eta(b^2-(1+c)b+c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} iv\eta(b^2+(-1+c)b-c)+\sum_{b\in\mathbb{F}_{p^n}} ju\eta(b^2+(1-c)b-c)\\
&+\sum_{b\in\mathbb{F}_{p^n}} jv\eta(b^2+(1+c)b+c)+\sum_{b\in\mathbb{F}_{p^n}} uv\eta(b^2-c^2)\\
&+\sum_{b\in\mathbb{F}_{p^n}} iju\eta((b^2-1)(b-c))+\sum_{b\in\mathbb{F}_{p^n}} ijv\eta((b^2-1)(b+c))\\
&+\sum_{b\in\mathbb{F}_{p^n}} iuv\eta((b-1)(b^2-c^2)+\sum_{b\in\mathbb{F}_{p^n}} juv\eta((b+1)(b^2-c^2))\\
&+\sum_{b\in\mathbb{F}_{p^n}} ijuv\eta((b^2-1)(b^2-c^2)).
\end{aligned}
$$

The cubics and the quartics will be more complicated to deal with. As for the quadratics (taking into account that $c \neq \pm 1, 0$), and using Equation (3), which gives the Jacobsthal sum in terms of the discriminant d of the polynomial f, we obtain

$$
\begin{aligned}
&f(b) = b^2-1, d = 4 \neq 0,\\
&\qquad \text{thus, } \sum_{b\in\mathbb{F}_{p^n}} ij\eta(b^2-1) = -ij\eta(1) = -ij,
\end{aligned}
$$

$$f(b) = b^2 - (1+c)b + c, d = (1+c)^2 - 4c = c^2 - 2c + 1 = (c-1)^2 \neq 0$$
$$\text{thus, } \sum_{b \in \mathbb{F}_{p^n}} iu\eta(b^2 - (1+c)b + c) = -iu\eta(1) = -iu,$$
$$f(b) = b^2 + (-1+c)b - c, d = (-1+c)^2 + 4c = c^2 + 2c + 1 = (c+1)^2 \neq 0,$$
$$\text{thus, } \sum_{b \in \mathbb{F}_{p^n}} iv\eta(b^2 + (-1+c)b - c) = -iv\eta(1) = -iv,$$
$$f(b) = b^2 + (1-c)b - c, d = (1-c)^2 + 4c = c^2 + 2c + 1 = (c+1)^2 \neq 0,$$
$$\text{thus, } \sum_{b \in \mathbb{F}_{p^n}} ju\eta(b^2 + (1-c)b - c) = -ju\eta(1) = -ju,$$
$$f(b) = b^2 + (1+c)b + c, d = (1+c)^2 - 4c = c^2 - 2c + 1 = (c-1)^2 \neq 0,$$
$$\text{thus, } \sum_{b \in \mathbb{F}_{p^n}} jv\eta(b^2 + (1+c)b + c) = -jv\eta(1) = -jv,$$
$$f(b) = b^2 - c^2, d = 4c^2 \neq 0,$$
$$\text{thus, } \sum_{b \in \mathbb{F}_{p^n}} uv\eta(b^2 - c^2) = -uv\eta(1) = -uv.$$

Summarizing, we obtain,

$$\begin{aligned}
&\sum_{b \in \mathbb{F}_{p^n}} (1 + i\eta(b-1))(1 + j\eta(b+1))(1 + u\eta(b-c))(1 + v\eta(b+c)) \\
=&p^n - (ij + iu + iv + ju + jv + uv) \\
&+ ij \left(u \sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b-c)) + v \sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b+c)) \right) \\
&+ uv \left(i \sum_{b \in \mathbb{F}_{p^n}} \eta((b-1)(b^2-c^2) + j \sum_{b \in \mathbb{F}_{p^n}} \eta((b+1)(b^2-c^2)) \right) \\
&+ ijuv \sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b^2-c^2)).
\end{aligned}$$

We can further simplify the sums. If $\eta(-1) = \epsilon \in \{-1, 1\}$, then (changing b to $-b$), we get

$$\sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b-c)) = \epsilon \sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b+c))$$
$$\sum_{b \in \mathbb{F}_{p^n}} \eta((b-1)(b^2-c^2) = \epsilon \sum_{b \in \mathbb{F}_{p^n}} \eta((b+1)(b^2-c^2)).$$

Therefore, if $i = -\eta(-1)j$ and/or $u = -\eta(-1)v$, there are several simplifications. We denote by $A = \sum_{b\in\mathbb{F}_{p^n}} \eta((b^2-1)(b-c))$, $B = \sum_{b\in\mathbb{F}_{p^n}} \eta((b-1)(b^2-c^2)$ and $C = \sum_{b\in\mathbb{F}_{p^n}} \eta((b^2-1)(b^2-c^2))$.

