ON THE INEQUIVALENCE OF NESS-HELLESETH APN FUNCTIONS

XIANGYONG ZENG, LEI HU, YANG YANG, AND WENFENG JIANG

Abstract. In this paper, the Ness-Helleseth functions over F_{p^n} defined by the form $f(x) = ux^{\frac{p^n-1}{2}-1} + x^{p^n-2}$ are proven to be a new class of almost perfect nonlinear (APN) functions and they are CCZ-inequivalent with all other known APN functions when $p \geq 7$. The original method of Ness and Helleseth showing the functions are APN for $p = 3$ and odd $n \geq 3$ is also suitable for showing their APN property for any prime $p \geq 7$ with $p \equiv 3 \,(\mathrm{mod}\, 4)$ and odd n.

1. Introduction

To efficiently resist against differential attacks [2, 12, 15, 19], cryptographical functions used in block ciphers should have low differential uniformity. Let $f(x)$ be a function from a finite field F_{p^n} to itself, and it achieves an optimum resistance to the differential cryptanalysis if $\Delta_f = 1$ or $\Delta_f = 2$, where

$$\Delta_f = \max_{a,\, b \in F_{p^n}} \{\text{the number of solutions of } f(x+a) - f(x) = b \,|\, a \neq 0\}.$$

In the former case $f(x)$ is called perfect nonlinear (PN) [3, 5, 6, 11] and in the latter $f(x)$ is almost perfect nonlinear (APN) [1, 7, 8, 9, 10, 14, 18].

There are a few classes of PN and APN functions are found, and they are mostly power functions. Table 1 lists all known APN power functions. There is no non-power APN function found for the odd p case.

Recently, Ness and Helleseth introduced a family of ternary binomial functions [18]. They are the functions

$$f(x) = ux^{\frac{p^n-1}{2}-1} + x^{p^n-2} \tag{1}$$

defined over $F_{p^n} = F_{3^n}$ ($n \geq 3$ is odd), where the element $u \in F_{p^n}$ satisfies $\chi(u+1) = \chi(u-1) = \chi(u)$ and χ is the quadratic multiplicative character of F_{p^n}.

In fact, the original method of Ness and Helleseth in [18] showing the functions are APN for $p = 3$ is also suitable for showing they are APN for any prime $p \geq 7$ with $p \equiv 3 \,(\mathrm{mod}\, 4)$ and odd n. That is, assume p is a prime with $p \equiv 3 \,(\mathrm{mod}\, 4)$, n is odd, $p^n \geq 7$, and assume $u \in F_{p^n}$ satisfies

$$\chi(u+1) = \chi(u-1) = -\chi(5u+3), \text{ or } \chi(u+1) = \chi(u-1) = -\chi(5u-3), \tag{2}$$

then the Ness-Helleseth functions defined by Equality (1) are APN.

The purpose of the present paper is to prove that the Ness-Helleseth functions are a new class of APN functions, and they are inequivalent with all other known APN functions for $p \geq 7$ under the sense of a strong inequivalence – CCZ inequivalence.

Two functions f_1 and f_2 are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if the graphs of f_1 and f_2, namely the subsets $\{(x, f_1(x)) \,|\, x \in F_{p^n}\}$ and $\{(x, f_2(x)) \,|\, x \in F_{p^n}\}$ of

Key words and phrases. Almost perfect nonlinear (APN) function, Ness-Helleseth function, CCZ-equivalence.

X. Zeng and Y. Yang are with the Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China (e-mail: xzeng@hubu.edu.cn).

L. Hu and W. Jiang are with the State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing, 100049, China (e-mail: {hu,wfjiang}@is.ac.cn).

$F_{p^n} \times F_{p^n}$, are affine equivalent. In other words, f_1 and f_2 are CCZ-equivalent if and only if there exists an affine automorphism $L = (L_1, L_2)$ of $F_{p^n} \times F_{p^n}$ such that

$$y = f_1(x) \Longleftrightarrow L_2(x, y) = f_2(L_1(x, y)).$$

Note that in this case the function $L_1(x, f_1(x))$ has to be a permutation. CCZ-equivalence keeps APN property of functions [4], and it is an extensive equivalence in the sense that other equivalences such as affine-equivalence and EA-equivalence (extended affine equivalence) are special CCZ-equivalences.

Table 1. Known APN power functions $f(x) = x^d$ over F_{p^n}

Functions	Exponents d	Conditions	References
Kloosterman	$p^n - 2$	$p = 2$ and n is odd, or $p > 2$ and $p \equiv 2 \pmod 3$	[1] [19] [15]
Gold	$2^i + 1$	$p = 2$, gcd $(i, n) = 1$	[13]
Kasami	$2^{2i} - 2^i + 1$	$p = 2$, gcd $(i, n) = 1$	[16] [17]
Welch	$2^t + 3$	$p = 2$, $n = 2t + 1$	[7]
Niho	$2^t + 2^{t/2} - 1$ for even t $2^t + 2^{\frac{3t+1}{2}-1}$ for odd t	$p = 2$, $n = 2t + 1$	[9]
Inverse	$2^{2t} - 1$	$p = 2$, $n = 2t + 1$	[1] [19]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$p = 2$, $n = 5i$	[8]
Helleseth Sandberg	$\frac{p^n-1}{2} - 1$	$p \equiv 3, 7 \pmod{20}$, $p^n > 7$, $p^n \neq 27$ and n is odd	[15]
Dobbertin et. al. Felke	$\frac{3^{(n+1)/2}-1}{2}$ $\frac{3^{(n+1)/2}-1}{2} + \frac{3^n-1}{2}$	$p = 3$, $n \equiv 3 \pmod 4$ $p = 3$, $n \equiv 1 \pmod 4$	[10] [12]
Dobbertin et. al.	$\frac{3^{n+1}-1}{8}$ $\frac{3^{n+1}-1}{8} + \frac{3^n-1}{2}$	$p = 3$, $n \equiv 3 \pmod 4$ $p = 3$, $n \equiv 1 \pmod 4$	[10]
Helleseth Rong Sandberg	$\frac{p^n+1}{4} + \frac{p^n-1}{2}$ $\frac{p^n+1}{4}$ $\frac{2p^n-1}{3}$ $p^n - 3$	$p^n \equiv 3 \pmod 8$ $p^n \equiv 7 \pmod 8$ $p^n \equiv 2 \pmod 3$ $p = 3$, $n > 1$, n is odd	[14]
Trival	3	$p > 3$	[15]

2. Inequivalence of The Ness-Helleseth Functions With Known APN functions

In this section, we assume $p \geq 7$ and prove the Ness-Helleseth functions are CCZ-inequivalence with all APN power functions $g(x) = x^d$ listed in Table 1. By Table 1, if the opposite claim is assumed, the power exponent d will take at most five types of values as listed in Propositions 1-4 and Corollary 1 below. Thus, we need to prove such a CCZ-equivalence is impossible for these five types of d.

Suppose that $f(x)$ and $g(x) = x^d$ are CCZ-equivalent, then there exists an affine automorphism $L = (L_1, L_2)$ of $F_{p^n} \times F_{p^n}$ such that

$$L_2(x, f(x)) = g(L_1(x, f(x))) \pmod{x^{p^n} - x},$$

where $L_2(x, y) = a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i y^{p^i}$, $L_1(x, y) = c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i y^{p^i}$, $a, c, a_i, b_i, c_i, e_i \in F_{p^n}$ and $L_1(x, f(x))$ is a permutation. Thus, we have

$$a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i} = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^d \pmod{x^{p^n} - x}, \tag{3}$$

where $f(x)^{p^i}$ can be calculated as

$$f(x)^{p^i} = (ux^{\frac{p^n-1}{2}-1} + x^{p^n-2})^{p^i} = u^{p^i} x^{\frac{p^n-1}{2}-p^i} + x^{p^n-1-p^i}$$

since $\frac{p^n-1}{2} \equiv 1 \pmod 2$ for $p \equiv 3 \pmod 4$ and odd n.

