New results on the -1 conjecture on cross-correlation of m-sequences based on complete permutation polynomials

Gaofei Wu [*], Keqin Feng [†], Nian Li [‡], and Tor Helleseth [§]

Abstract

The cross-correlation between two maximum length sequences (m-sequences) of the same period has been studied since the end of 1960s. One open conjecture by Helleseth states that the cross-correlation between any two p-ary m-sequences takes on the value -1 for at least one shift provided that the decimation d obeys $d \equiv 1 \pmod{p-1}$. This was known as the -1 Conjecture. Up to now, the -1 Conjecture was confirmed for the following decimations: (1) Niho-type decimations, i.e., $d = s(p^{\frac{n}{2}} - 1) + 1$, where s is an integer; (2) all the complete permutation polynomial (CPP) exponents d satisfying $d \equiv 1 \pmod{p-1}$, and (3) the additional families of decimations tabulated in this paper. In this paper, we first discuss the connection between the -1 conjecture on cross-correlation of m-sequences and CPP exponents, then we confirm the -1 conjecture for a new type of decimations by giving a new class of CPP exponents. The decimations are of the type $d = 1 + l(p^{rtm} - 1)/(r + 1)$ over $\mathbb{F}_{p^{rtm}}$, where p is a prime, $r + 1$ is an odd prime satisfying $p^{\frac{r}{2}} \equiv -1 \pmod{r+1}$, t is an odd integer ($t > 2$ if $p = 2$) with $\gcd(t, r) = 1$, and m is a positive integer. We transform the problem of determining whether d is a CPP exponent into investigating the existence of irreducible polynomials over $\mathbb{F}_p$ with degree t satisfying a congruence equation. By a theorem given by Rosen that considered the number of irreducible polynomials with a special congruence relation, we prove that d is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ for sufficiently large t. When m is odd, our new CPP exponents are of Niho type; thus, we give a new class of CPP exponents of Niho type. When m is even, we obtain a new class of CPP exponents which are not of Niho type. As a consequence, we show that the -1 conjecture is true for $d = 1 + l(p^{rtm} - 1)/(r + 1)$ when t is a sufficiently large integer.

Index Terms Cross-correlation, m-sequences, Permutation polynomials, Finite Fields, Irreducible polynomials.

[*]G. Wu is with the State Key Laboratory of Integrated Service Networks, School of Cyber Engineering, Xidian University, Xi'an, 710071, China, and also with the Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China. Email: wugf@nipc.org.cn.

[†]K. Feng is with the Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China. Email: fengkq@tsinghua.edu.cn.

[‡]N. Li is with the Hubei Key Laboratory of Applied Mathematics, School of Cyber Science and Technology, Hubei University, Wuhan 430062, China. Email: nian.li@hubu.edu.cn.

[§]T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway. Email: Tor.Helleseth@uib.no.

1 Introduction

Let p be a prime and $\{s(i)\}_{i=0}^{p^n-2}$ be a p-ary m-sequence of period p^n-1, where n is a positive integer. The d-decimated sequence of $\{s(i)\}$ given by $\{s(di)\}$ is also an m-sequence if $\gcd(d, p^n-1) = 1$. The cross-correlation function between $\{s(i)\}$ and its d-decimated sequence $\{s(di)\}$ is defined by

$$C_d(t) \;=\; \sum_{i=0}^{p^n-2} \xi^{s(i+t)-s(di)},$$

where $0 \le t < p^n - 1$, and $\xi = e^{\frac{2\pi i}{p}}$ is a complex primitive p-th root of unity. In [24], Helleseth proposed the following conjecture.

Conjecture 1 *([24, Conjecture 5.1]) Suppose p is a prime. Let $\gcd(d, p^n-1) = 1$. When $d \equiv 1 \pmod{p-1}$, then -1 is one of the values that $C_d(t)$ takes on.*

There is a natural connection between Conjecture 1 and complete permutation monomials. Let $\mathbb{F}_{p^n}$ be a finite field of p^n elements. We denote by $\mathbb{F}_{p^n}^*$ the multiplicative group of $\mathbb{F}_{p^n}$. A polynomial $f \in \mathbb{F}_{p^n}[x]$ is called a permutation polynomial (PP) if the associated polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_{p^n}$ to itself is a permutation of $\mathbb{F}_{p^n}$. A polynomial $f \in \mathbb{F}_{p^n}[x]$ is called a complete permutation polynomial (CPP) if both $f(x)$ and $f(x)+x$ are permutations of $\mathbb{F}_{p^n}$. It is an interesting and important problem to find permutation polynomials with good cryptographic properties such as high nonlinearity [5, 8, 21], low differential uniformity [6, 7, 22, 45], low c-differential uniformity [18, 23, 39], and low boomerang uniformity [34, 36, 40, 50].

Conjecture 1 can be connected to the CPP exponents which are defined as follows.

Definition 1 *For a positive integer d and $a \in \mathbb{F}_{p^n}^*$, a monomial function ax^d is a complete permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $\gcd(d, p^n-1) = 1$ and $ax^d + x$ is a permutation polynomial of $\mathbb{F}_{p^n}$. Such d is called a CPP exponent over $\mathbb{F}_{p^n}$.*

To the best of our knowledge, Conjecture 1 was confirmed for the following cases: (1) Niho-type decimations [42], i.e., $d = s(p^{\frac{n}{2}}-1)+1$, where s is an integer [12, 17, 25, 46]; (2) all the CPP exponents d satisfying $d \equiv 1 \pmod{p-1}$, and (3) all the exponents listed in Table 1. In Table 2, we summarize some known CPP exponents over $\mathbb{F}_{p^n}$. In 2008, Charpin and Kyureghyan [13] determined all the parameters $0 \le i \le n-1$ and $a \ne 0$ such that $x^{2^i+2} + ax$ are permutation polynomials of $\mathbb{F}_{2^n}$. In 2014, Tu, Zeng, and Hu [51] gave three classes of CPP exponents over $\mathbb{F}_{2^n}$. In [52], a class of CPP exponents over $\mathbb{F}_{2^n}$ of Niho type was given. Some classes of CPP exponents of the form $d = \frac{2^{tm}-1}{2^m-1}+1$ over $\mathbb{F}_{2^{tm}}$ were given in [54]. The CPP exponents of the form $\frac{q^n-1}{q-1}+1$ over $\mathbb{F}_{q^n}$ were studied in [2] for the cases $n = 2$ and $n = 3$, [55] for the case $n = 4$, [43] for the case $n = 5$, and [3] for the case $n = 6$. In 2016, Bartoli et al.

Table 1: Exponents d over $\mathbb{F}_{p^n}$ such that -1 occurs as a value of $C_d(t)$

p	n	d	$d \equiv 1 \pmod{p-1}$	Refs.
2	any integer	2^m+1 or $2^{2m}-2^m+1$ $n/\gcd(n,m)$ is odd	YES	[22, 29]
2	$n=2m$ with m odd	$2^{m+1}+3$[1] or $2^m+2^{\frac{m+1}{2}}+1$	YES	[14]
2	$n=2m+1$	2^m+3	YES	[11, 20]
2	n odd	$2^{2m}+2^m-1$, $n\|4m+1$	YES	[20]
3	$n=2m+1$	$2\cdot 3^m+1$	YES	[15]
3	n odd	3^m+2, $n\|4m-1$	YES	[15, 30]
odd prime	any integer	$(p^{2m}+1)/2$ or $p^{2m}-p^m+1$ $n/\gcd(n,m)$ is odd	YES	[24, 49]
3	$n=3m$	3^m+2 or $3^{2m}+2$	YES	[57, 59]
2 or 3	any integer	p^n-2	YES	[31, 32]
2	$n=4m$ with odd m	$2^{2m}+2^m+1$	YES	[16]
2	n odd	$(2^l+1)/(2^m+1)$, $(l,m)\in\{(2t,t),(5t,t),(5t,3t)\}$	YES	[28, 58]
odd prime	$4\|p^n-1$	$\frac{p^n-1}{2}+p^i$	YES for even n	[24]
2	$n=4m$ with even m	$2^{2m}-2^m+1$	YES	[26]
$p\equiv 2 \pmod 3$	n even	$\frac{p^n-1}{3}+p^i$ $\frac{p^n-1}{3}p^i \not\equiv 2 \pmod 3$	YES	[24]
prime	$n=4m$, $p^m\not\equiv 2 \bmod 3$	$p^{2m}-p^m+1$	YES	[27]

[1] $2^{m+1}+3$ is a CPP exponent over $\mathbb{F}_{2^{2m}}$ for odd m, see Table 2.

[4] classified complete permutation monomials of degree $d=\frac{q^n-1}{q-1}+1$ over $\mathbb{F}_{q^n}$, where q is odd, $n+1$ is a prime and $(n+1)^4<q$. In 2019, by using Dickson polynomials and the AGW criteria, Feng et al. [19] further studied the CPP exponents of the form $\frac{q^n-1}{q-1}+1$ and showed that [55, Conjecture 4.18] is false in general.