If $\eta(-1) = 1$, we note that, since the map $b \mapsto -b$ also maps $\eta(b-1) \mapsto \eta(b+1)$ and $\eta(b-c) \mapsto \eta(b+c)$, then $\#S^c_{1,-1,1,1} = \#S^c_{-1,1,1,1}$, $\#S^c_{1,-1,1,-1} = \#S^c_{-1,1,-1,-1}$, $\#S^c_{1,1,1,-1} = \#S^c_{1,1,-1,1}$ and $\#S^c_{1,-1,-1,1} = \#S^c_{-1,1,1,-1}$. The cardinality of these cyclotomic sets is given here in lexicographic order:

$$\begin{aligned}
\#S^c_{1,1,1,1} &= \frac{1}{16}\,(p^n - 6 + 2A + 2B + C \\
&\qquad -2(2+\eta(2)+\eta(2c))(1+\eta(1-c))(1+\eta(1+c)))\,, \\
\#S^c_{1,1,1,-1} = \#S^c_{1,1,-1,1} &= \frac{1}{16}\,\big(p^n - 2B - C - 2(1+\eta(2))(1-\eta(1-c^2)) \\
&\qquad -2(1+\eta(1-c))(1+\eta(1+c)))\,, \\
\#S^c_{1,1,-1,-1} &= \frac{1}{16}(p^n + 2 - 2A + 2B + C \\
&\qquad -2(1+\eta(2))(1-\eta(1-c))(1-\eta(1+c)) \\
&\qquad -2(1+\eta(1-c))(1+\eta(1+c))(1-\eta(2c))), \\
\#S^c_{1,-1,1,1} &= \frac{1}{16}(p^n - 2A - C - 2(1+\eta(1-c))(1+\eta(1+c)) \\
&\qquad -2(1+\eta(2c))(1-\eta(1-c^2))), \\
\#S^c_{1,-1,1,-1} &= \frac{1}{16}(p^n + 2 + C \\
&\qquad -(2-\eta(2)-\eta(2c))(1+\eta(1-c))(1-\eta(1+c)) \\
&\qquad -(2+\eta(2)+\eta(2c))(1-\eta(1-c))(1+\eta(1+c))), \\
\#S^c_{1,-1,-1,1} &= \frac{1}{16}(p^n + 2 + C \\
&\qquad -(2-\eta(2)-\eta(2c))(1-\eta(1-c))(1+\eta(1+c)) \\
&\qquad -(2+\eta(2)+\eta(2c))(1+\eta(1-c))(1-\eta(1+c))), \\
\#S^c_{1,-1,-1,-1} &= \frac{1}{16}(p^n + 2A - C - 2(1-\eta(1-c))(1-\eta(1+c)) \\
&\qquad -2(1-\eta(2c))(1-\eta(1-c^2))), \\
\#S^c_{-1,1,1,1} &= \frac{1}{16}(p^n - 2A - C - 2(1+\eta(1-c))(1+\eta(1+c)) \\
&\qquad -2(1+\eta(2c))(1-\eta(1-c^2))), \\
\#S^c_{-1,1,1,-1} &= \frac{1}{16}(p^n + 2 + C \\
&\qquad -(2+\eta(2)+\eta(2c))(1+\eta(1-c))(1-\eta(1+c))
\end{aligned}$$

$$
\begin{aligned}
&\quad - (2-\eta(2)-\eta(2c))(1-\eta(1-c))(1+\eta(1+c))),\\
\#S^c_{-1,1,-1,1} &= \frac{1}{16}(p^n+2+C\\
&\quad - (2+\eta(2)+\eta(2c))(1-\eta(1-c))(1+\eta(1+c))\\
&\quad - (2-\eta(2)-\eta(2c))(1+\eta(1-c))(1-\eta(1+c))),\\
\#S^c_{-1,1,-1,-1} &= \frac{1}{16}(p^n+2A-C-2(1-\eta(1-c))(1-\eta(1+c))\\
&\quad - 2(1-\eta(2c))(1-\eta(1-c^2))),\\
\#S^c_{-1,-1,1,1} &= \frac{1}{16}(p^n+2+2A-2B+C\\
&\quad - 2(1-\eta(2))(1+\eta(1-c))(1+\eta(1+c))\\
&\quad - 2(1-\eta(c-1))(1-\eta(c+1))(1+\eta(2c))),\\
\#S^c_{-1,-1,1,-1} = \#S^c_{-1,-1,-1,1} &= \frac{1}{16}(p^n+2B-C\\
&\quad - 2(1-\eta(2))(1-\eta(1-c^2)) - 2(1-\eta(1-c))(1-\eta(1+c))),\\
\#S^c_{-1,-1,-1,-1} &= \frac{1}{16}(p^n-6-2A-2B+C\\
&\quad - 2(2-\eta(2)-\eta(2c))(1-\eta(1-c))(1-\eta(1+c))).
\end{aligned}
$$

For Cases A1 and B1 (that is, when $\eta(-1)=1$ and $\eta(1-c^2)=1$), the spectrum is (recall that $C=\sum_{b\in\mathbb{F}_{p^n}}\eta((b^2-1)(b^2-c^2))$)

$$
\begin{aligned}
{}_c\omega_0 &= \#S^c_{1,-1,-1,1} + \#S^c_{-1,1,1,-1} = \frac{1}{8}(p^n+2+C),\\
{}_c\omega_2 &= \#S^c_{1,-1,1,-1} + \#S^c_{-1,1,-1,1} = \frac{1}{8}(p^n+2+C),\\
{}_c\omega_1 &= p^n - ({}_c\omega_0 + {}_c\omega_2) = \frac{1}{4}(3p^n-2-C).
\end{aligned}
$$