The technique used in the following proofs is to expand the both sides of some equalities, and to compare and analyze the weights of the exponents of the monomials appeared in the expansions. Here a non-negative integer k with p-adic expansion $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$ $(0 \le k_i < p)$ is said to have *p-adic weight* as $wt(k) = k_0 + k_1 + \cdots + k_{n-1}$. Since we consider the equality (3) in the sense of moduloing $x^{p^n} - x$, a non-constant monomial x^γ is always treated by a monomial x^β with $0 < \beta \le p^n - 1$, where $\beta \equiv \gamma \,(\mathrm{mod}\, p^n - 1)$ if $\gamma \not\equiv 0 \,(\mathrm{mod}\, p^n - 1)$ and $\beta = p^n - 1$ if $\gamma \equiv 0 \,(\mathrm{mod}\, p^n - 1)$. The p-adic weight of such an integer β is regarded as the weight of γ.

In the following proofs to Propositions 1-4 and Corollary 1, we will encounter 35 kinds of monomials totally. Their exponents and the possible values of the corresponding weights are determined as in Table 2.

Lemma 1: Let $0 \le k,\ s,\ t,\ l,\ v \le n - 1$, and $q = p - 1$. The weights of the 35 kinds of exponents listed in Table 2 are correctly given in that table.

Proof: This can be carefully but tediously showed. We omit it here. □

Another simple fact below will be frequently used in the inequivalence proofs.

Lemma 2: Let $u \in F_{p^n}$ satisfy the condition in Equality (2) and $p \ge 7$. Then, none of the two systems of equations

$$\begin{cases} 2u^{p^i + p^j} + u^{2p^i} + 1 = 0; \\ u^{p^i + 2p^j} + u^{p^i} + 2u^{p^j} = 0, \end{cases} \quad \text{and} \quad \begin{cases} (u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j} = 0; \\ (u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j} = 0 \end{cases}$$

has solutions for any $i, j \in \{0, 1, \cdots, n-1\}$.

With the above preparation, the inequivalence of functions can now be discussed. The weights of exponents in Table 2 depend on p and n, and the proofs will be accordingly divided into three cases:
(1) $p \ge 7$ and $n \ge 3$;
(2) $p \ge 19$ and $n = 1$; and
(3) $p = 7$ or 11, and $n = 1$.

Below we give all inequivalence proofs only in the first case. Proofs in the second case can be shown in a similar way, and proofs in the last case can be directly verified with the help of a computer.

The reader will find the proof of Proposition 4 is very lengthy (more than five pages). We can not give a unified proof to these propositions and corollary.

Proposition 1: The function $f(x)$ is CCZ-inequivalent to $g(x) = x^3$ on F_{p^n}.

Proof: Suppose that $f(x)$ and $g(x) = x^3$ are CCZ-equivalent. Then, the exponents of indeterminate x in Equality (3) have 15 kinds of possible forms, which are exactly the first 15 kinds of exponents in Table 2.

Consider the exponent $3p^i$ of weight 3, where $i \in \{0, 1, \cdots, n-1\}$. By the weights of the first 15 kinds of exponents in Table 2, for $p \ge 7$ and $n \ge 3$, the exponent $3p^i$ only derives from the form $p^k + p^s + p^t$ with $k = s = t = i$. Therefore, the coefficient of x^{3p^i} on the right hand side (RHS) of Equality (3) is equal to c_i^3, and it is zero on the left hand side (LHS). This gives $c_i^3 = 0$, i.e., $c_i = 0$.

Considering the exponent $p^n - 1 - 3p^i$, similarly, one has $p^n - 1 - 3p^i = p^n - 1 - p^k - p^s - p^t$ and then $k = s = t = i$. As the case of x^{3p^i}, one can get that the coefficient of $x^{p^n - 1 - 3p^i}$ on the RHS of Equality (3) is equal to $e_i^3(3u^{2p^i} + 1)$, and it is zero on the LHS. Then, one has

$$e_i^3 (3u^2 + 1)^{p^i} = 0. \tag{4}$$

Table 2. Thirty-five kinds of exponents and their p-adic weights (with notation $q := p - 1$)

Exponent	p^k	$\frac{p^n-1}{2} - p^k$	$p^n - 1 - p^k$
Weight	1	$\frac{nq}{2} - 1$	$nq - 1$
Exponent	$p^k + p^s$	$p^n - 1 - p^k - p^s$	$p^k + \frac{p^n-1}{2} - p^s$
Weight	2	$nq - 2$	$\frac{nq}{2}$
Exponent	$\frac{p^n-1}{2} - p^k - p^s$	$p^k + p^s + p^t$	$p^k + p^s + \frac{p^n-1}{2} - p^t$
Weight	$\frac{nq}{2} - 2$	3	$\frac{nq}{2} + 1$
Exponent	$p^k + \frac{p^n-1}{2} - p^s - p^t$	$\frac{p^n-1}{2} - p^k - p^s - p^t$	$p^n - 1 - p^k - p^s - p^t$
Weight	$\frac{nq}{2} - 1$	$\frac{nq}{2} - 3\,(p^n > 7)$ $6\,(p^n = 7)$	$nq - 3$
Exponent	$p^k + p^n - 1 - p^s$	$p^k + p^s + p^n - 1 - p^t$	$p^k + p^n - 1 - p^s - p^t$
Weight	$(k-s)q$, or $(n+k-s)q$	$(k-t)q+1$, or $(s-t)q+1$, or $(n+\min\{k,s\}-t)q+1$	$(k-\min\{s,t\})q-1$, or $(n+k-s)q-1$, or $(n+k-t)q-1$
Exponent	$p^k + p^s + p^t + p^l$	$\frac{p^n-1}{2} - p^k - p^s - p^t - p^l$	$p^k + \frac{p^n-1}{2} - p^s - p^t - p^l$
Weight	4	$\frac{nq}{2} - 4\,(p > 7)$ $3n-4$ or $3n+2\,(p = 7)$	$\frac{nq}{2} - 2$
Exponent	$p^k + p^s + \frac{p^n-1}{2} - p^t - p^l$	$p^k + p^s + p^t + \frac{p^n-1}{2} - p^l$	$p^n - 1 - p^k - p^s - p^t - p^l$
Weight	$\frac{nq}{2}$	$\frac{nq}{2} + 2$	$nq - 4$
Exponent	$p^k + p^n - 1 - p^s - p^t - p^l$	$p^k + p^s + p^n - 1 - p^t - p^l$	$p^k + p^s + p^t + p^n - 1 - p^l$
Weight	$(k-\min\{s,t,l\})q-2$, or $(n+k-s)q-2$, or $(n+k-t)q-2$, or $(n+k-l)q-2$	$(k-\min\{t,l\})q$, or $(s-\min\{t,l\})q$, or $(k+s-t-l)q$, or $(n+\min\{k,s\}-l)q$, or $(n+\min\{k,s\}-t)q$, or $(n+k+s-t-l)q$	$(k-l)q+2$, or $(s-l)q+2$, or $(t-l)q+2$, or $(n+\min\{k,s,t\}-l)q+2$
Exponent	$p^k + p^s + p^t + p^l + p^v$	$\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v$	$p^k + \frac{p^n-1}{2} - p^s - p^t - p^l - p^v$
Weight	5	$\frac{nq}{2} - 5\,(p \geq 11, p^n > 11)$ $10(p^n = 11)$ $3n-5$ or $3n+1\,(p = 7)$	$\frac{nq}{2} - 3\,(p > 7)$, $3n-3$ or $3n+3\,(p = 7)$
Exponent	$p^k + p^s + \frac{p^n-1}{2} - p^t - p^l - p^v$	$p^k + p^s + p^t + \frac{p^n-1}{2} - p^l - p^v$	$p^k + p^s + p^t + p^l + \frac{p^n-1}{2} - p^v$
Weight	$\frac{nq}{2} - 1$	$\frac{nq}{2} + 1$	$\frac{nq}{2} + 3\,(p > 7)$, $3n+3$ or $3n-3\,(p = 7)$
Exponent	$p^n - 1 - p^k - p^s - p^t - p^l - p^v$	$p^k + p^n - 1 - p^s - p^t - p^l - p^v$	$p^k + p^s + p^t + p^l + p^n - 1 - p^v$
Weight	$nq - 5$	$(k-\min\{s,t,l,v\})q-3$, or $(n+k-s)q-3$, or $(n+k-t)q-3$, or $(n+k-l)q-3$, or $(n+k-v)q-3$	$(k-v)q+3$, or $(s-v)q+3$, or $(t-v)q+3$, or $(l-v)q+3$, or $(n+\min\{k,s,t,l\}-v)q+3$
Exponent	$p^k + p^s + p^t + p^n - 1 - p^l - p^v$ $(k \geq s \geq t$ and $l \geq v)$	$p^k + p^s + p^n - 1 - p^t - p^l - p^v$ $(k \geq s$ and $t \geq l \geq v)$	
Weight	$(k-v)q+1$, or $(s-v)q+1$, or $(t-v)q+1$, or $(k+s-l-v)q+1$, or $(k+t-l-v)q+1$, or $(s+t-l-v)q+1$, or $(n+t-l)q+1$, or $(n+t-v)q+1$, or $(n+s+t-l-v)q+1$, or $(n+k+t-l-v)q+1$	$(k-v)q-1$, or $(s-v)q-1$, or $(k+s-l-v)q-1$, or $(k+s-t-v)q-1$, or $(n+s-t)q-1$, or $(n+s-l)q-1$, or $(n+s-v)q-1$, or $(n+k+s-t-v)q-1$, or $(n+k+s-t-l)q-1$, or $(n+k+s-l-v)q-1$	