In this paper, we first show the relation between Conjecture 1 and CPP exponents, then we confirm Conjecture 1 for a new type of decimations by giving a new class of CPP exponents. More precisely, we consider a class of CPP exponents of the form $d=l\times\frac{p^{rtm}-1}{r+1}+1$, where $r+1$ is an odd prime satisfying $p^{\frac{r}{2}}\equiv -1 \pmod{r+1}$, t is an odd integer ($t>2$ if $p=2$) with $\gcd(t,r)=1$, and m is a positive integer. For odd m, we construct a new class of CPP exponents of Niho type. For even m, we construct a new class of CPP exponents which are not of Niho type. We systematically develop a method to transform the problem of determining whether d is a CPP exponent into investigating the existence of irreducible polynomials over $\mathbb{F}_p$ with degree t satisfying a congruence equation. Thanks to a theorem given by Rosen [47, Theorem 4.8], we show that d is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ for sufficiently large t. Our method is different from all the previous ones, and shows that proving the complete permutation property of a polynomial is usually difficult since determining the number of irreducible polynomials satisfying a congruence equation is usually hard.

Table 2: CPP exponents d over $\mathbb{F}_{p^n}$

p	n	d	$d \equiv 1 \pmod{p-1}$	Refs.
odd prime	any integer	$\frac{p^n+1}{2}$	YES for odd n; NO for even n	[41]
prime	$n = n_1 n_2 r$ $\mathrm{ord}_r(p)$[1]$= n_1$	$\frac{p^n-1}{r} + 1$	YES	[33]
prime	$n = 2m$	$s(p^m - 1) + 1$ $\gcd((s-1)(2s-1), p^m + 1) = 1$ $\gcd(s, p^m + 1) > 1$	YES	[52]
2	$n = 2m$, m odd	$2^m + 2$	YES	[2, 48]
3	$n = 2m$	$3^m + 2$	YES	[2, 55]
$p \equiv -1 \pmod 6$	$n = 2m$, m odd	$p^m + 2$	NO	[2]
2	$n = 3m$, $m > 1$	$2^{2m} + 2^m + 2$	YES	[2]
prime	$n = 2m$ $p^m \equiv 0, \pm 2 \pmod 5$	$2p^m + 3$	YES for $p = 2$; NO for odd prime	[51]
2	$n = rt$,$\gcd(r, t) = 1$ $r \in \{4, 6, 10\}$	$\frac{2^n-1}{2^t-1} + 1$	YES	[54]
odd prime	$n = (p-1)m$	$\frac{p^n-1}{p^m-1} + 1$	YES	[38, 55]
2	$n = 6m$ $\gcd(m, 3) = 1$	$2^{4m-1} + 2^{2m-1}$	YES	[38]
2	$n = 4m$	$(1 + 2^{2m-1})(1 + 2^{2m}) + 1$	YES	[38]
odd prime	$n = 4m$	$\frac{p^{4m}-1}{2} + p^{2m}$	YES	[38]
odd prime	$n = 4m$ $p^m \not\equiv 1 \pmod 5$	$\frac{p^{4m}-1}{p^m-1} + 1$	YES for $p = 3, 5$; NO for other p	[55]
odd prime	$n = 6m$ $p^m \not\equiv 1 \pmod 7$	$\frac{p^{6m}-1}{p^m-1} + 1$	YES for $p = 3, 7$; NO for other p	[3, 55]
odd prime	$n = 2m$	$(p^m - 1)\frac{p^i-1}{2} + p^i$ $1 \le i \le n$	YES	[55]
odd prime	$n = p - 1$	$t \cdot \frac{p^n-1}{p-1} + 1$ $1 \le t \le p - 2$	YES	[55]
2	$n = 2m$ $m > 2, m \not\equiv 2 \pmod 3$	$\frac{2^n-1}{3} + 1$	YES	[48]
prime	$n = rm$,$r + 1 \ne p$ $r + 1$ is prime $\gcd(r + 1, p^{2m} - 1) = 1$ $\mathrm{ord}_{r+1}(p^m) = r$	$\frac{p^{rm}-1}{p^m-1} + 1$	YES if $p - 1 \mid r$; NO for others	[19]
odd prime	$n = rm$, $r \mid p - 1$ $r > 1$	$\frac{p^{(p-1)m}-1}{p^m-1} + 1$	YES	[19]
odd prime	$n = rm$, $r \mid p^m - 1$ $r > 1$	$\frac{p^{(p^m-1)m}-1}{p^m-1} + 1$	YES	[19]
2	$n = 2m$ $m \ge 3$ is odd	$l \cdot \frac{2^n-1}{3} + 1$, $l = 1, 2$ $ml \not\equiv -1 \pmod 3$	YES	[35]

[1] We denote the order of p modulo r by $\mathrm{ord}_r(p)$.

The rest of this paper is organized as follows. In Section 2, we introduce some preliminaries and show the relation between Conjecture 1 and CPP exponents. In Section 3, we show that for sufficiently large t, $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$. Section 4 concludes our paper with some conjectures.

2 Preliminaries

In [37], a criterion for permutation polynomials is given by using the additive characters of the underlying finite field.

Lemma 1 *([37, Theorem 7.7]) A mapping $g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is a permutation polynomial if and only if for every $\alpha \in \mathbb{F}_{p^n}^*$,*

$$\sum_{x \in \mathbb{F}_{p^n}} \xi^{\mathrm{Tr}_1^n(\alpha g(x))} = 0,$$

where the trace function from $\mathbb{F}_{p^n}$ onto $\mathbb{F}_p$ is defined by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{p^i}$, $x \in \mathbb{F}_{p^n}$.

The following lemmas will also be needed in the sequel.

Lemma 2 *([37, Corollary 3.47]) An irreducible polynomial over $\mathbb{F}_q$ of degree n remains irreducible over $\mathbb{F}_{q^m}$ if and only if $\gcd(m, n) = 1$.*

Lemma 3 *([1, 44, 53, 56]) Let p be a prime. Let l, n and s be positive integers such that $s|p^n - 1$. Let $g(x) \in \mathbb{F}_{p^n}[x]$. Then $f(x) = x^l g(x^{\frac{p^n-1}{s}})$ is a PP over $\mathbb{F}_{p^n}$ if and only if $\gcd(l, \frac{p^n-1}{s}) = 1$ and $x^l g(x)^{\frac{p^n-1}{s}}$ is a permutation of μ_s, where μ_s is the set of s-th roots of unity in $\mathbb{F}_{p^n}$.*

In the following we recall a lemma which considers the number of monic irreducible polynomials satisfying a congruence equation. Let $l(x)$ and $u(x)$ be two polynomials in $\mathbb{F}_q[x]$, where $\gcd(l(x), u(x)) = 1$. Let $\Phi(u)$ be the Euler function in $\mathbb{F}_q[x]$, i.e., $\Phi(u)$ is the size of the multiplicative group $\left(\mathbb{F}_q[x]/u(x)\right)^\times$. Denote by $\pi(l, u, n)$ the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ which are congruent to $l(x)$ modulo $u(x)$, i.e.,

$$\pi(l, u, n) = \left|\left\{ f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x] : f(x) \text{ is irreducible}, \ f(x) \equiv l(x) (\mathrm{mod}\ u(x)) \right\}\right|,$$

where $|S|$ is the cardinality of a finite set S.

Lemma 4 *([47, Theorem 4.8]) Let $l(x)$ and $u(x)$ be two polynomials in $\mathbb{F}_q[x]$ and $\gcd(l(x), u(x)) = 1$. Then*

$$\pi(l, u, n) = \frac{1}{\Phi(u)} \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Now we show the connection between Conjecture 1 and CPP exponents. Let α be a primitive element of $\mathbb{F}_{p^n}$. The trace representation of a p-ary m-sequence $\{s(i)\}$ is $s(i) = \mathrm{Tr}_1^n(\alpha^i)$. Thus, the cross-correlation function between $\{s(i)\}$ and $\{s(di)\}$ can be expressed by

$$C_d(t) = \sum_{i=0}^{p^n-2} \xi^{\mathrm{Tr}_1^n(\alpha^{i+t}) - \mathrm{Tr}_1^n(\alpha^{di})} = \sum_{x \in \mathbb{F}_{p^n}} \xi^{\mathrm{Tr}_1^n(\gamma x + x^d)} - 1,$$

where $\gamma = -\alpha^t$.

Therefore, to prove Conjecture 1 is equivalent to prove that there exists $\gamma \in \mathbb{F}_{p^n}^*$ such that

$$\sum_{x \in \mathbb{F}_{p^n}} \xi^{\mathrm{Tr}_1^n(x^d + \gamma x)} = 0.$$

From Lemma 1, if d is a CPP exponent over $\mathbb{F}_{p^n}$, then there exists $\gamma \in \mathbb{F}_{p^n}^*$ such that for any $\alpha \in \mathbb{F}_{p^n}^*$, $\sum_{x \in \mathbb{F}_{p^n}} \xi^{\mathrm{Tr}_1^n(\alpha(x^d + \gamma x))} = 0$, which implies that Conjecture 1 is true for d. As a result, a sufficient condition for Conjecture 1 to be true is that d is a CPP exponent over $\mathbb{F}_{p^n}$. It can be easily seen that if $d \equiv 1 \pmod{p-1}$, then $d^{-1} \equiv 1 \pmod{p-1}$. It is known that if d is a CPP exponent over $\mathbb{F}_{p^n}$, so is d^{-1} [41, Theorem 2]. Thus we have the following lemma immediately.

Lemma 5 *Conjecture 1 is true for any CPP exponent $d \equiv 1 \pmod{p-1}$ over $\mathbb{F}_{p^n}$.*

3 A class of CPP exponents of the form $d = l \times \frac{p^n-1}{r+1} + 1$

In this section, we consider a class of CPP exponents of the form $d = l \times \frac{p^n-1}{r+1} + 1$. The following notations will be used throughout the rest of the paper.