For Case C1 (that is, $\eta(-1)=1$, $\eta(1-c)=1, \eta(1+c)=-1$):

$$
\begin{aligned}
{}_c\omega_1 &= \#S^c_{1,1,1,1} + \#S^c_{1,1,-1,-1} + \#S^c_{-1,-1,1,1} + \#S^c_{-1,-1,-1,-1}\\
&\qquad + \begin{cases} 2, & \eta(2)=1, \eta(c)=1\\ 1, & \eta(c)=-1\\ 0, & \eta(2)=-1, \eta(c)=1 \end{cases}\\
&= \frac{1}{4}(p^n-2+C) + \begin{cases} 2, & \eta(2)=1, \eta(c)=1\\ 1, & \eta(c)=-1\\ 0, & \eta(2)=-1, \eta(c)=1, \end{cases}\\
{}_c\omega_2 &= \#S^c_{1,1,1,-1} + \#S^c_{1,-1,1,1} + \#S^c_{1,-1,-1,-1} + \#S^c_{-1,-1,1,-1} = \frac{1}{4}(p^n-C-4),
\end{aligned}
$$

$$
{}_c\omega_3 = \begin{cases} 1, & \eta(c) = -1 \\ 0, & \eta(c) = 1, \end{cases}
$$

$$
{}_c\omega_4 = \#S^c_{1,-1,1,-1} = \frac{1}{16}(p^n + 2 + C - 4(2 + \eta(2) + \eta(2c))),
$$

$$
{}_c\omega_0 = p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
$$

For the case D1 (that is, $\eta(-1) = 1$, $\eta(1-c) = -1, \eta(1+c) = 1$):

$$
{}_c\omega_1 = \#S^c_{1,1,1,1} + \#S^c_{1,1,-1,-1} + \#S^c_{-1,-1,1,1} + \#S^c_{-1,-1,-1,-1}
$$

$$
+ \begin{cases} 0, & \eta(2) = 1, \eta(c) = 1 \\ 1, & \eta(c) = -1 \\ 2, & \eta(2) = -1, \eta(2c) = -1, \end{cases}
$$

$$
= \frac{1}{4}(p^n - 2 + C) + \begin{cases} 0, & \eta(2) = 1, \eta(2c) = 1 \\ 1, & \eta(c) = -1 \\ 2, & \eta(2) = -1, \eta(2c) = -1, \end{cases}
$$

$$
{}_c\omega_2 = \#S^c_{-1,-1,-1,1} + \#S^c_{-1,1,-1,-1} + \#S^c_{-1,1,1,1} + \#S^c_{1,1,-1,1} = \frac{1}{4}(p^n - C - 4),
$$

$$
{}_c\omega_3 = \begin{cases} 2, & \eta(2) = 1, \eta(c) = 1 \\ 1, & \eta(c) = -1 \\ 0, & \eta(2) = -1, \eta(c) = 1, \end{cases}
$$

$$
{}_c\omega_4 = \#S^c_{-1,1,-1,1} = \frac{1}{16}(p^n + 2 + C - 4(2 - \eta(2) - \eta(2c))),
$$

$$
{}_c\omega_0 = p^n - ({}_c\omega_1 + {}_c\omega_2 + {}_c\omega_3 + {}_c\omega_4).
$$

Note that the symmetries in the sets and the spectra imply that we do not need the values of A and B.

We can furthermore transform the quartic C into the sum a quadratic and a cubic. Using the labelling $b^2 = a$, we get the sums

$$
\sum_{b \in \mathbb{F}_{p^n}} \eta((b^2-1)(b^2-c^2)) = \sum_{a \in \mathbb{F}_{p^n}} (\eta(a)+1)\eta((a-1)(a-c^2))
$$

$$
= \sum_{a \in \mathbb{F}_{p^n}} \eta(a(a-1)(a-c^2)) + \sum_{a \in \mathbb{F}_{p^n}} \eta((a-1)(a-c^2))
$$

$$
= \sum_{a \in \mathbb{F}_{p^n}} \eta(a(a-1)(a-c^2)) - 1,
$$

where we used Jacobsthal's sum (3) for the second sum.

In order to compute the sum corresponding to the above cubic, we count points on elliptic curves. We could consider several particular cases for

$c \neq 0, \pm 1$ (like $c^2 \in \mathbb{F}_p$), but we prefer simplicity (though, we make some remark after the proof of the theorem on that, as well as provide a result for $c^2 = -1$ in Theorem 2.4).