Similarly, the following equality can be obtained by considering the coefficient of $x^{\frac{p^n-1}{2}-3p^i}$,

$$e_i^3(u^3+3u)^{p^i}=0. \tag{5}$$

By Lemma 2, Equalities (4) and (5) imply $e_i=0$ for all $i\in\{0,1,\cdots,n-1\}$. Thus $L_1(x,f(x))=c$ is not a permutation.

Therefore, $f(x)$ and $g(x)=x^3$ are CCZ-inequivalent on F_{p^n}. □

Corollary 1: The function $f(x)$ is CCZ-inequivalent to $g(x)=x^{\frac{2p^n-1}{3}}$, where $p^n\equiv 2(\text{mod } 3)$.

Proof: For $p^n\equiv 2\,(\text{mod } 3)$ and $p\equiv 3\,(\text{mod } 4)$, one has $p\geq 11$. If $f(x)$ and $g(x)=x^{\frac{2p^n-1}{3}}$ are CCZ-equivalent on F_{p^n}, then one has

$$(a+\sum_{i=0}^{n-1}a_ix^{p^i}+\sum_{i=0}^{n-1}b_if(x)^{p^i})^3=c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i}(\text{mod } x^{p^n}-x). \tag{6}$$

A same analysis as in Proposition 1 gives $a_i=b_i=0$ for any $0\leq i\leq n-1$. Equality (6) can be reduced to

$$a^3=c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i}(\text{mod } x^{p^n}-x),$$

which implies $c_i=e_i=0$ for any i. Thus, $L_1(x,f(x))=c$. This contradicts with that $L_1(x,f(x))$ is a permutation. The contradiction proves CCZ-inequivalence of $f(x)$ and $g(x)=x^{\frac{2p^n-1}{3}}$. □

Proposition 2: The function $f(x)$ is CCZ-inequivalent to $g(x)=x^{p^n-2}$ on F_{p^n}, where $p\equiv 2(\text{mod } 3)$.

Proof: Suppose that $f(x)$ and x^{p^n-2} are CCZ-equivalent. By $p\equiv 3(\text{mod } 4)$ and $p\equiv 2(\text{mod } 3)$, one has $p\geq 11$. Multiplying both sides of Equality (3) by $(c+\sum\limits_{i=0}^{n-1}c_ix^{p^i}+\sum\limits_{i=0}^{n-1}e_if(x)^{p^i})^2$ implies

$$\begin{aligned}(a+\sum_{i=0}^{n-1}a_ix^{p^i}+\sum_{i=0}^{n-1}b_if(x)^{p^i})(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2\\ =c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i}\,(\text{mod}\,x^{p^n}-x).\end{aligned} \tag{7}$$

Then, the exponents of indeterminate x in Equality (7) have 15 kinds of possible forms, which are exactly the first 15 kinds of exponents in Table 2.

For any i, $0\leq i\leq n-1$, by a similar analysis as above for the coefficients of the exponents $3p^i$, $\frac{p^n-1}{2}-3p^i$, and p^n-1-3p^i in Equality (7), one has

$$\begin{cases}a_ic_i^2=0;\\ b_ie_i^2(u^3+3u)^{p^i}=0;\\ b_ie_i^2(3u^2+1)^{p^i}=0.\end{cases} \tag{8}$$

By Lemma 2, Equality (8) gives

$$a_ic_i=0 \text{ and } b_ie_i=0. \tag{9}$$

Considering the exponent $p^n-1-p^i-2p^j$ $(0\leq i\neq j\leq n-1)$, again by the weights of the first 15 exponents in Table 2, one has $p^n-1-p^i-2p^j=p^n-1-p^k-p^s-p^t$ and then $k=i$, $s=t=j$, or $s=i$, $k=t=j$, or $t=i$, $k=s=j$. Thus, by Equality (8), the coefficient of $x^{p^n-1-p^i-2p^j}$ on the LHS of Equality (7) is equal to

$$(b_ie_j^2+2b_je_ie_j)(2u^{p^i+p^j}+u^{2p^j}+1)=b_ie_j^2(2u^{p^i+p^j}+u^{2p^j}+1),$$

and it is zero on the RHS. Thus,

$$b_i e_j^2 (2u^{p^i+p^j} + u^{2p^j} + 1) = 0. \tag{10}$$

Similarly as above, from the coefficient of $x^{\frac{p^n-1}{2}-p^i-2p^j}$ $(i \neq j)$, one has

$$b_i e_j^2 (u^{p^i+2p^j} + u^{p^i} + 2u^{p^j}) = 0, \tag{11}$$

which together with Equality (10) implies that $b_i e_j = 0$ holds for any $0 \leq i \neq j \leq n-1$. This together with Equality (9) shows that $b_i e_j = 0$ for any $i,\ j \in \{0, 1, \cdots, n-1\}$. That is to say that $b_0 = b_1 = \cdots = b_{n-1} = 0$ or $e_0 = e_1 = \cdots = e_{n-1} = 0$.

Consider the exponent $p^i + 2p^j$ $(i \neq j)$ of weight 3, where $i,\ j \in \{0, 1, \cdots, n-1\}$. Among the first 15 kinds of exponents in Table 2, the exponent $p^i + 2p^j$ only derives from the form $p^k + p^s + p^t$ with $k = i$ and $s = t = j$, or $s = i$ and $k = t = j$, or $t = i$ and $k = s = j$. Therefore, the coefficient of $x^{p^i+2p^j}$ on the LHS of Equality (7) is equal to $a_i c_j^2 + 2a_j c_i c_j$, and it is zero on the RHS. This gives

$$a_i c_j^2 + 2a_j c_i c_j = 0. \tag{12}$$

By Equalities (9) and (12), one has $a_i c_j = 0$ for any $i,\ j \in \{0, 1, \cdots, n-1\}$. That is to say that $a_0 = a_1 = \cdots = a_{n-1} = 0$ or $c_0 = c_1 = \cdots = c_{n-1} = 0$.