- p is a prime.
- $r+1$ is an odd prime such that $\frac{r}{2}$ is the least positive integer satisfying $p^{\frac{r}{2}} \equiv -1 \pmod{r+1}$ (i.e., p is a primitive element of $\mathbb{F}_{r+1}$), and $p^r = k(r+1)+1$.
- t is an odd integer ($t > 2$ if $p = 2$) with $\gcd(t, r) = 1$.
- ω is a $(r+1)$-th primitive root in $\mathbb{F}_{p^r}$, i.e., $\omega \in \mathbb{F}_{p^r} \setminus \{1\}$ and $\omega^{r+1} = 1$.

Proposition 1 *Let m be an integer and $n = rtm$. Let $d = l \times \frac{p^n-1}{r+1} + 1$, where $1 \le l \le r$. For any $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$, suppose that $(a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i$ for some $0 \le i \le r$. Then $x^d + ax$ is a PP over $\mathbb{F}_{p^n}$ if and only if $\gcd(ilm+1, r+1) = 1$.*

Proof: Since $\gcd(r,t)=1$, then $\{t, 2t, 3t, \cdots, (r-1)t\} \pmod r = \{1, 2, 3, \cdots, r-1\}$, which implies

$$\{p^{jt} \pmod{p^r - 1} \,|\, 0 \le j \le r-1\} = \{p^j \,|\, 0 \le j \le r-1\}.$$

Thus,

$$\{p^{jt} \pmod{r+1} \,|\, 0 \le j \le r-1\} = \{p^j \pmod{r+1} \,|\, 0 \le j \le r-1\} = \{1, 2, \cdots, r\},$$

where the last equal sign holds due to p is a primitive element of $\mathbb{F}_{r+1}$. It follows that

$$\{\omega^{p^{jt}} \,|\, 0 \le j \le r-1\} = \{\omega^j \,|\, 1 \le j \le r\}.$$

From $(a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i$, we have $(a^{p^{jt}} + \omega^{p^{jt}})^{\frac{p^{rt}-1}{r+1}} = \omega^{i \cdot p^{jt}}$. Since $a \in \mathbb{F}_{p^t}$, we have $(a+\omega^{p^{jt}})^{\frac{p^{rt}-1}{r+1}} = \omega^{i \cdot p^{jt}}$. Let $\omega^{p^{jt}} = \omega^s$, then $(a+\omega^s)^{\frac{p^{rt}-1}{r+1}} = \omega^{is}$ for $1 \le s \le r$. Since $(a+1) \in \mathbb{F}_{p^t}$, one has

$$(a+\omega^0)^{\frac{p^{rt}-1}{r+1}} = (a+1)^{(p^t-1)\frac{1+p^t+\cdots+p^{(r-1)t}}{r+1}} = 1 = \omega^0,$$

where the second equal sign holds due to

$$1 + p^t + \cdots + p^{(r-1)t} \equiv 1 + 2 + \cdots + r \pmod{r+1} \equiv (1+r) \cdot \frac{r}{2} (\mathrm{mod}\ r+1) \equiv 0 \pmod{r+1}.$$

Thus, $(a+\omega^s)^{\frac{p^{rt}-1}{r+1}} = \omega^{is}$ for $0 \le s \le r$. Replacing s with ls, we have $(a+\omega^{ls})^{\frac{p^{rt}-1}{r+1}} = \omega^{ils}$. As a consequence,

$$(a+\omega^{ls})^{\frac{p^n-1}{r+1}} = (a+\omega^{ls})^{\frac{p^{rt}-1}{r+1} \cdot \frac{p^n-1}{p^{rt}-1}} = \omega^{ils \cdot \frac{p^n-1}{p^{rt}-1}} = \omega^{ilsm},$$

where the last equal sign holds due to $\omega \in \mathbb{F}_{p^r}$.

From Lemma 3, to prove that $x^d + ax$ is a PP over $\mathbb{F}_{p^n}$ is equivalent to prove that $x(a+x^l)^{\frac{p^n-1}{r+1}}$ is a permutation of $\mu_{r+1} = \{x \,|\, x^{r+1} = 1,\, x \in \mathbb{F}_{p^n}\} = \{\omega^j \,|\, 0 \le j \le r\}$.

From $(a+\omega^{ls})^{\frac{p^n-1}{r+1}} = \omega^{ilsm}$, we have $\omega^s(a+\omega^{ls})^{\frac{p^n-1}{r+1}} = \omega^{ilsm+s} = \omega^{(ilm+1)s}$. Then $\{\omega^{(ilm+1)s} \,|\, 0 \le s \le r\}$ is a permutation of μ_{r+1} if and only if $\gcd(ilm+1, r+1) = 1$. This completes the proof. $\square$

Lemma 6 *Let $p^r = k(r+1)+1$. Then*

(1) $\frac{p^{rt}-1}{r+1} \equiv kt \pmod{r+1}$,

(2) $(p^t - 1) | \frac{p^{rt}-1}{r+1}$.

Proof: (1)

$$\begin{aligned}
\frac{p^{rt}-1}{r+1} &= \frac{1}{r+1}\left[\left(k(r+1)+1\right)^t - 1\right] \\
&= \frac{1}{r+1}\left[k^t (r+1)^t + \binom{t}{1} k^{t-1} (r+1)^{t-1} + \cdots + \binom{t}{t-1} k (r+1) + 1 - 1\right] \\
&= k^t (r+1)^{t-1} + t k^{t-1} (r+2)^{t-2} + \cdots + kt \\
&\equiv kt \pmod{r+1}.
\end{aligned}$$

(2) Note that $\gcd(t, r) = 1$, which implies t is odd due to r is even. Thus,

$$\gcd(p^{\frac{r}{2}}+1, p^t-1) = \begin{cases} 1, & \text{if } p = 2, \\ 2, & \text{if } p \text{ is an odd prime.} \end{cases}$$

Remember that $p^{\frac{r}{2}} \equiv -1 \pmod{r+1}$, we have $r+1 | (p^{\frac{r}{2}}+1)$. By $(p^{\frac{r}{2}}+1) | (p^{rt}-1)$ and $(p^t-1) | (p^{rt}-1)$, we have $(p^t-1)(p^{\frac{r}{2}}+1) \mid p^{rt}-1$ if $p = 2$, and $(p^t-1)\frac{p^{\frac{r}{2}}+1}{2} \mid p^{rt}-1$ if p is an odd prime. As a consequence, $(p^t-1)\frac{(p^{\frac{r}{2}}+1)}{r+1} \mid \frac{p^{rt}-1}{r+1}$ if $p = 2$, and $(p^t-1)\frac{(p^{\frac{r}{2}}+1)}{2(r+1)} \mid \frac{p^{rt}-1}{r+1}$ if p is an odd prime, which implies $p^t - 1 \mid \frac{p^{rt}-1}{r+1}$. This completes the proof. □

Lemma 7 *Let* $d = l \times \frac{p^{rtm}-1}{r+1} + 1$. *Then* $\gcd(d, p^{rtm}-1) = 1$ *if and only if* $\gcd(ktml+1, r+1) = 1$.

Proof: Recall that $p^r = k(r+1) + 1$. By Lemma 6, we have $l \times \frac{p^{rtm}-1}{r+1} \equiv ktlm \pmod{r+1}$, then $\gcd(l \times \frac{p^{rtm}-1}{r+1} + 1, r+1) = 1$ if and only if $\gcd(ktml+1, r+1) = 1$. Together with $\gcd(l \times \frac{p^{rtm}-1}{r+1} + 1, \frac{p^{rtm}-1}{r+1}) = 1$, we have $\gcd(l \times \frac{p^{rtm}-1}{r+1} + 1, p^{rtm}-1) = 1$ if and only if $\gcd(ktml+1, r+1) = 1$. □

Corollary 1 *Let* $n = rtm$, *where* $r+1 | m$. *Let* $d = l \times \frac{p^n-1}{r+1} + 1$, *where* $1 \le l \le r$. *Then* d *is a CPP exponent over* $\mathbb{F}_{p^n}$.

Proof: We have that $\gcd(ktml+1, r+1) = 1$. Thus, by Lemma 7, $\gcd(l \times \frac{p^{rtm}-1}{r+1} + 1, p^{rtm}-1) = 1$. On the other hand, we have $\gcd(ilm+1, r+1) = 1$ for any i and l. By Proposition 1, for each $a \in \mathbb{F}_{p^t}^*$ and $a \neq -1$, $x^d + ax$ is a PP over $\mathbb{F}_{p^n}$. Then the conclusion follows. □

Corollary 2 *Let* $n = rtm$, *where* $r+1 \nmid m$. *For each* $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$, *there exists an* $1 \le l \le r$, *such that* $x^d + ax$ *is a PP over* $\mathbb{F}_{p^n}$, *where* $d = l \times \frac{p^n-1}{r+1} + 1$.

Proof: Recall that for each $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$, we have $(a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i$ for some $0 \le i \le r$. Suppose that for some $1 \le l' \le r$ such that $\gcd(il'm+1, r+1) = r+1$, then $r+1 | (il'm+1)$, which implies $i \neq 0$.

Since $r+1 \nmid m$, we have $\gcd(i(l'+1)m+1, r+1) = 1$. Then the conclusion follows from Proposition 1. $\square$

In the following, we will concentrate on the case $\gcd(r+1, m) = 1$. Let

$$C_i = \{a \in \mathbb{F}_{p^t}^* \backslash \{-1\} : (a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i\},$$

and $N_i = |C_i|$ be the number of elements in C_i.