In order to find $\sum_{a \in \mathbb{F}_{p^n}} \eta(a(a-1)(a-c^2))$, we consider the elliptic curve $E(\mathbb{F}_{p^n}) : \ y^2 = x(x-1)(x-c^2)$ over the field $\mathbb{F}_{p^n}$. By the Hasse-Weil inequality [15, Corollary 4.15], we know that $|\#E(\mathbb{F}_{p^n}) - (p^n+1)| \leq 2\sqrt{p^n}$. If we denote by $a_{p^n}^{(c)} = \#E(\mathbb{F}_{p^n}) - (p^n+1)$, the Hasse-Weil inequality error, then

$$\begin{aligned} C+1 &= \sum_{a \in \mathbb{F}_{p^n}} \eta(a(a-1)(a-c^2)) \\ &= \#\{a \neq 0,1,c^2 \, : \, a(a-1)(a-c^2) \text{ is a square}\} \\ &\qquad - \#\{a \neq 0,1,c^2 \, : \, a(a-1)(a-c^2) \text{ is a non-square}\} \\ &= 2\#\{a \neq 0,1,c^2 \, : \, a(a-1)(a-c^2) \text{ is a square}\} - p^n + 3 \\ &= \#E(\mathbb{F}_{p^n}) - p^n + 3 = a_{p^n}^{(c)} + 4, \end{aligned}$$

and so, $C = a_{p^n}^{(c)} + 3$.

Substituting this in the spectra expressions given above, we get the claimed spectra and the theorem is shown. □

We can express the sum C with respect to a smaller field, namely $\mathbb{F}_q = \mathbb{F}_p(c^2)$, where $q = p^r$, for some positive integer r, in the following way. First, we recall a (particular case of a) celebrated result of Weil and generalized by Deligne (see [15, Theorem 4.12], for more details). Given an elliptic curve in the Weierstrass form $y^2 = x^3 + Ax + B$ over some finite field $\mathbb{F}_q$ (q is a prime power), if the number of rational points of the elliptic curve over the base field $\mathbb{F}_q$ is $\#E(\mathbb{F}_q) = q + 1 - a_q$, the Frobenius polynomial of the curve is $T^2 - a_q T + q = (T-\alpha)(T-\beta)$ (for some complex numbers α, β), and the number of points of the same curve over the extension field $\mathbb{F}_{q^n}$ is $\#E(\mathbb{F}_{q^n}) = (1-\alpha^n)(1-\beta^n) = 1 + q^n - (\alpha^n + \beta^n)$, for all $n \geq 1$. We thus get $a_{p^n}^{(c)} = \alpha^n + \beta^n$, where $\alpha = \frac{1}{2}\left(a_q^{(c)} + \sqrt{\left(a_q^{(c)}\right)^2 - 4q}\right)$, $\beta = \frac{1}{2}\left(a_q^{(c)} - \sqrt{\left(a_q^{(c)}\right)^2 - 4q}\right)$. Observe that when $c^2 \in \mathbb{F}_p$, then $q = p$.

We will consider the special case of $c^2 = -1$ (and so, $p \equiv 1 \pmod 4$, or, $p \equiv 3 \pmod 4$ and n even) below.

Theorem 2.4. *Let p be a prime number such that either $p \equiv 1 \pmod 4$, or $p \equiv 3 \pmod 4$ and n even. Let c be a square root of -1 in $\mathbb{F}_{p^n}$. The c-differential spectrum of $x \mapsto x^{\frac{p^n+1}{2}}$ on $\mathbb{F}_{p^n}$ is given by the following:*

(*i*) *If n is even and either $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$ (that is, $p \equiv 3 \pmod 4$ and n even), then*

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}\left(p^n + 2(-p)^{\frac{n}{2}} + 5\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(3p^n - 2(-p)^{\frac{n}{2}} - 5\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(p^n + 2(-p)^{\frac{n}{2}} + 5\right).
\end{aligned}
$$

Note that this implies that the map is APcN.

(*ii*) *Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$, a, b integers, b even, and $a + b \equiv 1 \pmod 4$.*

(1) *If $p \equiv 1 \pmod 8$, or, $p \equiv 5 \pmod 8$ and n even, then*

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}\left(p^n + (a+bc)^n + (a-bc)^n + 5\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(3p^n - (a+bc)^n - (a-bc)^n - 5\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(p^n + (a+bc)^n + (a-bc)^n + 5\right).
\end{aligned}
$$

Note that this implies that the map is APcN.

(2) *If $p \equiv 5 \pmod 8$ and n odd, then*

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{16}\left(7p^n - (a+bc)^n - (a-bc)^n - 5\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(p^n + (a+bc)^n + (a-bc)^n + 5\right), \\
{}_c\omega_2 &= \frac{1}{4}\left(p^n - (a+bc)^n - (a-bc)^n - 7\right), \\
{}_c\omega_3 &= 1, \\
{}_c\omega_4 &= \frac{1}{16}\left(p^n + (a+bc)^n + (a-bc)^n - 3\right).
\end{aligned}
$$