Assume that $e_j = 0$ for any $j \in \{0, 1, \cdots, n-1\}$. Since $L_1(x, f(x))$ is a permutation, there exists some j_0 such that $c_{j_0} \neq 0$. Thus, one has $a_i = 0$ for any i, and then Equality (7) can be reduced to

$$(a + \sum_{i=0}^{n-1} b_i f(x)^{p^i})(c + \sum_{i=0}^{n-1} c_i x^{p^i})^2 = c + \sum_{i=0}^{n-1} c_i x^{p^i} \pmod{x^{p^n} - x}. \tag{13}$$

By Table 2, the exponent $p^n - 1 - p^i + 2p^j$ $(i \neq j)$ has weight $\alpha(p-1)+1$, where $i,\ j \in \{0, 1, \cdots, n-1\}$ and $1 \leq \alpha \leq n-1$, then the exponent $p^n - 1 - p^i + 2p^j$ $(i \neq j)$ only derives from the form $p^k + p^s + p^n - 1 - p^t$ with $t = i$, $k = s = j$. Therefore, the coefficient of $x^{p^n-1-p^i+2p^j}$ on the LHS of Equality (7) is equal to $b_i c_j^2 + 2a_j c_j e_i$, and it is zero on the RHS. This together with Equality (9) show

$$b_i c_j^2 = 0. \tag{14}$$

For $j = j_0$, the equation $b_i c_{j_0}^2 = 0$ implies that $b_i = 0$ for any $i \neq j_0$. For $i = j_0$, the equation $b_{j_0} c_j^2 = 0$ implies that $b_{j_0} = 0$ or $c_j = 0$ for any $j \neq j_0$. In other words, one has $b_i = 0$ for any i, or $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$.

When $b_i = 0$ for any $i \in \{0, 1, \cdots, n-1\}$, Equality (3) is equal to

$$a = (c + \sum_{i=0}^{n-1} c_i x^{p^i})^{p^n-2} \pmod{x^{p^n} - x}. \tag{15}$$

Then $L_2(x, f(x)) = a$ and $L_1(x, f(x))^{p^n-2}$ is a permutation. This is impossible.

When $b_{j_0} c_{j_0} \neq 0$ and $b_j = c_j = 0$ for any $j \neq j_0$, then Equality (13) is further reduced to

$$(a + b_{j_0} f(x)^{p^{j_0}})(c + c_{j_0} x^{p^{j_0}})^2 = c + c_{j_0} x^{p^{j_0}} \pmod{x^{p^n} - x}. \tag{16}$$

Since the coefficient of $x^{\frac{p^n-1}{2}+p^{j_0}}$ on the LHS of Equality (16) is equal to $b_{j_0} c_{j_0}^2 u^{p^{j_0}}$, one has $b_{j_0} c_{j_0}^2 u^{p^{j_0}} = 0$ which implies $b_{j_0} c_{j_0} = 0$. That is also a contradiction.

Now one should assume that there exists some integer j_0 such that $e_{j_0} \neq 0$. Then $b_j = 0$ for any j. If $a_i = 0$ for any i, then by Equality (15), one has $L_1(x, f(x)) = c$. This is impossible, and then there exists at least one nonzero element in $\{a_i \,|\, 0 \leq i \leq n-1\}$. Thus, $c_j = 0$ for any j, and Equality (7) is reduced to

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i})(c + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^2 = c + \sum_{i=0}^{n-1} e_i f(x)^{p^i} \,(\text{mod}\, x^{p^n} - x). \tag{17}$$

Also by Table 2, the exponent $p^n - 1 + p^i - 2p^j$ $(i \neq j)$ has weight $\alpha(p-1) - 1$, where i, $j \in \{0, 1, \cdots, n-1\}$ and $1 \leq \alpha \leq n-1$. Then, the exponent $p^n - 1 + p^i - 2p^j$ $(i \neq j)$ only derives from the form $p^n - 1 + p^k - p^s - p^t$ with $k = i$ and $s = t = j$. Therefore, the coefficient of $x^{p^n - 1 + p^i - 2p^j}$ on the LHS of Equality (7) is equal to $a_i e_j^2 (u^{2p^j} + 1)$, and it is zero on the RHS. This gives

$$a_i e_j^2 (u^2 + 1)^{p^j} = 0, \tag{18}$$

and then

$$a_i e_j^2 = 0 \tag{19}$$

since $u^2 + 1 \neq 0$.

For $j = j_0$, the equation $a_i e_{j_0}^2 = 0$ implies that $a_i = 0$ for any $i \neq j_0$ since $e_{j_0} \neq 0$. Since there exists at least one nonzero element in $\{a_i \,|\, 0 \leq i \leq n-1\}$, one has $a_{j_0} \neq 0$ and the equation $a_{j_0} e_j^2 = 0$ implies $e_j = 0$ for any $j \neq j_0$. Thus, one has $a_{j_0} e_{j_0} \neq 0$ and $b_j = c_j = 0$ for any j. Equality (7) is reduced to

$$(a + a_{j_0} x^{p^{j_0}})(c + e_{j_0} f(x)^{p^{j_0}})^2 = c + e_{j_0} f(x)^{p^{j_0}} \,(\text{mod}\, x^{p^n} - x). \tag{20}$$

Considering the coefficient of $x^{p^{j_0}}$ in Equality (20), one has $a_{j_0} c^2 = 0$ and then $c = 0$. From the coefficients of $x^{p^n - 1 - p^{j_0}}$ and $x^{\frac{p^n-1}{2} - p^{j_0}}$, one has

$$\begin{cases} a_{j_0} e_{j_0}^2 (u^2 + 1)^{p^{j_0}} = e_{j_0}; \\ 2a_{j_0} e_{j_0}^2 u^{p^{j_0}} = e_{j_0} u^{p^{j_0}}, \end{cases}$$

which implies $u = \pm 1$ since $a_{j_0} e_{j_0} \neq 0$. This contradicts with $u \neq \pm 1$.

The arguments above prove that $f(x)$ and $g(x) = x^{p^n - 2}$ are CCZ-inequivalent on F_{p^n}. □

By analyzing the weights of the exponents in Equality (3), the following proposition can be proved in a similar way.

Proposition 3: The functions $f(x)$ and $g(x) = x^d$ are CCZ-inequivalent on F_{p^n}, if $d = \frac{p^n+1}{4}$ for $p^n \equiv 7 \,(\text{mod } 8)$ and $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$ for $p^n \equiv 3 \,(\text{mod } 8)$.

Proof: Assume that $f(x)$ and $g(x) = x^d$ are CCZ-equivalent. Then, by Equality (3), one has

$$(a + \sum_{i=0}^{n-1} a_i x^{p^i} + \sum_{i=0}^{n-1} b_i f(x)^{p^i})^4 = (c + \sum_{i=0}^{n-1} c_i x^{p^i} + \sum_{i=0}^{n-1} e_i f(x)^{p^i})^2 (\text{mod } x^{p^n} - x). \tag{21}$$

The exponents of indeterminate x in Equality (21) have 24 kinds of possible forms, and they are the first 24 kinds of the exponents in Table 2. From this table, the weight of $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l$ depends on whether the character p is 7 or not. The following discussion is divided into two subcases $p > 7$ and $p = 7$.

Case 1: $p > 7$.

Consider the exponent $4p^i$ of weight 4, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $4p^i$ only derives from $p^k + p^s + p^t + p^l$ with $k = s = t = l = i$. Therefore, the coefficient of x^{4p^i} on the LHS of Equality (21) is equal to a_i^4, and it is zero on the RHS. This gives $a_i^4 = 0$, i.e., $a_i = 0$.

Considering the exponent $\frac{p^n-1}{2}-4p^i$ of weight $\frac{n(p-1)}{2}-4$, by Table 2, $\frac{p^n-1}{2}-4p^i=\frac{p^n-1}{2}-p^k-p^s-p^t-p^l$ and then $k=s=t=l=i$. Since the coefficient of $x^{\frac{p^n-1}{2}-4p^i}$ on the LHS of Equality (21) is equal to $b_i^4(4u^3+4u)^{p^i}$, and it is zero on the RHS, one has

$$b_i^4(4u^3+4u)^{p^i}=0, \tag{22}$$

which implies that $b_i=0$ since $4u^3+4u=4u(u^2+1)\neq 0$.

Thus, Equality (21) can be rewritten as

$$a^4=(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2(\text{mod } x^{p^n}-x). \tag{23}$$

Since the LHS of Equality (21) is a constant and the RHS runs through $\{z\in F_{p^n}|\chi(z)=0,1\}$, it is a contradiction, which shows that $f(x)$ is CCZ-inequivalent to $g(x)=x^d$ for $p>7$.

Case 2: $p=7$.