Proposition 2 *Let $n = rtm$ with $\gcd(r+1, m) = 1$. Let $d = l \times \frac{p^n-1}{r+1} + 1$, where $1 \le l \le r$. Then d is a CPP exponent over $\mathbb{F}_{p^n}$ if both of the following conditions are satisfied:*

(1) $\gcd(ktml + 1, r+1) = 1$;

(2) $|C_{-(lm)^{-1}}| < p^t - 2$.

Proof: If $\gcd(ktml+1, r+1) = 1$, then $\gcd(l \times \frac{p^{rtm}-1}{r+1} + 1, p^{rtm} - 1) = 1$ by Lemma 7. Since $\gcd(r+1, m) = 1$, $\gcd(ilm+1, r+1) = r+1$ has a unique solution $i \equiv -(lm)^{-1} \pmod{r+1}$. By Proposition 1, for $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$, $x^d + ax$ is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $a \notin C_{-(lm)^{-1}}$. Thus, if $|C_{-(lm)^{-1}}| < p^t - 2$, then there exists $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$ such that $x^d + ax$ is a permutation polynomial of $\mathbb{F}_{p^n}$. This completes the proof. $\square$

Remark 1 *By Lemma 6, we have $p^t - 1 | \frac{p^{rt}-1}{r+1}$, thus $p - 1 | \frac{p^n-1}{r+1}$, which implies that $d = l \times \frac{p^n-1}{r+1} + 1 \equiv 1 \pmod{p-1}$. As a consequence, if d satisfies the conditions in Proposition 2, then Conjecture 1 is true for d.*

The following theorem is our main result.

Theorem 1 *Suppose $\gcd(m, r+1) = 1$. There exists a constant T such that for each $t \ge T$, $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ if $\gcd(ktml+1, r+1) = 1$.*

To prove Theorem 1, according to Proposition 2, we need to show that $|C_{-(lm)^{-1}}| < p^t - 2$ for $t \ge T$. Recall that $p^r = k(r+1)+1$. We will first show in Lemma 9 that if $ktml \not\equiv -2 \pmod{r+1}$, then $|C_{-(lm)^{-1}}| < p^t - 2$. Then we prove that if $ktml \equiv -2 \pmod{r+1}$, then $|C_{-(lm)^{-1}}| < p^t - 2$ for $t \ge T$ in Lemmas 10-12.

Lemma 8 *Recall that $C_i = \{a \in \mathbb{F}_{p^t}^* \backslash \{-1\} : (a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i\}$. Then $|C_i| = |C_{kt-i}|$, where k is an integer such that $p^r = k(r+1)+1$.*

Proof: If $a \in C_i$, then $(a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i$. Consider

$$(a^{-1}+\omega^{-1})^{\frac{p^{rt}-1}{r+1}} = \big(\frac{a+\omega}{a\omega}\big)^{\frac{p^{rt}-1}{r+1}} = \frac{\omega^i}{(a\omega)^{\frac{p^{rt}-1}{r+1}}}.$$

By Lemma 6, we have $a^{\frac{p^{rt}-1}{r+1}} = 1$ and $\omega^{\frac{p^{rt}-1}{r+1}} = \omega^{kt}$. Therefore from the above equation, we get

$$(a^{-1}+\omega^{-1})^{\frac{p^{rt}-1}{r+1}} = \omega^{i-kt}.$$

Taking the $p^{\frac{r}{2}}$-th power on both sides of the above equation, we have

$$(a^{-p^{\frac{r}{2}}}+\omega^{-p^{\frac{r}{2}}})^{\frac{p^{rt}-1}{r+1}} = \omega^{(i-kt)p^{\frac{r}{2}}}.$$

Remember that $\omega^{p^{\frac{r}{2}}} = \omega^{-1}$, thus we have

$$(a^{-p^{\frac{r}{2}}}+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^{kt-i},$$

thus, $a^{-p^{\frac{r}{2}}} \in C_{kt-i}$.

Since $f(x) = x^{-p^{\frac{r}{2}}}$ is a permutation of $\mathbb{F}_{p^t}^* \backslash \{-1\}$, thus for $a_1 \in C_i$ and $a_2 \in C_i$ with $a_1 \neq a_2$, we have

$$a_1^{-p^{\frac{r}{2}}} \in C_{kt-i},\ a_2^{-p^{\frac{r}{2}}} \in C_{kt-i}, \text{ and } a_1^{-p^{\frac{r}{2}}} \neq a_2^{-p^{\frac{r}{2}}}.$$

This completes the proof. □

Lemma 9 *Let* $\gcd(r+1,m)=1$. *Suppose that* $p^r = k(r+1)+1$. *Then* $|C_{-(lm)^{-1}}| < p^t-2$ *if one of the following conditions is satisfied:*

(1) $\gcd(kt, r+1) = r+1$,

(2) $\gcd(kt, r+1) = 1,\ -(lm)^{-1} \not\equiv kt + (lm)^{-1} \pmod{r+1}$ *(or* $ktml \not\equiv -2 \pmod{r+1}$*).*

Proof: (1) Suppose $\gcd(r+1, kt) = r+1$, i.e. $r+1|kt$. From Lemma 8, we have

$$|C_i| = |C_{kt-i}| = |C_{r+1-i}|,$$

then $|C_{-(lm)^{-1}}| = |C_{r+1-(lm)^{-1}}| = |C_{(lm)^{-1}}| < p^t-2$ due to $C_{r+1-(lm)^{-1}} \bigcap C_{(lm)^{-1}} = \emptyset$.

(2) Suppose $\gcd(r+1, kt) = 1$ and $ktml \not\equiv r-1 \pmod{r+1}$. Then $ktml \not\equiv -2 \pmod{r+1}$, which implies

$$-(lm)^{-1} \not\equiv kt + (lm)^{-1} \pmod{r+1}.$$

Thus the result follows from $|C_{-(lm)^{-1}}| = |C_{kt+(lm)^{-1}}|$ and $C_{-(lm)^{-1}} \bigcap C_{kt+(lm)^{-1}} = \emptyset$. □

By Proposition 2 and Lemma 9, we have

Proposition 3 *Suppose that* $ktml \not\equiv -2 \pmod{r+1}$ *and* $ktml \not\equiv -1 \pmod{r+1}$. *Then* $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ *is a CPP exponent over* $\mathbb{F}_{p^{rtm}}$.

Proof: Suppose that $\gcd(m, r+1) = 1$. By Lemma 9, if $ktml \not\equiv -2 \pmod{r+1}$, then $|C_{-(lm)^{-1}}| < p^t - 2$. Together with $ktml \not\equiv -1 \pmod{r+1}$, both conditions in Proposition 2 are satisfied, thus $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$.

Suppose that $\gcd(r+1, m) = r+1$. Corollary 1 shows that $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$. This completes the proof. □

Now let us consider the case $ktml \equiv -2 \pmod{r+1}$. The following lemma which considers the number of monic irreducible polynomials satisfying a congruence equation will be used in the sequel.

Lemma 10 *There exists a constant* T *such that for each odd prime* $t \geq T$, *there are some monic irreducible polynomials* $f(z)$ *over* $\mathbb{F}_p$ *with degree* t *such that* $f(z) \not\equiv z^{2^{-1}t} h(z) \pmod{z^{r+1}-1}$ *for any* $h(z)$ *satisfying* $h^k(z) \equiv 1 \pmod{z^{r+1}-1}$.

Proof: see Appendix A. □

Using Lemma 6 and Lemma 10, we have the following lemma.

Lemma 11 *There exists a constant* T *such that for each odd prime* $t \geq T$, $|C_{-(lm)^{-1}}| < p^t - 2$ *if* $\gcd(t, r) = 1$ *and* $ktlm \equiv -2 \pmod{r+1}$.

Proof: see Appendix B. □

Lemma 12 *Suppose that* $t' = ts$, *where* s *is a positive integer. If* $|C_{-(lm)^{-1}}| < p^t - 2$, *then* $|C'_{-(lm)^{-1}}| < p^{t'} - 2$, *where*

$$C'_{-(lm)^{-1}} = \{a \in \mathbb{F}^*_{p^{t'}} \backslash \{-1\} | (a+\omega)^{\frac{p^{rt'}-1}{r+1}} = \omega^{-(lm)^{-1}}\}$$

and

$$C_{-(lm)^{-1}} = \{a \in \mathbb{F}^*_{p^t} \backslash \{-1\} | (a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^{-(lm)^{-1}}\}.$$

Proof: See Appendix C. □

Proof of Theorem 1: Let $\gcd(r+1, m) = 1$ and $t \geq T$ be an odd integer, where T is a fixed positive integer for each r. By Proposition 2, to complete the proof of Theorem 1, it is enough to show that for $t \geq T$, $|C_{-(lm)^{-1}}| < p^t - 2$. If $ktml \not\equiv -2 \pmod{r+1}$, by Lemma 9, $|C_{-(lm)^{-1}}| < p^t - 2$. For the case $ktml \equiv -2 \pmod{r+1}$, Lemma 11 and Lemma 12 show that $|C_{-(lm)^{-1}}| < p^t - 2$ for $t \geq T$. □

In the following we consider a special case $r=2$ of Theorem 1, i.e., $r=2$ and $p \equiv -1 \pmod 3$. We will show that if $r=2$, then for any integer m and odd integer t ($t \geq 3$ if $p=2$), $d = \frac{p^{2tm}-1}{3}+1$ is a CPP exponent over $\mathbb{F}_{p^{2tm}}$ if and only if $p^{tm} \equiv \pm 1, \pm 2 \pmod 9$; $d = 2 \cdot \frac{p^{2tm}-1}{3}+1$ is a CPP exponent over $\mathbb{F}_{p^{2tm}}$ if and only if $p^{tm} \equiv \pm 1, \pm 4 \pmod 9$.

