On Some Permutation Binomials and Trinomials Over F 2 n

Srimanta Bhattacharya, Sumanta Sarkar

On Some Permutation Binomials and Trinomials Over $\mathbb{F}_{2^n}$

Srimanta Bhattacharya and Sumanta Sarkar

Center of Excellence in Cryptology,
Indian Statistical Institute, Kolkata, India.
mail.srimanta@gmail.com,
sumanta.sarkar@gmail.com

Abstract. In this work, we completely characterize (i) permutation binomials of the form $f(x) = x^{\frac{2^n-1}{2^k-1}+1} + ax \in \mathbb{F}_{2^n}[x]$, k odd and $n = 2^r k (r \geq 1)$, $a \in \mathbb{F}_{2^{2k}}^*$, and (ii) permutation trinomials of the form $x^{2^r+1} + x^{2^{r-1}+1} + \alpha x \in \mathbb{F}_{2^k}[x], k$ odd. First result, which was our primary motivation, is a consequence of the second result. Second result may be of independent interest.

Keywords: Finite field, permutation binomial, permutation trinomial.

1 Introduction

1.1 Background and Statement of Our Contribution

Let $\mathbb{F}_q$ denote the finite field of order q. A polynomial $F(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $F : a \to F(a), a \in \mathbb{F}_q$, induced by $F(x)$ is a bijection of $\mathbb{F}_q$. PPs have numerous applications in cryptography, coding theory and combinatorial designs. Characterization of PPs is an important problem from practical as well as theoretical point of view, and significant amount of research have been devoted to this purpose. Characterization of important classes of PPs such as Linearized polynomials, Dickson polynomials, etc., have already been done (cf. [8]). Also, there seems to be renewed interest in the problem in recent times. However, despite considerable attention, the problem remains unsolved in general.

Among polynomials, monomials are easily characterized for their permutation properties; the monomial $F(x) = x^d$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$. However, the problem is already difficult for binomials of the form $x^d + ax$. In fact, even for binomials of the specific form $x^{\frac{q-1}{m}+1} + ax \in \mathbb{F}_q[x]$, where m is a divisor of $q-1$[1], precise characterization is available only for small values of m. For example, in [10], the authors characterize permutation binomials corresponding to $m = 2$. Our first result, which was our primary motivation, pertains

[1] These permutation binomials fall in the class of *cyclotomic mapping* permutations; see [6, 11] for details.

to this class of binomials. Before stating the result we give a brief overview of relevant results for this class.

In [2], it was proven that for a given m and for sufficiently large prime power q such that $m \mid q-1$, there exists PP of the form $x^{\frac{q-1}{m}+1}+ax$; the case $m=3$ was proven earlier in [1]. In [17], number of such binomial permutations was estimated to be $\frac{m!}{m^m}q+O(\sqrt{q})$. This estimate was refined and extended in [7,9]. On the other hand, it follows immediately from Hermite-Dickson criteria (to be discussed in the next section) that if $d \mid q-1$ then there are no PP of degree d over $\mathbb{F}_q$. One of the most important general nonexistence results is Carlitz's conjecture, proven in [4,16], which states that if $\gcd(n, q-1)=1$ and $q > n^4$ (see [10,15] for slightly better estimate for binomials of the form x^d+ax) then there is no PP of degree n over $\mathbb{F}_q$. These results are general, and though they present an overall picture, their accuracy is limited when it comes to specific cases. So, it is naturally motivating to make the above results precise, at least in specific cases. Exact results broaden our understanding of the problem and are also useful for practical applications.