Consider the exponent $3p^i+p^j$ $(i\neq j)$ of weight 4, where $i,\, j\in\{0,1,\cdots,n-1\}$. By Table 2, the exponent $3p^i+p^j$ only derives from $p^k+p^s+p^t+p^l$ with $k=s=t=i$ and $l=j$. Therefore, the coefficient of $x^{3p^i+p^j}$ on the LHS of Equality (21) is equal to $4a_i^3a_j$, and it is zero on the RHS. This gives $4a_i^3a_j=0$. If $a_{i_0}\neq 0$, then one has $a_i=0$ for any $i\neq i_0$. That is to say, there exists at most one nonzero element in $\{a_i\,|\,0\leq i\leq n-1\}$.

Considering the exponent p^n-1-4p^i of weight $6n-4$, by Table 2, the exponent has two forms $p^n-1-p^k-p^s-p^t-p^l$ with $k=s=t=l=i$, or $p^k+p^s+p^t+p^n-1-p^l$ with $k=s=t=i$, $l=i+1$. Since the coefficient of $x^{p^n-1-4p^i}$ on the LHS of Equality (21) is equal to $4a_i^3b_{i+1}+b_i^4(u^4+6u^2+1)^{p^i}$, and it is zero on the RHS, one has

$$4a_i^3b_{i+1}+b_i^4(u^4+6u^2+1)^{p^i}=0, \tag{24}$$

which implies $b_i=0\,(i\neq i_0)$ since $a_i=0$ for any $i\neq i_0$ and

$$u^4+6u^2+1=(u^2+2)(u^2+4)=(u^2+3^2)(u^2+2^2)\neq 0. \tag{25}$$

For $i=i_0$, one has $b_{i_0+1}=0$. Then, the equality $4a_{i_0}^3b_{i_0+1}+b_{i_0}^4(u^4+6u^2+1)^{p^{i_0}}=0$ implies $b_{i_0}=0$. Therefore, $b_i=0$ for any i.

Consider the exponent $4p^i$ of weight 4, where $i\in\{0,1,\cdots,n-1\}$. By Table 2, the exponent $4p^i$ has the forms as $p^k+p^s+p^t+p^l$ with $k=s=t=l=i$, or $p^k+p^n-1-p^s-p^t-p^l$ with $k=i+1$ and $s=t=l=i$. Since the coefficient of x^{4p^i} on the LHS of Equality (21) is equal to $a_i^4+12a_{i+1}b_i^3u^{2p^i}+4a_{i+1}b_i^3$, and it is zero on the RHS. This gives

$$a_i^4+12a_{i+1}b_i^3u^{2p^i}+4a_{i+1}b_i^3=0. \tag{26}$$

Then, one has

$$a_i^4=0 \tag{27}$$

since $b_i=0$ for any i. Equality (27) shows $a_i=0$ for any $i\in\{0,1,\cdots,n-1\}$. Thus, Equality (23) can be rewritten as

$$a^4=(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^2\,(\text{mod}\,x^{p^n}-x). \tag{28}$$

Similar to the analysis after Equality (23), the function $f(x)$ is CCZ-inequivalent to $g(x)=x^d$ for $p=7$.

Proposition 4: The functions $f(x)$ and $g(x)=x^d$ are CCZ-inequivalent on F_{p^n}, if $d=\frac{p^n-1}{2}-1$ for $p\equiv 3,7\,(\text{mod } 20)$.

Proof: Assume that $f(x)$ and $g(x)=x^d$ are CCZ-equivalent. Squaring both sides of Equality (3) and multiplying $(c+\sum\limits_{t=0}^{n-1}c_tx^{p^t}+\sum\limits_{t=0}^{n-1}e_tf(x)^{p^t})^3$ for both sides imply

$$\begin{aligned}&(a+\sum_{s=0}^{n-1}a_sx^{p^s}+\sum_{s=0}^{n-1}b_sf(x)^{p^s})^2(c+\sum_{t=0}^{n-1}c_tx^{p^t}+\sum_{t=0}^{n-1}e_tf(x)^{p^t})^3\\ &=c+\sum_{t=0}^{n-1}c_tx^{p^t}+\sum_{t=0}^{n-1}e_tf(x)^{p^t}(\mathrm{mod}\ x^{p^n}-x).\end{aligned}\tag{29}$$

We claim that there exists some integer j_0 such that $e_{j_0}\neq 0$. Otherwise, if $e_j=0$ holds for any j, Equality (29) can be reduced to

$$(a+\sum_{s=0}^{n-1}a_sx^{p^s}+\sum_{s=0}^{n-1}b_sf(x)^{p^s})^2(c+\sum_{t=0}^{n-1}c_tx^{p^t})^3=c+\sum_{t=0}^{n-1}c_tx^{p^t}(\mathrm{mod}\ x^{p^n}-x).\tag{30}$$

Consider the exponent $\frac{p^n-1}{2}-2p^i+3p^j$ $(i\neq j)$ of weight $\frac{n(p-1)}{2}+1$. By Table 2, the exponent $\frac{p^n-1}{2}-2p^i+3p^j$ only has the form $p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$ with $k=s=t=j$ and $l=v=i$. The coefficient of $\frac{p^n-1}{2}-2p^i+3p^j$ on the LHS of Equality (30) is equal to $2b_i^2c_j^3u^{p^i}$ and it is zero on the RHS. Thus, $b_ic_j=0$ for any $i\neq j$.

Since $L_1(x,f(x))$ is a permutation, there exists some integer j_0 such that $c_{j_0}\neq 0$. For $i\neq j$, the equation $b_ic_j=0$ implies that $b_i=0$ for any i, or $b_{j_0}c_{j_0}\neq 0$ and $b_j=c_j=0$ for any $j\neq j_0$.

When $b_i=0$ for any i, Equality (30) is equal to

$$(a+\sum_{s=0}^{n-1}a_sx^{p^s})^2(c+\sum_{t=0}^{n-1}c_tx^{p^t})^3=c+\sum_{t=0}^{n-1}c_tx^{p^t}\,(\mathrm{mod}\,x^{p^n}-x).$$

Since the coefficient of x^{5p^i} on the LHS of the above equality is $a_i^2c_i^3$ and it is zero on the RHS, one has $a_ic_i=0$. Similarly, from the coefficient of $x^{2p^i+3p^j}$ $(i\neq j)$ in the equality above, one has $a_i^2c_j^3+6a_ia_jc_ic_j^2+3a_j^2c_i^2c_j=a_i^2c_j^3=0$ since $a_ic_i=0$ for any i. Thus, $a_ic_j=0$ for any i and j. The inequality $c_{j_0}\neq 0$ implies $a_i=0$ for any i.

We next show $L_1(x,f(x))$ is not a permutation when $a_i=b_i=0$ for any i.

By $a_i=b_i=0$, Equality (3) can be reduced to

$$a=(c+\sum_{t=0}^{n-1}c_tx^{p^t}+\sum_{t=0}^{n-1}e_tf(x)^{p^t})^{\frac{p^n-1}{2}-1}(\mathrm{mod}\ x^{p^n}-x).\tag{31}$$

Since $\gcd(\frac{p^n-1}{2}-1,p^n-1)=2$, there exists an integer λ such that $\lambda(\frac{p^n-1}{2}-1)\equiv 2(\mathrm{mod}\ p^n-1)$. Thus, from Equality (31), one has

$$a^\lambda=(c+\sum_{t=0}^{n-1}c_tx^{p^t}+\sum_{t=0}^{n-1}e_tf(x)^{p^t})^2\,(\mathrm{mod}\ x^{p^n}-x).$$

By the similar analysis after Equality (23), the equality above is impossible.