Lemma 13 *Let p be a prime such that $p \equiv -1 \pmod 3$. Let t be an odd integer ($t > 1$ if $p = 2$) and $r = 2$. Then for each $1 \leq i \leq 2$, $|C_i| > 0$.*

Proof: Recall that $\omega \in \mathbb{F}_{p^r} \backslash \{1\}$ and $\omega^{r+1} = 1$. Let $r=2$ and $p \equiv -1 \pmod 3$. Since t is odd, then every element $u \in \mathbb{F}_{p^{2t}}$ can be represented uniquely as $u = u_0 + u_1\omega$, where $u_i \in \mathbb{F}_{p^t}$.

For any $0 \leq i \leq 2$, there are $\frac{p^{2t}-1}{3}$ elements $u_0 + u_1\omega \in \mathbb{F}_{p^{2t}}$ such that $(u_0+u_1\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$.

Case 1: let $p > 5$, or $p = 5, t \geq 3$, or $p = 2, t \geq 5$. If $(-1+\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$, then we have

$$(-1 \times u_0 + u_0\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$$

for any $u_0 \in \mathbb{F}_{p^t}^*$ due to $u_0^{\frac{p^{2t}-1}{3}} = 1$. Similarly, if $(0+\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$, then we have

$$(0 + u_0\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$$

for any $u_0 \in \mathbb{F}_{p^t}^*$. Suppose that $p > 5$, or $p = 5, t \geq 3$, or $p = 2, t \geq 5$. Then $3(p^t-1) < \frac{p^{2t}-1}{3}$. This means that for any $0 \leq i \leq 2$, there exist elements $u_0+u_1\omega \in \mathbb{F}_{p^{2t}}^* \setminus \{0+u_0\omega, -u_0+u_0\omega, u_0+0\times\omega : u_0 \in \mathbb{F}_{p^t}^*\}$ such that $(u_0+u_1\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$, i.e., $(u_1^{-1}u_0+\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$, where $u_1^{-1}u_0 \neq 0, -1$. Thus, $|C_i| > 0$ for $0 \leq i \leq 2$.

Case 2: let $t = 1$ and $p = 5$. Note that $(0+\omega)^{\frac{5^2-1}{3}} = \omega^8 = \omega^2$, $(-1+\omega)^{\frac{5^2-1}{3}} = (-1+\omega)^8 = \omega$, and $u_0^{\frac{5^2-1}{3}} = 1$. Since $p-1 < \frac{p^2-1}{3}$, then there exists an element $a \in \mathbb{F}_{p^t}^* \setminus \{-1\}$ such that $(a+\omega)^{\frac{p^{2t}-1}{3}} = \omega^i$, where $0 \leq i \leq 2$, i.e., $|C_i| > 0$ for $0 \leq i \leq 2$.

Case 3: let $t = 3$ and $p = 2$. It can be checked that $C_1 = \{\alpha, \alpha^2, \alpha^4\}$ and $C_2 = \{\alpha^3, \alpha^5, \alpha^6\}$, where α is a primitive element of $\mathbb{F}_{2^3}$. $\square$

By Lemma 13 and Proposition 1, we have the following corollaries.

Corollary 3 *Let p be a prime such that $p \equiv -1 \pmod 3$. Let $n = 2tm$, where m is an integer, and t is an odd integer with $t \geq 3$ if $p = 2$. Let $d = l \times \frac{p^n-1}{3}+1$. Then there exists $a \in \mathbb{F}_{p^t}^*$ such that $x^d + ax$ is a PP over $\mathbb{F}_{p^n}$. Thus, $d = l \times \frac{p^n-1}{3}+1$ is a CPP exponent over $\mathbb{F}_{p^n}$ if $ktml \not\equiv -1 \pmod 3$.*

Corollary 4 *Let p be an odd prime such that $p \equiv -1 \pmod 3$. Let $n = 2m$, where m can be any integer. Then $l \times \frac{p^n-1}{3} + 1$ is a CPP exponent over $\mathbb{F}_{p^{2m}}$ if $p^m \equiv \pm 1 \pmod 9$. Moreover, $\frac{p^{2m}-1}{3} + 1$ is a CPP exponent over $\mathbb{F}_{p^{2m}}$ if and only if $p^m \equiv \pm 1, \pm 2 \pmod 9$, and $2 \times \frac{p^{2m}-1}{3} + 1$ is a CPP exponent over $\mathbb{F}_{p^{2m}}$ if and only if $p^m \equiv \pm 1, \pm 4 \pmod 9$.*

Proof: Since $p \equiv -1 \pmod 3$, we get $\gcd(\frac{p^{2m}-1}{3} + 1, p^{2m} - 1) = 1$ if and only if $p^m \equiv \pm 1, \pm 2 \pmod 9$, and $\gcd(2 \cdot \frac{p^{2m}-1}{3} + 1, p^{2m} - 1) = 1$ if and only if $p^m \equiv \pm 1, \pm 4 \pmod 9$. In the following we show that $x^{l \times \frac{p^n-1}{3} + 1} + ax$ is a PP over $\mathbb{F}_{p^n}$ for $a = \frac{p+1}{2}$.

Let $a = \frac{p+1}{2}$. By Lemma 3, $x^{l \times \frac{p^n-1}{3} + 1} + ax$ is a PP over $\mathbb{F}_{p^n}$ if and only if $x(x^l + a)^{\frac{p^n-1}{3}}$ permutes $\{1, \omega, \omega^2\}$. Since $p \equiv -1 \pmod 3$, we have

$$\begin{aligned}(a+\omega)^{\frac{p^2-1}{3}} &= (a+\omega)^{(p-1)\frac{p+1}{3}} = (\frac{a+\omega^p}{a+\omega})^{\frac{p+1}{3}} = (\frac{a+\omega^2}{a+\omega})^{\frac{p+1}{3}} = (\frac{a-1-\omega}{a+\omega})^{\frac{p+1}{3}} \\ &= (\frac{(p-1)/2-\omega}{-((p-1)/2-\omega)})^{\frac{p+1}{3}} = 1,\end{aligned}$$

where the last equal sign holds due to $\frac{p+1}{3}$ is even. Similarly, it can be shown that $(a+\omega^2)^{\frac{p^2-1}{3}} = 1$ and $(a+1)^{\frac{p^2-1}{3}} = 1$. Thus,

$$(a+\omega)^{\frac{p^n-1}{3}} = ((a+\omega)^{\frac{p^2-1}{3}})^{\frac{p^n-1}{p^2-1}} = 1,$$

$(a+\omega^2)^{\frac{p^n-1}{3}} = 1$, and $(a+1)^{\frac{p^n-1}{3}} = 1$.

Therefore, for $l = 1, 2$, $(x^l + a)^{\frac{p^n-1}{3}} = 1$ if $x \in \{1, \omega, \omega^2\}$, as a consequence, $x(x^l + a)^{\frac{p^n-1}{3}}$ permutes $\{1, \omega, \omega^2\}$. Thus, $x^{l \times \frac{p^n-1}{3} + 1} + \frac{p+1}{2}x$ is a PP over $\mathbb{F}_{p^n}$ for any odd prime $p \equiv -1 \pmod 3$ and even n. $\square$

Remark 2 *Corollary 4 gives a new class of CPP exponents, and the following CPP exponents over $\mathbb{F}_{p^n}$ are some examples of Corollary 4, which can be explained for the first time:*

(1) $p = 11, n = 4$, $d = 2 \times \frac{11^4-1}{3} + 1 = 9761$*;*

(2) $p = 5, n = 4$, $d = 1 \times \frac{5^4-1}{3} + 1 = 209$*; and*

(3) $p = 11, n = 2$, $d = 1 \times \frac{11^2-1}{3} + 1 = 41$.

By Corollary 1 and Theorem 1, the following theorem can be obtained immediately.

Theorem 2 *There exists a constant T such that for each $t \geq T$, $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ if $ktml \not\equiv -1 \pmod{r+1}$.*

Theorem 2 shows that if $ktml \not\equiv -1 \pmod{r+1}$, then Conjecture 1 is true for $d = l \times \frac{p^{rtm}-1}{r+1} + 1$, where $t \geq T$.

Let m be odd in Theorem 2. Then $p^{\frac{r}{2}tm} \equiv -1 \,(\bmod\, r+1)$ by $p^{\frac{r}{2}} \equiv -1 \,(\bmod\, r+1)$. Therefore, $d = l \times \frac{p^{rtm}-1}{r+1} + 1 = l \times \frac{p^{\frac{r}{2}tm}+1}{r+1}(p^{\frac{r}{2}tm} - 1) + 1$ is an Niho-type exponent. It was shown in [52] that if $\gcd(l \cdot \frac{p^{\frac{r}{2}tm}+1}{r+1} - 1, p^{\frac{r}{2}tm} + 1) = 1$, then d is a CPP exponent over $\mathbb{F}_{p^n}$. Thus, Theorem 2 gives a new class of CPP exponents of Niho type if $\gcd(l \cdot \frac{p^{\frac{r}{2}tm}+1}{r+1} - 1, p^{\frac{r}{2}tm} + 1) \neq 1$. Similar as in Lemma 6, let $p^{\frac{r}{2}} = k'(r+1) - 1$, it can be shown that $\gcd(l \cdot \frac{p^{\frac{r}{2}tm}+1}{r+1} - 1, p^{\frac{r}{2}tm} + 1) \neq 1$ if and only if $\gcd(k'tml - 1, r+1) = r+1$. From $p^r = 1 + k(r+1) = (k'(r+1)-1)^2 = (p^{\frac{r}{2}})^2$, we have $k = \frac{(k'(r+1)-1)^2-1}{r+1} = k'^2(r+1) - 2k'$. By $ktml = (k'^2(r+1) - 2k')tml \equiv -2k'tml \pmod{r+1}$, it can be shown that $\gcd(k'tml - 1, r+1) = r+1$ if and only if $ktml \equiv -2 \pmod{r+1}$. As a result, if m is odd, Theorem 2 gives a new class of CPP exponents of Niho type if $ktml \equiv -2 \pmod{r+1}$.