Proof. We use Theorem 2.3 and observe that the curve corresponding to the sum C is now $y^2 = x^3 - x$ over $\mathbb{F}_p$. We will need a result [15, Theorem 4.23]

dealing with the number of points of the well-known (since Gauss' time) elliptic curve $y^2 = x^3 - kx$ over $\mathbb{F}_p$, $k \not\equiv 0 \pmod{p}$. If $p \equiv 3 \pmod 4$, then $a_p = 0$; if $p \equiv 1 \pmod 4$, writing $p = a^2 + b^2$, a, b integers, b even and $a + b \equiv 1 \pmod 4$, then

$$a_p = \begin{cases} 2a & \text{if } k \text{ is a 4th power mod } p \\ -2a & \text{if } k \text{ is a square but not a 4th power mod } p \\ \pm 2b & \text{if } k \text{ is not a 4th power mod } p. \end{cases}$$

In our case $k = 1$, and the first case above applies when $p \equiv 1 \pmod 4$. We will go through several cases, depending on the residue of $p \pmod 8$, since we know that 2 is a quadratic residue if and only if $p \equiv \pm 1 \pmod 8$, or n is even. We will use below the observation that when $c^2 = -1$, then $1 + c = -c^2 + c = c(1 - c)$ and so, $\eta(1 + c) = \eta(c)\eta(1 - c)$, and so, $\eta(1 + c), \eta(1 - c)$ have opposite signs if and only if $\eta(c) = -1$. For simplicity, we write in the proof below a_p, a_{p^n}, in lieu of $a_p^{(c)}, a_{p^n}^{(c)}$, and they will all be attached curve $y^2 = x^3 - x$ over $\mathbb{F}_p$, respectively, $\mathbb{F}_{p^n}$.

Case 1. Let n be even and $p \equiv 3 \pmod 8$ or $p \equiv 7 \pmod 8$. Since $a_p = 0$ in this case, then the Frobenius polynomial of the curve $y^2 = x^3 - x$ becomes $T^2 + p = (T - \sqrt{-p})(T + \sqrt{-p})$, which renders $a_{p^n} = 2(-p)^{\frac{n}{2}}$. We now apply Theorem 2.3 (i), obtaining claim (i) of our theorem.

Case 2. Let $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$ and n even. Let $p = a^2 + b^2$, where b is even. In this case, the Frobenius polynomials for $y^2 = x^3 - x$ is $T^2 - 2aT + p = (T - \alpha)(T - \beta)$, where $\alpha = a + bc, \beta = a - bc$ (recall that c is a root of -1). Therefore, $a_{p^n} = (a + bc)^n + (a - bc)^n$. We thus get claim $(ii)\,(1)$, using Theorem 2.3 (i).

Case 3. Let $p \equiv 5 \pmod 8$ and n odd, $p = a^2 + b^2$, b even. As above, $a_{p^n} = (a + bc)^n + (a - bc)^n$. We know that 2 is not a square residue. We therefore get $(ii)\,(2)$, via Theorem 2.3 (ii/iii) (note that both cases give the same spectrum in this case, due to $\eta(c) = -1$).

The theorem is shown. □

We continue with the case of $c \neq 0, \pm 1$, $\eta(-1) = -1$ (that is, $p \equiv 3 \pmod 4$ and n odd).

Theorem 2.5. *Let $F(x) = x^d$, where $d = \frac{p^n+1}{2}$ (p odd prime, $n \geq 1$). If $c \neq 0, \pm 1$ and $\eta(-1) = -1$, then,*

(i) If $\eta(-1) = -1$ and $\eta(1 - c^2) = 1$:

$$_c\omega_0 = \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} - 3\right),$$

$$
\begin{aligned}
{}_c\omega_1 &= \frac{1}{4}\left(p^n - a_{p^n}^{(c)} + 1\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} + 1\right).
\end{aligned}
$$

(ii) If $\eta(-1) = -1$ *and* $\eta(1-c) = 1, \eta(1+c) = -1$:

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} - 21\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(p^n - a_{p^n}^{(c)} + 1\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} + 19\right).
\end{aligned}
$$

(iii) If $\eta(-1) = -1$ *and* $\eta(1-c) = -1, \eta(1+c) = 1$:

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} + 3 + 4\eta(2)\right), \\
{}_c\omega_1 &= \frac{1}{4}\left(p^n - a_{p^n}^{(c)} + 1\right), \\
{}_c\omega_2 &= \frac{1}{8}\left(3p^n + a_{p^n}^{(c)} - 5 - 4\eta(2)\right).
\end{aligned}
$$

Proof. We consider several cases.
Case (i)**.** Let $\eta(-1) = -1$, $\eta(1-c) = 1, \eta(1+c) = 1$. Then:

$$
\begin{aligned}
&\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1, \\
&\eta(x_4) = -\eta(b+1) = 1, \eta(x_4+1) = -\eta(b+c) = -1, \\
&\eta(x_5) = \eta(b-1) = -1, \eta(x_5+1) = \eta(b+c) = 1, \\
&\eta(x_6) = -\eta(b+1) = 1, \eta(x_6+1) = -\eta(b-c) = -1.
\end{aligned}
$$

We see that, for a fixed b, if x_3 exists, then x_5 cannot exist, and vice-versa. Also, if x_4 exists, then x_6 cannot exist, and vice-versa. We can at most have x_3 and x_4, or x_3 and x_6, or x_4 and x_5, or x_5 and x_6.