In [13], it was shown that for any even $n>4$, there exists $a \in \mathbb{F}_{2^n}$ such that $x^{\frac{2^n-1}{3}+1}+ax$ is a permutation binomial, also for $n=2^it, i>0, t$ odd, exact count of a's in the subfield $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^n}$ was given; this is sharpening of Carlitz's result [1] in even characteristic. Further, permutation binomials of the form $x^{\frac{2^{2n}-1}{2^n-1}+1}+ax \in \mathbb{F}_{2^{2n}}[x]$ were completely characterized in [13] [2]. In a more recent work [19], the authors considered permutation binomials of the form $x^{\frac{2^{tk}-1}{2^k-1}+1}+ax$ over $\mathbb{F}_{2^{tk}}$ for $t \in \{3,4,6,10\}$, and for these cases they obtained partial characterizations and counts of permutation binomials Our result is motivated by the problem of obtaining full characterization of permutation binomials in the above cases, as well as for other exponents of this class. While trying to extend the results of [19] for $t=4$ case to $t=8$ case we observed that though there exists (and fully charcterized in [19], also in Theorem 1 below) $a \in \mathbb{F}_{2^{2k}}$ such that $x^{\frac{2^{4k}-1}{2^k-1}+1}+ax$ is a PP of $\mathbb{F}_{2^{4k}}$, there does not exist any $a \in \mathbb{F}_{2^{2k}}$ such that $x^{\frac{2^{8k}-1}{2^k-1}+1}+ax$ is a PP of $\mathbb{F}_{2^{8k}}$. This observation is extended to the following interesting generalization.

Theorem 1. *Let r,k be positive integers with k odd and $n=2^rk$. Then the polynomial $f(x)=x^{\frac{2^n-1}{2^k-1}+1}+ax$, $a \in \mathbb{F}^*_{2^{2k}}$ is a PP of $\mathbb{F}_{2^n}$ if and only if (i) $r=1,2$ and (ii) $a \in w\mathbb{F}^*_{2^k} \cup w^2\mathbb{F}^*_{2^k}$, where $w \in \mathbb{F}_{2^2}$ is a root of the equation $w^2+w+1=0$.*

Observe that the above result does not follow from Carlitz's conjecture, not even for large enough n (with respect to k).

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called *complete mapping polynomial* of $\mathbb{F}_q$ if both $f(x)$ and $f(x)+x$ are permutations of $\mathbb{F}_q$. Such polynomials are useful for construction of orthogonal latin squares and check digit systems (see [14,18]). It

[2] This is a specific case of a more general result proven in [3], where it was shown that binomials of the form $x^{2^k+2}+ax \in \mathbb{F}_{2^{2n}}[x]$ are permutations only when $k=n$.

is easy to see that $x^{\frac{q-1}{m}+1}+ax$ is a PP of $\mathbb{F}_q$ iff $a^{-1}x^{\frac{q-1}{m}+1}$ is a complete mapping polynomial of $\mathbb{F}_q$ ($a^{-1}x^{\frac{q-1}{m}+1}$ is always PP of $\mathbb{F}_q$). So, our first result is also a characterization of complete mapping polynomials of the form $ax^{\frac{2^{2^rk}-1}{2^k-1}} \in \mathbb{F}_{2^{2^rk}}$, k odd, $a \in \mathbb{F}_{2^{2k}}$.

Our proof of Theorem 1 is through another nonexistence result of permutation trinomials. Below we state the theorem.

Theorem 2. *$x^{2^r+1}+x^{2^{r-1}+1}+\alpha x \in \mathbb{F}_{2^k}[x], k$ odd, is a PP of $\mathbb{F}_{2^k}$ if and only if $\alpha = 1$, and $r = 1$ or 2.*

We use Theorem 2 along with a theorem (Theorem 5, stated in the next section) due to Wan and Lidl to derive Theorem 1. Though we use Theorem 2 to prove Theorem 1, it may be of independent interest, especially since permutation properties of trinomials are much less known.

In the next subsection, we state results we will use in our proofs. In the subsequent section, first we prove Theorem 2, and then Theorem 1.

1.2 Useful Results

Hermite-Dickson criteria (Theorem 3) and Lucas' theorem (Theorem 4) are our main tools in our proof of Theorem 2; in fact, we use a corollary (Corollary 1) of Lucas' theorem. Finally, we derive Theorem 1 from Theorem 2 using Wan-Lidl criteria.

Theorem 3 (Hermite,Dickson (see [5,8])). *A polynomial $f \in \mathbb{F}_q[x]$ is a PP if and only if*

1. *f has exactly one root in $\mathbb{F}_q$,*
2. *$f^t \mod (x^q-x)$ has degree less than $q-1$, for all $1 \le t \le q-2, p \nmid t$, where p is the characteristic of $\mathbb{F}_q$.*

Remark 1. In the above theorem one can remove the condition $p \nmid t$; in fact, we will do so in the proof of Theorem 2.