Let m be even in Theorem 2, then $p^{\frac{r}{2}tm} \equiv 1 \,(\bmod\, r+1)$. Therefore, $d = l \times \frac{p^{rtm}-1}{r+1} + 1 = l \times \frac{p^{\frac{r}{2}tm}-1}{r+1}(p^{\frac{r}{2}tm} + 1) + 1$ is not of Niho-type. As a result, Theorem 2 gives a new class of CPP exponents which are not of Niho type, and thus confirms Conjecture 1 for a new class of decimations.

Example 1 *Let $p = 5, r = 2$, and $t = 1$. Then $d = l \times \frac{5^{2m}-1}{3} + 1$. From $p^r = (r+1) \times k + 1$, one gets $k = 8$. If m is odd and $ktml = 8ml \equiv -2 \pmod 3$, i.e., $ml \equiv -1 \pmod 3$, then $d = l \times \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent of Niho type. Thus, we get $d_1 = \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent of Niho type if $m \equiv 5 \pmod 6$, and $d_2 = 2 \times \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent of Niho type if $m \equiv 1 \pmod 6$.*

If m is even and $ktml = 8ml \not\equiv -1 \pmod 3$, i.e., $ml \not\equiv 1 \pmod 3$, then $d = l \times \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent which is not of Niho type. Thus, we get $d_1 = \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent which is not of Niho type if $m \equiv 0, 2 \pmod 6$, and $d_2 = 2 \times \frac{5^{2m}-1}{3} + 1$ is a new CPP exponent which is not of Niho type if $m \equiv 0, 4 \pmod 6$.

Example 2 *Let $p = 3$ and $r = 4$. Then $d = l \times \frac{3^{4tm}-1}{5} + 1$. From $p^r = (r+1) \times k + 1$, one gets $k = 16$. Let m be even and $t = 1$. By Proposition 3, if $ktml = 16ml \not\equiv -1 \pmod 5$ and $ktml = 16ml \not\equiv -2 \pmod 5$, i.e., $ml \not\equiv -1 \pmod 5$ and $ml \not\equiv -2 \pmod 5$, then $d = l \times \frac{3^{4m}-1}{5} + 1$ is a new CPP exponent which is not of Niho type. Thus, $d_1 = \frac{3^{4m}-1}{5} + 1$ is a new CPP exponent if $m \equiv 2, 6 \pmod{10}$[1], $d_2 = 2 \cdot \frac{3^{4m}-1}{5} + 1$ is a new CPP exponent if $m \equiv 6, 8 \pmod{10}$, $d_3 = 3 \cdot \frac{3^{4m}-1}{5} + 1$ is a new CPP*

[1]Let $m = 2$, then the CPP exponent $d_1 = \frac{3^8-1}{5} + 1 = 1313$ over $\mathbb{F}_{3^8}$ can now be explained for the first time.

exponent if $m \equiv 2, 4 \pmod{10}$[2], *and* $d_4 = 4 \cdot \frac{3^{4m}-1}{5} + 1$ *is a new CPP exponent if* $m \equiv 4, 8 \pmod{10}$.

Let m *be odd and* $ktml = 16tml \equiv -2 \pmod 5$, *i.e.,* $tml \equiv -2 \pmod 5$, *where* $t \geq 3$ *is an odd integer. Then* $d = l \times \frac{3^{4tm}-1}{5} + 1$ *is a new CPP exponent of Niho type.*

4 Conclusion

In this paper, we confirmed Conjecture 1 for a new class of decimations by constructing a new class of CPP exponents d with $d \equiv 1 (\bmod\, p-1)$. We summarized some known results on CPP exponents over finite fields, and discussed the connection between Conjecture 1 and CPP exponents. Suppose that $r+1$ is an odd prime such that $p^{\frac{r}{2}} \equiv -1 \,(\bmod\, r+1)$ and t is an integer such that $\gcd(r, t) = 1$. We analyzed a class of exponents of the form $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ and proved that d is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ for sufficiently large t. Since $d \equiv 1(\bmod\, p-1)$, we confirm Conjecture 1 for a new class of decimations. Note that Carlitz and Wells [9, 10] proved that $x^{\frac{q-1}{m}+1} + ax$ is a PP of $\mathbb{F}_q$ for any $m|q-1$ and sufficiently large q. However, the method we used to show the CPP property of $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is quite different from all the previous ones. Specially, we transferred the problem of determining whether d is a CPP exponent into investigating the existence of irreducible polynomials satisfying a congruence equation, which may be of independent interest. Moreover, in Proposition 3, for the case $ktml \not\equiv -2 \,(\bmod\, r+1)$, we proved that $d = l \times \frac{p^{rtm}-1}{r+1} + 1$ is a CPP exponent over $\mathbb{F}_{p^{rtm}}$ without the condition t is sufficiently large. At the end of this paper, we propose a conjecture based on computer experiments. Recall that $C_i = \{a \in \mathbb{F}_{p^t}^* \backslash \{-1\} : (a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^i\}$. In Tables 3 and 4, we lists the number of elements in C_i for some p and r. Computer experiments indicate the following conjecture.

Conjecture 2 *Let* t *be an odd prime such that* $\gcd(t, r) = 1$ *and* $ktlm \equiv -2 \pmod{r+1}$. *Then* $|C_{-(lm)^{-1}}| < p^t - 2$.

According to Lemma 9 and Lemma 12, if the above conjecture is true, then $|C_{-(lm)^{-1}}| < p^t - 2$ for all $t \neq 1$ such that $\gcd(t, r) = 1$. By the proof of Lemma 11, Conjecture 2 is equivalent to the following conjecture.

Conjecture 3 *Let* t *be an odd prime such that* $\gcd(t, r) = 1$ *and* $ktlm \equiv -2 \pmod{r+1}$. *Then for any* $h(z)$ *such that* $h^k(z) \equiv 1 \pmod{z^{r+1}-1}$, *there exists irreducible polynomials* $f(z)$ *over* $\mathbb{F}_p$ *with degree* t *such that* $f(z) \not\equiv z^{2^{-1}t} h(z) \pmod{z^{r+1}-1}$.

[2]Let $m = 2$, then the CPP exponent $d_3 = 3 \cdot \frac{3^8-1}{5} + 1 = 3937$ over $\mathbb{F}_{3^8}$ can now be explained for the first time.

Table 3: Number of elements in C_i for $p = 2$ and $r = 4$

t	N_0	N_1	N_2	N_3	N_4
3	3	0	0	0	3
5	0	10	5	5	10
7	21	21	21	42	21
9	111	72	111	108	108
11	385	429	429	385	418
13	1573	1677	1690	1677	1573
15	6486	6560	6580	6580	6560
17	26452	26452	26010	26146	26010
19	105412	104842	105412	104310	104310
21	418575	419580	419580	418575	420840

Table 4: Number of elements in C_i for $p = 3$ and $r = 4$

t	N_0	N_1	N_2	N_3	N_4
1	0	0	0	1	0
3	6	6	6	6	1
5	41	60	40	40	60
7	420	421	420	462	462
9	3894	3876	4141	3876	3894
11	35684	35684	35332	35113	35332

Appendix A: proof of Lemma 10

Proof: Since $h^k(z) \equiv 1 \pmod{z^{r+1} - 1}$, then $\gcd(h^k(z), z^{r+1} - 1) = \gcd(h(z), z^{r+1} - 1) = 1$. According to Lemma 4, for any $h(z)$ satisfying $h^k(z) \equiv 1 \pmod{z^{r+1} - 1}$, the number of monic irreducible polynomials $f(z)$ over $\mathbb{F}_p$ with degree t such that $f(z) \equiv z^{2^{-1}t} h(z) \pmod{z^{r+1} - 1}$ is

$$\frac{1}{\Phi(z^{r+1} - 1)} \frac{p^t}{t} + O\left(\frac{p^{\frac{t}{2}}}{t}\right).$$

Note that one root of the polynomial $1 + z + z^2 + \cdots + z^r$ is w with $w^{r+1} = 1$, and the minimal polynomial of ω is $1 + z + z^2 + \cdots + z^r$, thus $1 + z + z^2 + \cdots + z^r$ is irreducible over $\mathbb{F}_p$. It is known that

$$\mathbb{F}_p[z]/(z^{r+1} - 1) \cong \mathbb{F}_p[z]/(z - 1) \oplus \mathbb{F}_p[z]/(1 + z + z^2 + \cdots + z^r),$$

where $\oplus$ is the direct sum. Since $\mathbb{F}_p[z]/(1 + z + z^2 + \cdots + z^r) \cong \mathbb{F}_{p^r}$, we have

$$\mathbb{F}_p[z]/(z - 1) \oplus \mathbb{F}_p[z]/(1 + z + z^2 + \cdots + z^r) \cong \mathbb{F}_p \oplus \mathbb{F}_{p^r}.$$

As a consequence, $\mathbb{F}_p[z]/(z^{r+1}-1)$ is isomorphic to $\mathbb{F}_p \oplus \mathbb{F}_{p^r}$. Thus, $h(z) \pmod{z^{r+1}-1}$ can be represented by a polynomial pair

$$\Big(h(1), h(z)\big(\mathrm{mod}\ \frac{z^r-1}{z-1}\big)\Big) = (h(1), h(\omega)),$$

where $h^k(\omega)=1$, i.e., $h(\omega) \in R = \{\omega \,|\, \omega^k = 1,\ \omega \in \mathbb{F}_{p^r}\}$. Thus, the number of polynomials $h(z)$ such that $h^k(z) \equiv 1 \pmod{2^{r+1}-1}$ is $|R| = k$.