When $b_{j_0}c_{j_0}\neq 0$ and $b_j=c_j=0$ for any $j\neq j_0$, Equality (30) becomes

$$(a+\sum_{s=0}^{n-1}a_sx^{p^s}+b_{j_0}f(x)^{p^{j_0}})^2(c+c_{j_0}x^{p^{j_0}})^3=c+c_{j_0}x^{p^{j_0}}(\mathrm{mod}\ x^{p^n}-x).\tag{32}$$

Consider the coefficient of $x^{2p^i+3p^{j_0}}$ $(i\neq j_0)$ in Equality (32), one has $a_i^2c_{j_0}^3=0$. This implies $a_i=0$ for $i\neq j_0$ since $c_{j_0}\neq 0$. Thus, Equality (32) becomes

$$(a+a_{j_0}x^{p^{j_0}}+b_{j_0}f(x)^{p^{j_0}})^2(c+c_{j_0}x^{p^{j_0}})^3=c+c_{j_0}x^{p^{j_0}}(\mathrm{mod}\ x^{p^n}-x).\tag{33}$$

From the coefficients of $x^{5p^{j_0}}$ and $x^{3p^{j_0}}$ in Equality (33), one has

$$\begin{cases} a_{j_0}^2 c_{j_0}^3 = 0; \\ a^2 c_{j_0}^3 + 6aca_{j_0}c_{j_0}^2 + 3c^2 a_{j_0}^2 c_{j_0} = 0, \end{cases}$$

which implies $a_{j_0} = a = 0$. Furthermore, from the coefficient of $x^{\frac{p^n-1}{2}-2p^{j_0}+3p^{j_0}}$, one has $b_{j_0}^2 c_{j_0}^3 = 0$. This is a contradiction.

Therefore, there exists some integer j_0 such that $e_{j_0} \neq 0$.

Since the weights of some exponents in Table 2 depend on the concrete values of p and n, the following discussion will be divided into three subcases: (1) $p > 7$; (2) $p = 7$ and $n \geq 5$; (3) $p = 7$ and $n = 3$.

Case 1: $p > 7$.

Consider the exponent $\frac{p^n-1}{2} - 5p^i$ of weight $\frac{n(p-1)}{2} - 5$, where $i \in \{0, 1, \cdots, n-1\}$. By Table 2, the exponent $\frac{p^n-1}{2} - 5p^i$ only has the form as $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v$ with $k = s = t = l = v = i$. Since the coefficient of $x^{\frac{p^n-1}{2}-5p^i}$ on the LHS of Equality (29) is equal to $b_i^2 e_i^3 (u^5 + 10u^3 + 5u)^{p^i}$, and it is zero on the RHS, one has

$$b_i^2 e_i^3 (u^5 + 10u^3 + 5u)^{p^i} = 0. \tag{34}$$

Similarly, comparing the coefficients of $x^{p^n-1-5p^i}$ on both sides of Equality (29), one has

$$b_i^2 e_i^3 (5u^4 + 10u^2 + 1)^{p^i} = 0. \tag{35}$$

By Lemma 2, Equalities (34) and (35) imply that $b_i e_i = 0$ for any i.

The coefficient of $x^{\frac{p^n-1}{2}-2p^i-3p^j} (i \neq j)$ on the LHS of Equality (29) is

$$(b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}),$$

and it is zero on the RHS. Thus, one has

$$(b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}) = 0. \tag{36}$$

Similarly, from the coefficient of $x^{p^n-1-2p^i-3p^j} (i \neq j)$, one has

$$(b_i^2 e_j^3 + 6b_i b_j e_i e_j^2 + 3b_j^2 e_i^2 e_j)((u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}) = 0. \tag{37}$$

which together with Equality (36) implies

$$\begin{cases} b_i^2 e_j^3 ((u^2+1)^{p^i}(u^3+3u)^{p^j} + 2u^{p^i}(3u^2+1)^{p^j}) = 0; \\ b_i^2 e_j^3 ((u^2+1)^{p^i}(3u^2+1)^{p^j} + 2u^{p^i}(u^3+3u)^{p^j}) = 0. \end{cases} \tag{38}$$

since $b_i e_i = 0$ for any i.

By Lemma 2, Equality (38) implies that $b_i e_j = 0$ for any $i \neq j$. By $b_i e_i = 0$, one has $b_i e_j = 0$ for any i and j. Since there exists some integer j_0 such that $e_{j_0} \neq 0$, one has $b_i = 0$ for any i.

From the coefficients of $x^{p^n-1-3p^j+2p^i} (i \neq j)$ and $x^{\frac{p^n-1}{2}-3p^j+2p^i} (i \neq j)$, one has

$$\begin{cases} (a_i^2 e_j^3 + 6a_i b_j c_i e_j^2 + 3b_j^2 c_i^2 e_j)(3u^2+1)^{p^j} = 0; \\ (a_i^2 e_j^3 + 6a_i b_j c_i e_j^2 + 3b_j^2 c_i^2 e_j)(u^3+3u)^{p^j} = 0. \end{cases}$$

Since $b_i = 0$ for any i, the equality above becomes

$$\begin{cases} a_i^2 e_j^3 (3u^2+1)^{p^j} = 0; \\ a_i^2 e_j^3 (u^3+3u)^{p^j} = 0, \end{cases}$$

which implies that $a_ie_j = 0$ for any $i \neq j$ by Lemma 2. For $j = j_0$, the equality $a_ie_{j_0} = 0$ implies $a_i = 0$ for any $i \neq j_0$. Equality (3) can be reduced to

$$a + a_{j_0}x^{p^{j_0}} = (c + \sum_{i=0}^{n-1} c_ix^{p^i} + \sum_{i=0}^{n-1} e_jf(x)^{p^j})^{\frac{p^n-1}{2}-1} \,(\mathrm{mod}\, x^{p^n} - x). \tag{39}$$

Since $\gcd(\frac{p^n-1}{2} - 1, p^n - 1) = 2$, the monomial $x^{\frac{p^n-1}{2}-1}$ is not a permutation. The LHS of Equality (39) is a constant or a permutation and its RHS is not a permutation, i.e., its LHS has image $\{a\}$ if $a_{j_0} = 0$, or F_{p^n} if $a_{j_0} \neq 0$, while its RHS has image $\{z \in F_{p^n} | \chi(z) = 0, 1\}$. Thus, Equality (39) is impossible.

According to the arguments above, $f(x)$ and $g(x) = x^{\frac{p^n-1}{2}-1}$ are CCZ-inequivalent on F_{p^n} when $p > 7$ and n is odd.

Case 2: $p = 7, n \geq 5$.

Consider the exponents $\frac{p^n-1}{2} - 2p^i - 3p^j$ $(i \neq j)$ and $p^n - 1 - 2p^i - 3p^j$ $(i \neq j)$, one has Equalities (36) and (37), which implies that

$$b_i^2e_j^3 + 6b_ib_je_ie_j^2 + 3b_j^2e_i^2e_j = ((b_ie_j + 3b_je_i)^2 + b_j^2e_i^2)e_j = 0. \tag{40}$$

For $j = j_0$, since $e_{j_0} \neq 0$ and -1 is nonsquare, one has $b_ie_{j_0} + 3b_{j_0}e_i = b_{j_0}e_i = 0$, i.e.,

$$b_ie_{j_0} = b_{j_0}e_i = 0. \tag{41}$$

This implies that $b_i = 0$ for any i, or $b_{j_0} \neq 0$ and $b_i = e_i = 0$ for any $i \neq j_0$.

From the coefficient of the monomial with exponent $2p^i + \frac{p^n-1}{2} - 3p^j$ $(i \neq j)$, one has

$$(a_i^2e_j^3 + 6a_ib_jc_ie_j^2 + 3b_j^2c_i^2e_j)(u^3 + 3u)^{p^j} = 0. \tag{42}$$

Since -1 is a nonsquare element in F_{p^n}, one has $\chi(3) = \chi(-4) = -1$. We say $u^3 + 3u \neq 0$. Otherwise, $u = 0$, 2, or 5 and then $\chi(u + 1) \neq \chi(u - 1)$. This is a contradiction. Therefore, Equality (42) implies that

$$a_i^2e_j^3 + 6a_ib_jc_ie_j^2 + 3b_j^2c_i^2e_j = ((a_ie_j + 3b_jc_i)^2 + b_j^2c_i^2)e_j = 0. \tag{43}$$

For $j = j_0$, one has $a_ie_{j_0} + 3b_{j_0}c_i = b_{j_0}c_i = 0$ since -1 is a nonsquare element, i.e., $a_i = 0$ for any $i \neq j_0$. If $b_{j_0} \neq 0$, then $c_i = 0$ for any $i \neq j_0$. If $b_i = 0$ for any i, Equality (43) can be reduced to $a_ie_j = 0$.