Theorem 4 (Lucas (see [8])). *Let p be a prime, and $n, r_1, r_2, \ldots, r_t$ be non-negative integers such that*
$n = d_0 + d_1p + d_2p^2 + \ldots + d_sp^s$ $(0 \le d_i \le p-1, \forall\ 0 \le i \le s)$
$r_j = d_{j0} + d_{j1}p + d_{j2}p^2 + \ldots + d_{js}p^s$ $(0 \le d_{ji} \le p-1, \forall\ 1 \le j \le t, \forall\ 0 \le i \le s)$
Then

$$\binom{n}{r_1, r_2, \ldots, r_t} = \binom{d_0}{d_{10}, d_{20}, \ldots, d_{t0}} \cdots \binom{d_s}{d_{1s}, d_{2s}, \ldots, d_{ts}} \mod (p)$$

We will need the following corollary of the above theorem.

Corollary 1. $\binom{n}{r_1, r_2, \ldots, r_t} \neq 0 \mod (p)$ *iff* $\sum_{i=1}^{t} d_{ij} = d_j, \forall\ 0 \le j \le s$.

Theorem 5 (Wan, Lidl [12]). *Let m and s be two positive integers such that m divides $q-1$. Let α be a primitive element in $\mathbb{F}_q$ and assume $P(x)$ is a polynomial in $\mathbb{F}_q[x]$. Then $Q(x) = x^sP(x^{\frac{q-1}{m}})$ is a PP of $\mathbb{F}_q$ if and only if the following conditions are satisfied. (i) $\gcd(s, \frac{q-1}{m}) = 1$, (ii) for all i, $0 \le i < m$, $P(\alpha^{i\frac{q-1}{m}}) \neq 0$, (iii) for all i, j, $0 \le i < j < m$, $Q(\alpha^i)^{\frac{q-1}{m}} \neq Q(\alpha^j)^{\frac{q-1}{m}}$.*

Let $a = \sum_{i=0}^{l} a_i 2^i$ be the 2-adic representation of a, then we denote by a_i the ith bit [3] of a. For example, $a = 2$ has base-2 representation 10; its 0th bit is 0, and 1st bit is 1. Also, let $\mathrm{wt}(a) \triangleq |\{i|a_i \neq 0\}|$.

2 Proofs

2.1 Proof of Theorem 2

Proof. Note that it is sufficient to consider the cases with $r < k$, as for $r \geq k$, the polynomial $x^{2^r+1} + x^{2^{r-1}+1} + \alpha x$ can be reduced modulo $x^{2^k} + x$ to get a polynomial $x^{2^{r'}+1} + x^{2^{r'-1}+1} + \alpha x, r' < k$, which induces identical mapping on $\mathbb{F}_{2^k}$.

First, we consider the cases corresponding to $r = 0, 1, 2$, and for these cases we directly refer to the work of Dickson [5] (see also [8]), where all PPs of degree ≤ 5 for all characteristics have been characterized. The characterization is in terms of *reduced* or *normalized* polynomials. A polynomial f of degree n is normalized if a) f is monic b) $f(0) = 0$, and c) when degree of f is not divisible by the characteristic, coefficient of the term of degree $n-1$ is zero.

For $r = 0$, $f(x) = x^2 + x^{2^{k-1}+1} + \alpha x$. Note that $f(x)$ is a PP iff $g(x) = f(x)^2 \mod (x^{2^k} + x)$ is a PP. Now, $g(x) = f(x)^2 \mod (x^{2^k} + x) = x^4 + x^3 + \alpha^2 x^2$. So, $g(x)$ is in normalized form and it follows from [5] that $g(x)$ is not a PP of $\mathbb{F}_{2^k}$ for any k.

Similarly, it also follows from [5] that for the cases $r = 1$ and 2, $f(x) = x^{2^r+1} + x^{2^{r-1}+1} + \alpha x \in \mathbb{F}_{2^k}[x]$ is a PP of $\mathbb{F}_{2^k}$ if and only if k is odd and $\alpha = 1$. In fact, for $r = 2, \alpha = 1$, $f(x) = x^5 + x^3 + \alpha x$ is the *Dickson polynomial* (see [8] for more details on this very important class of polynomials), $D_5(x, 1)$, which is a PP of $\mathbb{F}_{2^k}$, k odd, since $\gcd(2^{2k} - 1, 5) = 1$.