On the other hand, $\Phi(1+z+z^2+\cdots+z^r) = p^r$ due to $1+z+z^2+\cdots+z^r$ is irreducible over $\mathbb{F}_p$. Thus, $\Phi(z^{r+1}-1) = \Phi(z-1)\Phi(1+z+z^2+\cdots+z^r) = p^r$. As a consequence, the number of monic irreducible polynomials $f(z)$ over $\mathbb{F}_p$ with degree t such that $f(z) \equiv z^{2^{-1}t}h(z) \pmod{z^{r+1}-1}$ for any $h(z)$ satisfying $h^k(z) \equiv 1 \pmod{2^{r+1}-1}$ is

$$\begin{aligned} \frac{k}{\Phi(z^{r+1}-1)}\frac{p^t}{t} + O\Big(\frac{p^{\frac{t}{2}}}{t}\Big) &= \frac{k}{p^r}\cdot\frac{p^t}{t} + O\Big(\frac{p^{\frac{t}{2}}}{t}\Big) \\ &= \frac{k}{k(r+1)+1}\frac{p^t}{t} + O\Big(\frac{p^{\frac{t}{2}}}{t}\Big) \\ &\approx \frac{1}{r+1}\frac{p^t}{t}. \end{aligned}$$

It is known that the number of irreducible polynomials over $\mathbb{F}_p$ with degree t (t is prime) is $\frac{1}{t}(p^t-p)$ [37, Theorem 3.25]. Therefore, we can always find a sufficiently large integer T for each r such that $\frac{1}{t}(p^t-p) > \frac{k}{k(r+1)+1}\frac{p^t}{t} + O\Big(\frac{p^{\frac{t}{2}}}{t}\Big)$ if $t > T$. Thus we complete the proof. $\square$

Appendix B: proof of Lemma 11

Proof: Suppose $\alpha \in \mathbb{F}_{p^t} \setminus \mathbb{F}_p$. Define

$$f(z) = \prod_{\lambda=0}^{t-1}(\alpha^{p^\lambda} + z) \in \mathbb{F}_p[z].$$

It is well known that $f(z)$ is the minimal polynomial of $-\alpha \in \mathbb{F}_{p^t}\setminus\mathbb{F}_p$ in $\mathbb{F}_p$, and $f(z)$ is irreducible over $\mathbb{F}_p$ with degree t. Recall that $\omega \in \mathbb{F}_{p^r}\setminus\{1\}$ and $\omega^{r+1}=1$. Let $z=\omega$, we have

$$\begin{aligned} f(\omega) &= \prod_{\lambda=0}^{t-1}(\alpha^{p^\lambda}+\omega) = \prod_{\lambda=0}^{t-1}(\alpha^{p^{r\lambda}}+\omega) = \prod_{\lambda=0}^{t-1}(\alpha+\omega)^{(p^r)^\lambda} \\ &= (\alpha+\omega)^{1+p^r+p^{2r}+\cdots+p^{(t-1)r}} = (\alpha+\omega)^{\frac{p^{rt}-1}{p^r-1}}, \end{aligned}$$

where the second equation is due to $\{r, 2r, 3r, \cdots, (t-1)r\} \pmod t = \{1, 2, 3, \cdots, t-1\}$ by $\gcd(r, t) = 1$.

Remember $p^r = k(r+1)+1$, thus if $\alpha \in C_j = \{a \in \mathbb{F}_{p^t}^* \backslash \{-1\} \mid (a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^j\}$, then $f(\omega)^k = (\alpha+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^j$. Since $f(z) \in \mathbb{F}_p[z]$, we have $f(\omega^{p^i})^k = f(\omega)^{p^i \cdot k} = \omega^{p^i \cdot j}$. Then $f(\omega^i)^k = \omega^{ij}$ for $i \in \{1, 2, \cdots, r\}$ due to $\{p^i \pmod{r+1}, 0 \le i \le r-1\} = \{1, 2, \cdots, r\}$. By Lemma 6, we have $p^t - 1 | \frac{p^{rt}-1}{r+1}$, then $f(1)^k = (\alpha+1)^{\frac{p^{rt}-1}{r+1}} = 1$. Therefore we have $f(\omega^i)^k = \omega^{ij}$ for $i \in \mathbb{Z}_{r+1}$.

Consider $f^k(z) = (z^{r+1}-1)g(z) + r(z)$, then the degree of $g(z)$ is $\deg\big(g(z)\big) = kt - (r+1)$, and $\deg(r(z)) \le r$. For $i \in \mathbb{Z}_{r+1}$, $r(\omega^i) = f^k(\omega^i) = \omega^{ij}$. Thus, $r(z) = z^j$ since $\deg(r(z)) \le r$. As a consequence, $f^k(z) \equiv z^j \pmod{z^{r+1}-1}$, which is equivalent to $f(z) \equiv z^{k^{-1}j} h(z) \pmod{z^{r+1}-1}$, where $h^k(z) \equiv 1 \pmod{z^{r+1}-1}$. Now we have shown that if $\alpha \in C_j$, then $f(z) \equiv z^{k^{-1}j} h(z) \pmod{z^{r+1}-1}$ for some $h(z)$ satisfying $h^k(z) \equiv 1 \pmod{z^{r+1}-1}$.

Let $j = -(lm)^{-1}$. Since $ktlm \equiv -2 \pmod{r+1}$, thus $k^{-1}j = -(klm)^{-1} \equiv 2^{-1}t \pmod{r+1}$. By Lemma 10, if $t \ge T$, then for any $h(z)$ such that $h^k(z) \equiv 1 \pmod{z^{r+1}-1}$, there exists an irreducible polynomial $f'(z)$ over $\mathbb{F}_p$ with degree t such that $f'(z) \not\equiv z^{2^{-1}t} h(z) \pmod{z^{r+1}-1}$. Let α' be a root of $f'(z)$. Then $\alpha' \in \mathbb{F}_{p^t}^* \setminus \{-1\}$, but $\alpha' \notin C_j = C_{-(lm)^{-1}}$. Thus, $|C_{-(lm)^{-1}}| < p^t - 2$. $\square$

Appendix C: proof of Lemma 12

Proof: If $|C_{-(lm)^{-1}}| < p^t - 2$, then there exists $j \in \mathbb{Z}_{r+1}$ with $j \not\equiv -(lm)^{-1} \pmod{r+1}$ such that $|C_j| = |C_{kt-j}| > 0$. Thus, there exist $a, b \in \mathbb{F}_{p^t}^* \backslash \{-1\}$ such that $(a+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^j$ and $(b+\omega)^{\frac{p^{rt}-1}{r+1}} = \omega^{kt-j}$. As a consequence,

$$(a+\omega)^{\frac{p^{rt'}-1}{r+1}} = (a+\omega)^{\frac{p^{rt}-1}{r+1}\frac{p^{rt'}-1}{p^{rt}-1}} = (\omega^j)^{\frac{p^{rt'}-1}{p^{rt}-1}} = \omega^{js},$$

and

$$(b+\omega)^{\frac{p^{rt'}-1}{r+1}} = (b+\omega)^{\frac{p^{rt}-1}{r+1}\frac{p^{rt'}-1}{p^{rt}-1}} = (\omega^{kt-j})^{\frac{p^{rt'}-1}{p^{rt}-1}} = \omega^{(kt-j)s},$$

i.e., $a \in C'_{js}$ and $b \in C'_{kt'-js}$. Therefore, $|C'_{js}| > 0$ and $|C'_{kt'-js}| > 0$.

Since $j \not\equiv -(lm)^{-1} \pmod{r+1}$ and $-(lm)^{-1} \equiv kt + (lm)^{-1} \pmod{r+1}$, we have $j \not\equiv kt - j \pmod{r+1}$, then $js \not\equiv kt' - js \pmod{r+1}$[3], that is $C'_{js} \cap C'_{kt'-js} = \emptyset$, together with $|C'_{js}| > 0$ and $|C'_{kt'-js}| > 0$, we obtain $0 < |C'_{js}| < p^{t'} - 2$ and $0 < |C'_{kt'-js}| < p^{t'} - 2$. Then it follows that $|C'_{-(lm)^{-1}}| < p^{t'} - 2$. $\square$

[3]Here we assume that $\gcd(s, r+1) = 1$, since if $\gcd(s, r+1) = r+1$, then $\gcd(kt', r+1) = \gcd(kts, r+1) = r+1$. By (1) in Lemma 9, $|C'_{-(lm)^{-1}}| < p^{t'} - 2$.