According to the discussion after Equalities (41) and (43), we derive that $b_i = 0$ for any i and $a_ie_j = 0$ for any $i \neq j$, or $b_{j_0} \neq 0$ and $a_i = b_i = c_i = e_i = 0$ for any $i \neq j_0$.

Assume that $b_i = 0$ for any i and $a_ie_j = 0$ for any $i \neq j$. If $a_{j_0} = 0$, i.e., $a_i = 0$ for any i since $e_{j_0} \neq 0$, then $L_1(x, f(x)) = c$ is not a permutation. If $a_{j_0} \neq 0$, then $a_{j_0}e_j = 0$ implies $e_j = 0$ for any $j \neq j_0$. Therefore, Equality (29) can be reduced to

$$a + a_{j_0}x^{p^{j_0}} = (c + \sum_{i=0}^{n-1} c_ix^{p^i} + e_{j_0}f(x)^{p^{j_0}})^{\frac{p^n-1}{2}-1} \,(\mathrm{mod}\, x^{p^n} - x). \tag{44}$$

By similar to the analysis after Equality (39), Equality (44) is impossible.

Assume that $b_{j_0} \neq 0$ and $a_i = b_i = c_i = e_i = 0$ for any $i \neq j_0$. Equality (29) can be reduced to

$$(a+a_{j_0}x^{p^{j_0}} + b_{j_0}f(x)^{p^{j_0}})^2(c+c_{j_0}x^{p^{j_0}} + e_{j_0}f(x)^{p^{j_0}})^3 = c+c_{j_0}x^{p^{j_0}} + e_{j_0}f(x)^{p^{j_0}} \,(\mathrm{mod}\, x^{p^n} - x). \tag{45}$$

Considering the coefficients of $x^{\frac{p^n-1}{2}-5p^{j_0}}$ and $x^{p^n-1-5p^{j_0}}$ in Equality (45), one has

$$\begin{cases} b_{j_0}^2e_{j_0}^3(u^5 + 10u^3 + 5u)^{p^{j_0}} = 0; \\ b_{j_0}^2e_{j_0}^3(5u^4 + 10u^2 + 1)^{p^{j_0}} = 0, \end{cases}$$

which implies $b_{j_0}e_{j_0}=0$ by Lemma 2. That's a contradiction with $b_{j_0}e_{j_0}\neq 0$. Therefore, $f(x)$ and $g(x)=x^{\frac{p^n-1}{2}-1}$ are CCZ-inequivalent on F_{7^n}, where $n\geq 5$ is odd.

Case 3: $p=7, n=3$.

For all integers i, j with $0\leq i\neq j\leq 2$, considering the coefficients of $x^{2p^i+\frac{p^n-1}{2}-3p^j}$, it can be similarly proven that Equalities (42) and (43) hold. From these two equalities, one has

$$a_ie_j=e_jb_jc_i=0,\ i\neq j. \tag{46}$$

Considering the exponent $\frac{p^n-1}{2}-2p^i-3p^j\,(i\neq j)$, where $i,j=0,1,2$, it has two forms $\frac{p^n-1}{2}-p^k-p^s-p^t-p^l-p^v$, and $p^k+p^s+p^t+p^l$ with $k=i$ and $w\neq i,j$, where $w=s=t=l$. Then, its coefficients on both sides of Equality (29) give

$$\begin{split}(b_i^2e_j^3+6b_ib_je_ie_j^2+3b_j^2e_i^2e_j)[(u^2+1)^{p^i}(u^3+3u)^{p^j}+2u^{p^i}(3u^2+1)^{p^j}]\\ +2aa_ic_w^3+6a_ia_wcc_w^2+6aa_wc_ic_w^2+6a_w^2cc_ic_w=0.\end{split} \tag{47}$$

For $i,j=0,1,2$, considering the exponent $p^n-1-2p^i-3p^j\,(i\neq j)$, it has a unique form $p^n-1-p^k-p^s-p^t-p^l-p^v$. Then, its coefficients on both sides of Equality (29) give

$$(b_i^2e_j^3+6b_ib_je_ie_j^2+3b_j^2e_i^2e_j)[(u^2+1)^{p^i}(3u^2+1)^{p^j}+2u^{p^i}(u^3+3u)^{p^j}]=0. \tag{48}$$

Considering the coefficients of the monomials with exponents $p^n-1-2p^i+3p^{i+1}(=19,133,247)$, one has

$$\begin{cases}(3a_1^2c_1e_0^2+6a_1b_0c_1^2e_0+b_0^2c_1^3)(u^2+1)=0;\\ (3a_2^2c_2e_1^2+6a_2b_1c_2^2e_1+b_1^2c_2^3)(u^2+1)^7=0;\\ (3a_0^2c_0e_2^2+6a_0b_2c_0^2e_2+b_2^2c_0^3)(u^2+1)^{49}=0.\end{cases} \tag{49}$$

Since $u^2+1\neq 0$ and $a_ie_j=0$ for any $i\neq j$, one has

$$b_0^2c_1^3=b_1^2c_2^3=b_2^2c_0^3=0.$$

Therefore, there exist eight possible cases as follows.

1) $c_0=c_1=c_2=0$;
2) $c_1=c_2=b_2=0,\ c_0\neq 0$;
3) $c_2=c_0=b_0=0,\ c_1\neq 0$;
4) $c_0=c_1=b_1=0,\ c_2\neq 0$;
5) $c_1=b_1=b_2=0,\ c_0c_2\neq 0$;
6) $c_2=b_2=b_0=0,\ c_1c_0\neq 0$;
7) $c_0=b_0=b_1=0,\ c_2c_1\neq 0$;
8) $b_0=b_1=b_2=0,\ c_0c_1c_2\neq 0$.

We only give the analysis of Cases 1), 2), 5), and 8). The Cases 3), 4), 6), and 7) can be similarly analyzed.

1) Considering the exponent $\frac{p^n-1}{2}-5p^i\,(=5+2p+3p^2, 3+5p+2p^2, 2+3p+5p^2)$ of weight 10, it has 4 possible forms as $p^k+p^s+\frac{p^n-1}{2}-p^t$, $p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$, and $\frac{p^n-1}{2}-p^k-p^s-p^t-p^l-p^v$ where $k,s,t,l,v\in\{0,1,2\}$.

If $p^k+p^s+\frac{p^n-1}{2}-p^t\equiv\frac{p^n-1}{2}-5p^i\ (\mathrm{mod}\ p^n-1)$, one has $k=s=i$, $t=i+1$. Then, the coefficient of the monomial with exponent $p^k+p^s+\frac{p^n-1}{2}-p^t$ is

$$3a_i^2c^2e_{i+1}+12aa_icc_ie_{i+1}+6a_ib_{i+1}c^2c_i+3a^2c_i^2e_{i+1}+6ab_{i+1}cc_i^2+6a_ib_{i+1}c^2c_i=0$$

since $c_i=0$ and $a_ie_j=0$, where subscripts are operated mod n. Also by $c_i=0$, the coefficient of the monomial with exponent $p^k+p^s+p^t+\frac{p^n-1}{2}-p^l-p^v$ is equal to 0.

If $\frac{p^n-1}{2} - p^k - p^s - p^t - p^l - p^v \equiv \frac{p^n-1}{2} - 5p^i \pmod{p^n-1}$, one has $k=s=t=l=v=i$. The coefficient of the monomial with such an exponent is equal to $b_i^2e_i^3(u^5+10u^3+5u)^{p^i}$ on the LHS of Equality (29), and it is zero on the RHS.

By the analysis above, the coefficients of $\frac{p^n-1}{2} - 5p^i$ on the both sides of Equality (29) satisfy the following equation

$$b_i^2e_i^3(u^5+10u^3+5u)^{p^i}=0.$$

A similar discussion for the exponent p^n-1-5p^i shows

$$b_i^2e_i^3(5u^4+10u^2+1)^{p^i}=0.$$

The two equalities imply $b_ie_i=0$ for any i.