Now, we show that f is not a PP for $r \geq 3$ by applying the Hermite-Dickson criteria (Theorem 3). For this we raise f to $2^k - 3$ and $2^k - 4$ modulo $x^{2^k} + x$ and show that the degree of the resulting polynomial is $2^k - 1$ in at least one of the two cases. Here it is important to note that for any polynomial $g \in \mathbb{F}_{2^k}[x]$, exactly those terms whose exponents are multiples of $2^k - 1$ reduce to the term with exponent $2^k - 1$ when g is reduced modulo $x^{2^k} + x$. More precisely, and specifically for our case, we note the following fact which will be used later.

Fact 1 *Let* $g = \sum_i a_i x^i \in \mathbb{F}_{2^k}[x]$, *and let* $g \mod (x^{2^k} + x) = b_{2^k-1} x^{2^k-1} + \sum_{i=0}^{2^k-2} b_i x^i$. *Then* $b_{2^k-1} = \sum_{\substack{j \\ 2^k-1|j}} a_j$

Hence, we will be done if we can show that sum of the coefficients of the terms whose exponents are multiples of $2^k - 1$ in the exapnsion of f^{2^k-3} or f^{2^k-4} is non-zero. For this we first consider the expansion of f^{2^k-3} and then of f^{2^k-4} and show that if in the first case the sum is zero then it is non-zero in the second case; though the approaches are similar in these two cases, they are not exactly

[3] We will use the abbreviation 'bit' for binary digit.

same.

Case 1. f^{2^k-3} : First note that coefficient of a term whose exponent is $\ell(2^k-1), \ell \geq 1$, in the expansion of f^{2^k-3} is $(\binom{2^k-3}{a,b,c} \mod (2))\alpha^c$, where $0 \leq a, b, c \leq 2^k-3$ are such that the following conditions hold

$$a+b+c = 2^k-3 \tag{1}$$
$$(2^r+1)a + (2^{r-1}+1)b + c = \ell(2^k-1). \tag{2}$$

Let $\mathcal{S} = \{(a,b,c,\ell) | a,b,c,\ell \text{ non-negative, and satisfies (1) and (2)}\}$. Our goal is to find expression of the sum $\sum_{(a,b,c,\ell)\in\mathcal{S}} (\binom{2^k-3}{a,b,c} \mod (2))\alpha^c$; we do this by splitting the sum into parts according to the value of ℓ, and investigating contribution from each part.

Henceforth, for this case, whenever we write $\binom{2^k-3}{a,b,c}$, we implicitly assume values of a, b, c satisfying, possibly along with some other constraints, (1) and (2) for some ℓ whose value will be clear from the context. Also, we have the following observation.

Observation 6. *1st bit of* 2^k-3 *is zero. Hence, if any of* $a, b, c \in \{2, 3\} \mod (4)$ *then following Corollary 1* $\binom{2^k-3}{a,b,c} = 0 \mod (2)$.

Now, (2)−(1) yields

$$2^r a + 2^{r-1} b = 2^k(\ell-1) - (\ell-3). \tag{3}$$

Clearly, both a and b can not be zero at the same time, and since $k > r$, we have from (3), $\ell = 3 \mod (2^{r-1})$. Also, from (1) and (2), $\ell \leq 2^r + 1$. So, possible values of ℓ are 3 and $2^{r-1}+3$. We consider the following two subcases based on these two values of ℓ.

Subcase 1.1. $\ell = 3$: In this case (3) yields $b = 2^{k-r+2} - 2a$. Depending on $\mathrm{wt}(a)$ we consider the following subcases.