NB: For $b = 1$, if $\eta(2) = 1$ (that is, $p \equiv \pm 1 \pmod 8$, or, $p \equiv \pm 3 \pmod 8$ and n even), we get a solution $x_4 \neq 0$. If $\eta(2) = -1$ (that is, $p \equiv \pm 3 \pmod 8$ and n odd), we get a solution $x_6 \neq 0$. Regardless, we can see that $b = 1$ gives two distinct solutions. For $b = c$, if $\eta(2c) = 1$, we get two distinct solutions, x_4, x_5.

The distribution in this case is:

- If $\eta(2c) = 1$,

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,1,-1,1} \cup S^c_{-1,-1,1,-1} \cup S^c_{-1,-1,-1,1} \cup \{b = -c\}),\\
{}_c\omega_2 &= \#(S^c_{1,1,1,1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,1,-1} \cup S^c_{-1,1,1,1}\\
&\qquad\qquad \cup S^c_{-1,1,-1,1} \cup S^c_{-1,-1,1,1} \cup \{b = 1, c\}),\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2).
\end{aligned}
$$

- If $\eta(2c) = -1$,

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{1,1,1,-1} \cup S^c_{1,1,-1,1} \cup S^c_{-1,-1,1,-1} \cup S^c_{-1,-1,-1,1} \cup \{b = -c\}),\\
{}_c\omega_2 &= \#(S^c_{1,1,1,1} \cup S^c_{1,-1,1,1} \cup S^c_{1,-1,1,-1} \cup S^c_{-1,1,1,1}\\
&\qquad\qquad \cup S^c_{-1,1,-1,1} \cup S^c_{-1,-1,1,1} \cup \{b = 1\}),\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2).
\end{aligned}
$$

Using similar techniques as in the case $\eta(-1) = 1$, we see that the spectrum for Case (i) is

$$
\begin{aligned}
{}_c\omega_1 &= \frac{1}{4}(p^n - C) + 1 = \frac{1}{4}(p^n - C + 4),\\
{}_c\omega_2 &= \frac{1}{8}(3p^n + C - 2),\\
{}_c\omega_0 &= \frac{1}{8}(3p^n + C - 6).
\end{aligned}
$$

NB: The cases $\eta(2c) = 1$ and $\eta(2c) = -1$ yield the same result.
Case (ii)**.** Let $\eta(-1) = -1$, $\eta(1 - c) = -1, \eta(1 + c) = -1$. Then:

- If $\eta(2c) = 1$:

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,-1,1,-1} \cup S^c_{1,1,-1,1} \cup S^c_{1,1,1,-1} \cup \{b = -c\}),\\
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,-1,1} \cup S^c_{1,-1,-1,-1}\\
&\qquad\qquad \cup S^c_{1,-1,1,-1} \cup S^c_{1,1,-1,-1} \cup \{b = 1\}),\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2).
\end{aligned}
$$

- If $\eta(2c) = -1$:

$$
\begin{aligned}
{}_c\omega_1 &= \#(S^c_{-1,-1,-1,1} \cup S^c_{-1,-1,1,-1} \cup S^c_{1,1,-1,1} \cup S^c_{1,1,1,-1} \cup \{b = -c\}),\\
{}_c\omega_2 &= \#(S^c_{-1,-1,-1,-1} \cup S^c_{-1,1,-1,-1} \cup S^c_{-1,1,-1,1} \cup S^c_{1,-1,-1,-1}\\
&\qquad\qquad \cup S^c_{1,-1,1,-1} \cup S^c_{1,1,-1,-1} \cup \{b = 1, c\}),\\
{}_c\omega_0 &= p^n - ({}_c\omega_1 + {}_c\omega_2).
\end{aligned}
$$

In this case, then, we obtain the same spectrum as for Case (i), that is

$$
\begin{aligned}
{}_c\omega_1 &= \frac{1}{4}(p^n - C + 4),\\
{}_c\omega_2 &= \frac{1}{8}(3p^n + C - 2),\\
{}_c\omega_0 &= \frac{1}{8}(3p^n + C - 6).
\end{aligned}
$$

Case (iii)**.** Let $\eta(-1) = -1$, $\eta(1-c) = 1, \eta(1+c) = -1$. Then:

$$
\begin{aligned}
&\eta(x_3) = \eta(b-1) = 1, \eta(x_3+1) = \eta(b-c) = 1,\\
&\eta(x_4) = -\eta(b+1) = -1, \eta(x_4+1) = -\eta(b+c) = -1,\\
&\eta(x_5) = -\eta(b-1) = -1, \eta(x_5+1) = -\eta(b+c) = 1,\\
&\eta(x_6) = \eta(b+1) = 1, \eta(x_6+1) = \eta(b-c) = -1.
\end{aligned}
$$

We see that, for a fixed b, if x_3 exists, then x_6 cannot exist, and vice-versa. Also, if x_4 exists, then x_5 cannot exist, and vice-versa. We can at most have x_3 and x_4, or x_3 and x_5, or x_4 and x_6, or x_5 and x_6.