Since $c_i=0$ and $b_ie_i=0$ for any i, Equalities (47) and (48) give

$$\begin{cases} b_i^2e_j^3((u^2+1)^{p^i}(u^3+3u)^{p^j}+2u^{p^i}(3u^2+1)^{p^j})=0; \\ b_i^2e_j^3((u^2+1)^{p^i}(3u^2+1)^{p^j}+2u^{p^i}(u^3+3u)^{p^j})=0, \end{cases}$$

which implies that $b_ie_j=0$ for any $0\le i\ne j\le n-1$.

Therefore, one has $b_ie_j=0$ for any i and j, i.e., $b_i=0$ for any i since $e_{j_0}\ne 0$.

By Equality (46), the equality $a_ie_{j_0}=0$ implies that $a_i=0$ for any $i\ne j_0$. Thus, Equality (3) is reduced to

$$a + a_{j_0}x^{p^{j_0}} = (c+\sum_{i=0}^{n-1} e_i f(x)^{p^i})^{\frac{p^n-1}{2}-1} \pmod{x^{p^n}-x}. \tag{50}$$

By similar analysis after Equality (39), Equality (50) is impossible.

2) In this case, Equality (29) is reduced to

$$\begin{aligned}(a+\sum_{i=0}^{n-1} a_ix^{p^i} + b_0f(x)+b_1f(x)^p)^2(c+c_0x+\sum_{i=0}^{n-1} e_if(x)^{p^i})^3 \\ = c+c_0x+\sum_{i=0}^{n-1} e_if(x)^{p^i} \pmod{x^{p^n}-x}.\end{aligned} \tag{51}$$

By Equality (46), there exists at most one nonzero element among a_0, a_1, a_2.

If $a_1=a_2=0$, the coefficient of x^5 satisfies $a_0^2c_0^3=0$ and then $a_0=0$ since $c_0\ne 0$. The coefficient of x^3 satisfies $a^2c_0^3=0$, and then $a=0$. The coefficient of x^{172} satisfies $2b_0^2c_0^3u=0$, which implies $b_0=0$. Thus, the coefficient of x satisfies $c_0=0$, and it contradicts with the fact $c_0\ne 0$.

If $a_1=0$ and $a_2\ne 0$, one also has $a_0=0$. By Equality (46), the equality $a_2e_j=0$ implies $e_0=e_1=0$. Considering the coefficient of x^{101}, one has $a_2^2c_0^3=0$. This contradicts with $a_2c_0\ne 0$.

If $a_1\ne 0$ and $a_2=0$, then one has $a_0=0$. By Equality (46), the equality $a_1e_j=0$ implies $e_0=e_2=0$. Considering the coefficient of x^{17}, one has $a_1^2c_0^3=0$. This contradicts with $a_1c_0\ne 0$.

5) In this case, Equality (29) can be rewritten as

$$\begin{aligned}(a+\sum_{i=0}^{n-1} a_ix^{p^i} + b_0f(x))^2(c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1} e_if(x)^{p^i})^3 \\ = c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1} e_if(x)^{p^i} \pmod{x^{p^n}-x}.\end{aligned} \tag{52}$$

Considering the coefficient of x^{17}, the coefficient on the LHS of Equality (52) is equal to $a_1^2c_0^3$ and it is zero on the RHS. Thus, one has $a_1^2c_0^3=0$ and then $a_1=0$ since $c_0\ne 0$. Similarly, the coefficient of x^{101} satisfies

$$a_2^2c_0^3+6a_0a_2c_0c_2^2+3a_0^2c_0c_2^2=((a_2c_0+3a_0c_2)^2+a_0^2c_2^2)c_0=0.$$

Since $c_0\neq 0$ and -1 is nonsquare, one has $a_2c_0+3a_0c_2=a_0c_2=0$, i.e., $a_0=a_2=0$ since $c_0c_2\neq 0$. Thus, Equality (52) can be reduced to

$$(a+b_0f(x))^2(c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^3=c+c_0x+c_2x^{p^2}+\sum_{i=0}^{n-1}e_if(x)^{p^i}\ (\mathrm{mod}\, x^{p^n}-x). \quad (53)$$

From the coefficient of x^3 in Equality (53), one has $a^2c_0^3=0$. Thus, $a=0$ and then $c=0$. The coefficient of x^{172} satisfies $2b_0^2c_0^3u=0$. This gives $b_0=0$ and then $a_i=b_i=0$ for any i. By similar arguments after Equality (31), one has $L_1(x,f(x))=c$. That's a contradiction.

8) In this case, Equality (29) is rewritten as

$$a+a_{j_0}x^{p^{j_0}}=(c+\sum_{i=0}^{n-1}c_ix^{p^i}+\sum_{i=0}^{n-1}e_if(x)^{p^i})^{\frac{p^n-1}{2}-1}\ (\mathrm{mod}\, x^{p^n}-x). \quad (54)$$

By similar analysis after Equality (39), Equality (54) is impossible.

From the arguments of Cases 1-8, $f(x)$ and $g(x)=x^{\frac{p^n-1}{2}-1}$ are CCZ-inequivalent on F_{7^3}.

This finally finishes the proof of Proposition 4. □

3. Conclusion

As far as the authors are aware, except the Ness-Helleseth family in [18], all known APN functions over finite fields of odd characteristic are listed in Table 1. Therefore, by Propositions 1-4, and Corollary 1 proven above, for $p\geq 7$ and odd n, the Ness-Helleseth functions are CCZ-inequivalent to all other known APN functions, and they are a new class of APN functions.

Acknowledgement

The authors would like to thank Professor Cunsheng Ding for his helpful comments and suggestions on this paper.

References

[1] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 65-76.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no.1, pp. 3-72, 1991.

[3] C. Carlet and C. Ding, "Highly nonlinear mappings," *Journal of Complexity*, vol. 20, no. 2-3, pp. 205-244, April/June 2004.

[4] C. Carlet, P. Charpin and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125-156, 1998.

[5] R. S. Coulter, R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Designs, Codes and Cryptography*, vol. 10, no. 2, pp. 167-184, Feb. 1997.

[6] C. Ding and J. Yuan, "A family of skew Hadamard difference sets," *Journal of Combinatorial Theory Series A*, vol. 113, no. 7, pp. 1526-1535, Oct. 2006.

[7] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): The Welch case," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271-1275, May 1999.

[8] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): A new case for n divisible 5," in *Proceedings of Finite Fields and Applications FQ5*, D. Jungnickel and H. Niederreiter, Eds. Augsburg, Germany: Springer-Verlag, 2000, pp. 113-121.

[9] H. Dobbertin, "Almost perfect nonlinear power functions over GF(2^n): The Niho case," *Inf. Comput.*, vol. 151, pp. 57-72, 1999.

[10] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, and W. Willems, "APN functions in odd characteristic," *Discr. Math.*, vol. 267, pp. 95-112, 2003.

[11] P. Dembowski, T. G. Ostrom, "Planes of order n with collineation groups of order n^2", *Mathematische Zeitschrift*, vol. 103, no. 3, pp. 239-258, June 1968.

[12] P. Felke, "Computing the uniformity of power mappings: a systematic approach with the multi-variate method over finite fields of odd characteristic," Ph. D. dissertation, University of Bochum, Bochum, Germany, 2005.

[13] R. Gold, "Maximal recursive sequence with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154-156, Jan. 1968.

[14] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 475-485, March 1999.

[15] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, pp. 363-370, 1997.

[16] H. Janwa and R. Wilson, "Hyperplane sections of fermat varieties in P^3 in Char. 2 and some applications to cyclic codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 673, pp. 180-194, 1993.

[17] T. Kasami, "The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes," *Inf. Contr.*, vol. 18, pp. 369-394, 1971.

[18] G. J. Ness and T. Helleseth, "A new family of ternary almost perfect nonlinear mappings," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2581-2586, July 2007.

[19] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1993, vol. 765, pp. 55-64.