Acknowledgments

The authors would like to thank the anonymous referees and the Associate Editor, Dr. Daniel Katz, for their detailed comments. The first author would like to thank Chunlei Li and Yongbo Xia for many helpful suggestions. The work of G. Wu was supported by the Open Project Program from Hubei Key Laboratory of Applied Mathematics (Grant No. HBAM202102) and the Natural Science Basic Research Program of Shaanxi (Grant No. 2021JQ-192). The work of K. Feng was supported by the National Natural Science Foundation of China (Grant No. 12031011). The work of N. Li was supported by the National Natural Science Foundation of China (Grant No. 62072162), the Natural Science Foundation of Hubei Province of China (Grant No. 2021CFA079), and the Knowledge Innovation Program of Wuhan-Basic Research (Grant No. 2022010801010319). The work of T. Helleseth was supported by the Research Council of Norway (Grant No. 247742/O70).

References

[1] A. Akbary, Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci., (2007) 23408.

[2] L. Bassalygo, V. Zinoviev, Permutation and complete permutation polynomials, Finite Fields Appl., 33 (2015) 198-211.

[3] D. Bartoli, M. Giulietti, G. Zini, On monomial complete permutation polynomials, Finite Fields Appl., 41 (2016) 132-158.

[4] D. Bartoli, M. Giulietti, L. Quoos, G. Zini, Complete permutation polynomials from exceptional polynomials, J. Number Theory, 176 (2017) 46-66.

[5] C. Bracken, C. H. Tan, Y. Tan, Binomial differentially 4-uniform permutations with high nonlinearity, Finite Fields Appl., 18 (3) (2012) 537-546.

[6] C. Beierle, M. Brinkmann, G. Leander, Linearly self-equivalent APN permutations in small dimension, IEEE Trans. Inf. Theory, 67 (7) (2021) 4863-4875.

[7] C. Beierle, G. Leander, New instances of quadratic APN functions, IEEE Trans. Inf. Theory, 68 (1) (2022) 670-678.

[8] A. Canteaut, S. Duval, L. Perrin, A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}, IEEE Trans. Inf. Theory, 63 (11) (2017) 7575-7591.

[9] L. Carlitz, Some theorems on permutation polynomials, Bull. Amer. Math. Soc., 68 (2) (1962) 120-122.

[10] L. Carlitz, C. Wells, The number of solutions of a special system of equations in a finite field, Acta Arithmetica, 12 (1966) 77-84.

[11] A. Canteaut, P. Charpin, H. Dobbertin, Binary m-sequences with three-valued cross correlation: a proof of Welch's conjecture, IEEE Trans. Inf. Theory, 46 (1) (2000) 4-8.

[12] P. Charpin, Cyclic codes with few weights and Niho exponents, J. Comb. Theory A, 108 (2) (2004) 247-259.

[13] P. Charpin, G. M. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}$, SIAM J. Discrete Math., 22 (2) (2008) 650-665.

[14] T. W. Cusick, H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences, IEEE Trans. Inf. Theory, 42 (4) (1996) 1238-1240.

[15] H. Dobbertin, T. Helleseth, P. Kumar, H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type, IEEE Trans. Inf. Theory, 47 (4) (2001) 1473-1481.

[16] H. Dobbertin, One-to-one highly nonlinear power functions on GF(2^n), Appl. Algebr. Eng. Comm., 9 (2) (1998) 139-152.

[17] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl, Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums, IEEE Trans Inf. Theory, 52 (2) (2006) 613-627.

[18] P. Ellingsen, P. Felke, C. Riera, P. Stanica, A. Tkachenko, C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity, IEEE Trans. Inf. Theory, 66 (9) (2020) 5781-5789.

[19] X. Feng, D. Lin, L. Wang, Q. Wang, Further results on complete permutation monomials over finite fields, Finite Fields Appl., 57 (2019) 47-59.

[20] H. D. L. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, Finite Fields Appl., 7 (2) (2001) 253-286.

[21] S. Fu, X. Feng, B. Wu, Differentially 4-uniform permutations with the best known nonlinearity from butterflies, IACR Trans. Symmetric Cryptol., (2) (2017) 228-249.

[22] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions (Corresp.), IEEE Trans. Inf. Theory, 14 (1) (1968) 154-156.

[23] S. Hasan, M. Pal, P. Stanica, The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials, IEEE Trans. Inf. Theory, 68 (1) (2022) 679-691.

[24] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math., 16 (1976) 209-232.

[25] T. Helleseth, J. Lahtonen, P. Rosendahl, On Niho type cross-correlation functions of m-sequences, Finite Fields Appl., 13 (2) (2007) 305-317.

[26] T. Helleseth, A note on the cross-correlation function between two binary maximal length linear sequences, Discrete Math., 23 (3) (1978) 301-307.

[27] T. Helleseth, Pairs of m-sequences with a six-valued cross-correlation. In Mathematical Properties of Sequences and Other Combinatorial Structures, pp. 1-6. Springer US (2003).

[28] A. Johansen, T. Helleseth, A family of m-sequences with five-valued cross correlation, IEEE Trans. Inf. Theory, 55 (2) (2009) 880-887.

[29] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, Information and Control, 18 (4) (1971) 369-394.

[30] D. J. Katz, P. Langevin, Proof of a conjectured three-valued family of Weil sums of binomials, Acta Arithmetica, 169 (2) (2015) 181-199.

[31] N. Katz, R. Livne, Sommes de Kloosterman et courbes elliptiques universelles en caracteristiques 2 et 3, C. R. Acad. Sci. Paris Ser. I Math. 309 (11) (1989) 723-726.

[32] G. Lachaud, J. Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caracteristique 2, C. R. Acad. Sci. Paris Ser. I Math. 305 (20) (1987) 881-883.

[33] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl., 13 (1) (2007) 58-70.

[34] K. Li, L. Qu, B. Sun, C. Li, New results about the boomerang uniformity of permutation polynomials, IEEE Trans. Inf. Theory, 65 (11) (2019) 7542-7553.

[35] L. Li, C. Li, C. Li, X. Zeng, New classes of complete permutation polynomials, Finite Fields Appl., 55 (2019) 177-201.

[36] N. Li, M. Xiong, X. Zeng, On permutation quadrinomials and 4-uniform BCT, IEEE Trans. Inf. Theory, 67 (7) (2021) 4845-4855.

[37] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia Math. Appl. Cambridge University Press (1997).

[38] J. Ma, T. Zhang, T. Feng, G. Ge, Some new results on permutation polynomials over fnite felds, Des., Codes Cryptogr., 83 (2017) 425-443.

[39] S. Mesnager, C. Riera, P. Stanica, H. Yan, Z. Zhou, Investigations on c-(almost) perfect nonlinear functions, IEEE Trans. Inf. Theory, 67 (10) (2021) 6916-6925.

[40] S. Mesnager, C. Tang, M. Xiong, On the boomerang uniformity of quadratic permutations, Des., Codes Cryptogr., 88 (10) (2020) 2233-2246.

[41] H. Niederreiter, K. H. Robinson, Complete mappings of finite fields, J. Aust. Math. Soc. Ser. A, 33 (2) (1982) 197-212.

[42] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences, Ph.D. dissertation, Univ. Southern, California, Los Angeles (1972).

[43] P. Ongan, B. Temr, A specific type of permutation and complete permutation polynomials over finite fields, J. Algebra Appl., 19 (4) (2020) 2050067:1-8.

[44] H. Park, J. Lee, Permutation polynomials and group permutation polynomials, Bull. Aust. Math. Soc., 63 (2001) 67-74.

[45] L. Qu, Y. Tan, C. H. Tan, C. Li, Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method, IEEE Trans. Inf. Theory, 59 (7) (2013) 4675-4686.

[46] K. Ranto, P. Rosendahl, On four-valued Niho type cross-correlation functions of m-sequences. IEEE Trans. Inf. Theory, 52 (12) (2006) 5533-5536.

[47] M. Rosen, Number theory in function fields, GTM 210 Springer-Verlag New York (2002).

[48] S. Sarkar, S. Bhattacharya, A. Cesmelioglu, On some permutation binomials of the form $x^{\frac{2^n-1}{k}+1}+ax$ over $\mathbb{F}_{2^n}$: Existence and Count, WAIFI (2012) 236-246.

[49] H. M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, PhD thesis, University of Southern California, Los Angeles (1970).

[50] Z. Tu, N. Li, X. Zeng, J. Zhou, A class of quadrinomial permutations with boomerang uniformity four, IEEE Trans. Inf. Theory, 66 (6) (2020) 3753-3765.

[51] Z. Tu, X. Zeng, L. Hu, Several classes of complete permutation polynomials, Finite Fields Appl., 25 (2014) 182-193.

[52] Z. Tu, X. Zeng, L. Hu, C. Li, A class of binomial permutation polynomials, arXiv:1310.0337v1, Oct. (2013).

[53] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, Monatshefte Math., 112 (1991) 149-163.

[54] G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of monomials complete permutation polynomials over finite fields of characteristic two, Finite Fields Appl., 28 (2014) 148-165.

[55] G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of complete permutation polynomials over $\mathbb{F}_q$, Science China Math., 58 (10) (2015) 2081-2094.

[56] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: Sequences, Subsequences, and Consequences, Springer, (2007) 119-128.

[57] Y. Xia, T. Helleseth, G. Wu. A note on cross-correlation distribution between a ternary m-sequence and its decimated sequence, SETA (2014) 249-259.

[58] N. Y. Yu, G. Gong. Cross-correlation properties of binary sequences with ideal two-level autocorrelation, SETA (2006) 104-118.

[59] T. Zhang, S. Li, T. Feng, G. Ge, Some new results on the cross correlation of m-sequences, IEEE Trans. Inf. Theory. 60 (5) (2014) 3062-3068.