NB: For $b = -1$, we can see that, if $\eta(2) = -1$, we get the distinct solutions x_3 and x_5. In this case, we can see that $b = -1$ gives two distinct solutions. For $b = -c$, if $\eta(2c) = 1$, we get the solution $x_6 \neq -1$. If $\eta(2c) = -1$, we get the solution $x_3 \neq -1$. We can see that $b = -c$ always gives two distinct solutions.

The distribution in this case is:

- If $\eta(2) = 1$:

$$
\begin{aligned}
{}_c\omega_0 &= \#(S^c_{1,-1,-1,1} \cup S^c_{-1,1,1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1,-1,1,-1}\\
&\qquad \cup S^c_{-1,-1,-1,1} \cup S^c_{-1,-1,-1,-1} \cup \{b = -1, c\}),\\
{}_c\omega_1 &= \#(S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{-1,1,-1,-1} \cup \{b = 1\}),\\
{}_c\omega_2 &= p^n - ({}_c\omega_0 + {}_c\omega_2).
\end{aligned}
$$

- If $\eta(2) = -1$:

$$
\begin{aligned}
{}_c\omega_0 &= \#(S^c_{1,-1,-1,1} \cup S^c_{-1,1,1,-1} \cup S^c_{-1,-1,1,1} \cup S^c_{-1,-1,1,-1}\\
&\qquad \cup S^c_{-1,-1,-1,1} \cup S^c_{-1,-1,-1,-1} \cup \{b = c\}),\\
{}_c\omega_1 &= \#(S^c_{1,-1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{-1,1,-1,-1} \cup \{b = 1\}),\\
{}_c\omega_2 &= p^n - ({}_c\omega_0 + {}_c\omega_2).
\end{aligned}
$$

Here the spectrum is therefore

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}(3p^n - 40 + C) + 2 = \frac{1}{8}(3p^n + C - 24),\\
{}_c\omega_1 &= \frac{1}{4}(p^n - C) + 1 = \frac{1}{4}(p^n - C + 4),\\
{}_c\omega_2 &= \frac{1}{8}(5p^n + 40 + C) - 3 = \frac{1}{8}(3p^n + C + 16).
\end{aligned}
$$

Case D2. Let $\eta(-1) = -1$, $\eta(1-c) = -1, \eta(1+c) = 1$. Then:

$$
\begin{aligned}
{}_c\omega_0 &= \#(S^c_{-1,1,1,-1} \cup S^c_{1,-1,-1,1} \cup S^c_{1,1,-1,-1} \cup S^c_{1,1,-1,1}\\
&\qquad\qquad \cup S^c_{1,1,1,-1} \cup S^c_{1,1,1,1} \cup \{b = -1, c\})\\
{}_c\omega_1 &= \#(S^c_{-1,1,-1,-1} \cup S^c_{-1,1,1,1} \cup S^c_{1,-1,-1,-1} \cup S^c_{1,-1,1,1} \cup \{b = 1\}),\\
{}_c\omega_2 &= p^n - ({}_c\omega_0 + {}_c\omega_2).
\end{aligned}
$$

Here the spectrum is

$$
\begin{aligned}
{}_c\omega_0 &= \frac{1}{8}(3p^n + C - 16 + 8\eta(2)) + 2 = \frac{1}{8}(3p^n + C + 4\eta(2)),\\
{}_c\omega_1 &= \frac{1}{4}(p^n - C) + 1 = \frac{1}{4}(p^n - C + 4),\\
{}_c\omega_2 &= \frac{1}{8}(5p^n + C + 16 - 8\eta(2)) - 3 = \frac{1}{8}(3p^n + C - 8 - 4\eta(2)).
\end{aligned}
$$

Setting the value of $C = a^{(c)}_{p^n} + 3$ as before, we obtain the claimed results. □

3 Conclusions

In this paper we concentrate on the map $x \mapsto x^{\frac{p^n+1}{2}}$ on a finite field $\mathbb{F}_{p^n}$, p being an odd prime and n a positive integer, and compute the complete c-differential spectrum, by using Weil sums and elliptic curve methods. Perhaps the methods we used can be applied to finding the spectrum of other interesting maps, with potential low differential or c-differential uniformity.

Acknowledgements. The authors extend their appreciation to the anonymous reviewer for their comments and to the editor for the prompt handling of the paper. The authors would also like to thank Professors Tor Helleseth and Daniel Katz for interesting discussions and for comments on a previous draft. H. Yan's research was supported by the National Natural Science Foundation of China (Grants No. 12471494).

Declarations

Conflict of interest The authors declare that they have no conflict of interest regarding the publication of this paper.

References

[1] N. Anbar, T. Kalayci, W. Meidl, C. Riera, P. Stănică, *$P_{\wp}N$ functions, complete mappings and quasigroup difference sets*, J. Combin. Designs 31:12, 667–690, 2023.

[2] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebraic Combin. 52 (2020), 187–213.

[3] B. C. Berndt, R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), 349–398.

[4] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer-Verlag, 2014.

[5] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021.

[6] S.-T. Choi, S. Hong, J.S. No, H. Chung, *Differential spectrum of some power functions in odd prime characteristic*, Finite Fields Appl. 21 (2013), 11–29.

[7] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications* (Ed. 2), Academic Press, San Diego, CA, 2017.

[8] P. Ellingsen, P. Felke, C. Riera P. Stănică, A. Tkachenko, *C-differentias, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.

[9] S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.

[10] R. Lidl, H. Niederreiter, *Finite Fields (Ed. 2)*, Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge, 1997.

[11] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.

[12] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou, *Investigation on c-(almost) perfect nonlinear functions*, IEEE Trans. Inform. Theory 67:10 (2021), 6916–6925.

[13] M. Pal, P. Stănică, *A connection between the boomerang uniformity and the extended differential in odd characteristic and applications*, Adv. Math. Communications, 2025, `https://doi.org/10.3934/amc.2024059`.

[14] N. Tokareva, *Bent Functions, Results and Applications to Cryptography*, Academic Press, San Diego, CA, 2015.

[15] L. Washington, *Elliptic Curves, Number Theory and Cryptography* (2nd ed.), 2008.

[16] H. Yan, S. Mesnager, X. Tan, *On a class of APN power functions over odd characteristic finite fields: their differential spectrum and c-differential properties*, Discrete Math. 374:4 (2024), 113881.

[17] H. Yan, K. Zhang, *On the c-differential spectrum of power functions over finite fields*, Des. Codes Cryptogr. 90 (2022), 2385–2405.

[18] X. Wang, D. Zheng, L. Hu, *Several classes of PcN power functions over finite fields*, Discrete Appl. Math. 322 (2022), 171–182.

[19] Z. Zha, L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Des. Codes Cryptogr. 89 (2021), 1193–1210.

Appendix A

We here list a few monomial functions with c-differential uniformity 1 or 2.

p	d	Condition	${}_c\Delta_F$	Refs.
any	2	$c \neq 1$	2	[8]
any	$p^m - 2$	$c = 0$	1	[8]
2	$2^m - 2$	$c \neq 0,\ \mathrm{Tr}_1^m(c) = \mathrm{Tr}_1^m(c^{-1}) = 1$	2	[8]
odd	$p^m - 2$	$c = 4,\ 4^{-1}$ or $\eta(c^2 - 4c) = \eta(1 - 4c) = -1$	2	[8]
3	$\frac{3^k+1}{2}$	$c = -1,\ \frac{m}{\gcd(k,m)} = 1$	1	[8]
odd	$\frac{p^2+1}{2}$	$c = -1,\ m$ odd	1	[2]
odd	$p^2 - p + 1$	$c = -1,\ m = 3$	1	[2]
odd	$p^4 + (p-2)p^2$ $+(p-1)p + 1$	$c = -1,\ m = 5$	1	[9]
odd	$\frac{p^5+1}{p+1}$	$c = -1,\ m = 5$	1	[9]
odd	$(p-1)p^6 + p^5 + (p-2)p^3$ $+(p-1)p^2 + p$	$c = -1,\ m = 7$	1	[9]
odd	$(p-2)p^6 + (p-2)p^5$ $+(p-1)p^4 + p^3 + p^2 + p$	$c = -1,\ m = 7$	1	[9]
odd	$\frac{p^7+1}{p+1}$	$c = -1,\ m = 7$	1	[9]
3	$\frac{3^m+3}{2}$	$c = -1,\ m$ even	2	[12]
3	$3^m - 3$	$c = 0$	2	[12]
odd	$\frac{p^m+1}{2}$	$c \neq \pm 1,\ \eta\left(\frac{1+c}{1-c}\right) = 1$ $p^m \equiv 1 \pmod 4$	≤ 2	[12]
odd	$p^k + 1$	$v_2(m) \leq v_2(k),\ 1 \neq c \in \mathbb{F}_{p^{\gcd(m,k)}}$	2	[12]
2	$2^k + 1$	$\frac{m}{\gcd(m,k)} \geq 3,\ m \geq 3,\ 1 \neq c \in \mathbb{F}_{2^{\gcd(m,k)}}$	1	[12]
3	$\frac{3^k+1}{2},\ d \equiv \frac{3^m+1}{2} \pmod{3^m - 1}$	$k,\ m$ odd, $\gcd(m,k) = 1$	1	[19]
5	$\frac{5^k+1}{2},\ d \equiv \frac{5^m+1}{2} \pmod{5^m - 1}$	$k,\ m$ positive integers, $\gcd(2m,k) = 1$	1	[19]
odd	$(p^k + 1)d \equiv 2 \pmod{p^m - 1}$ d odd	$p^m \equiv 3 \pmod 4,\ c = -1$	1	[18]
odd	$\frac{p^k+1}{2}d \equiv \frac{p^m+1}{2} \pmod{p^m - 1}$	$v_2(m) = v_2(k), p^m \equiv 1 \pmod 4, c = -1$	1	[18]
odd	$\frac{p^m-3}{2}$	$7 < 27 \neq p^m \equiv 3 \pmod 4$	2, 3	[16]

Table 1: PcN and APcN power functions $F(x) = x^d$ over $\mathbb{F}_{p^m}$ with $c \neq 1$.