Subsubcase 1.1.1. $\mathrm{wt}(a) > 1$: Let the first $t (t \geq 1)$ consecutive bits of a be 1, i.e., $a = \sum_{j=i_1-t+1}^{i_1} 2^j + \sum_{j=0}^{i_2} a_j 2^j$, where $i_1 \leq k-r, i_2 \leq i_1-t-1, a_j \in \{0,1\}, 0 \leq j \leq i_2$, and if $t = 1$ then at least one a_j is non-zero (since $\mathrm{wt}(a) > 1$). So, $b = 2^{k-r+2} - \sum_{j=i_1-t+2}^{i_1+1} 2^j - \sum_{j=1}^{i_2+1} a_{j-1} 2^j$. Hence, $b = 2^{i_1+2} - \sum_{j=i_1-t+2}^{i_1+1} 2^j - \sum_{j=1}^{i_2+1} a_{j-1} 2^j \mod (2^{i_1+2})$, since $i_1+2 \leq k-r+2$. Now, $2^{i_1+2} - \sum_{j=i_1-t+2}^{i_1+1} 2^j = 2^{i_1-t+2}$, and $\sum_{j=1}^{i_2+1} a_j 2^j < 2^{i_2+2} \leq 2^{i_1-t+1}$. So, $b \mod (2^{i_1+2}) \leq 2^{i_1-t+2}$, and $b \mod (2^{i_1+2}) > 2^{i_1-t+2} - 2^{i_1-t+1} = 2^{i_1-t+1}$. Again we have the following two possibilities.

- **(i)** $b \mod (2^{i_1+2}) < 2^{i_1-t+2}$: In this case (i_1-t+1)th bit of b is 1, since $b \mod (2^{i_1+2}) > 2^{i_1-t+1}$. So, i_1-t+1-th bits of both a and b are 1. Hence, following Corollary 1, $\binom{2^k-3}{a,b,c} = 0 \mod (2)$.
- **(ii)** $b = 2^{i_1-t+2} \mod (2^{i_1+2})$: In this case, note that $t > 1$. Since otherwise, at least one a_j in the sum $\sum_{j=0}^{i_2} a_j 2^j$, appearing in the binary representation of a, is non-zero, which implies $b < 2^{i_1-t+2} \mod (2^{i_1+2})$, a contradiction. Now, for $t > 1$, i_1-t+2th bit of both a and b are 1. So, again $\binom{2^k-3}{a,b,c} = 0 \mod (2)$.

Subsubcase 1.1.2. $\mathrm{wt}(a) \leq 1$: For $\ell = 3$, (3) implies $a \leq 2^{k-r+1}$. Also, if $a = 1$ then $b = 2^{k-r+2} - 2a$, i.e., $b = 2 \mod (4)$. So, by Observation 6, $\binom{2^k-3}{a,b,c} = 0 \mod (2)$. For the remaining possible values of a, i.e., for $a = 0$ or $2^i, 2 \leq i \leq k-r+1$ we examine the bit patterns of a, b, c in Table 1. For better understanding, we illustrate the case $k = 9, r = 3, i = 4$ in Table 2.

Table 1

Values		Bit positions with 1
$a = 0$, $b = 2^{k-r+2}$, $c = 2^k - 2^{k-r+2} - 3$	a	$\emptyset$
	b	$\{k-r+2\}$
	c	$\{u \mid u = 0, 2 \leq u \leq k-r+1, k-r+3 \leq u \leq k-1\}$
$a = 2^i$, $b = 2^{k-r+2} - 2^{i+1}$, $c = 2^k - 2^{k-r+2} + 2^i - 3$ $(2 \leq i \leq k-r+1)$	a	$\{i\}$
	b	$\{u \mid i+1 \leq p \leq k-r+1\}$
	c	$\{u \mid u = 0, 2 \leq u \leq i-1, k-r+2 \leq u \leq k-1\}$

Table 2

Value	Bit representation
$2^k - 3 = 2^9 - 3$	1 1 1 1 1 1 1 1 0 1
$a = 2^4$	0 0 0 0 0 1 0 0 0 0
$b = 2^8 - 2^5$	0 0 1 1 1 0 0 0 0 0
$c = 2^9 - 2^8 + 2^4 - 3$	0 1 0 0 0 0 1 1 0 1

From Table 1, it can be observed that for these $k-r+1$ values of a, none of a, b, c has 1 in the 1st bit position, each of a, b, c has 0 in the k-th bit position, and for any other bit position u, where $0 \leq u \leq k-1, u \neq 1$, exactly one among a, b, c has 1 in the uth position. Hence, for each of these $k-r+1$ values of a, $\binom{2^k-3}{a,b,c} = 1 \mod (2)$.

So, coefficient of the term with exponent $3(2^k-1)$ in the expansion of f^{2^k-3} is $\alpha^{2^k-2^{k-r+2}-3}(1 + \sum_{i=2}^{k-r+1} \alpha^{2^i})$.

Subcase 1.2. $\ell = 2^{r-1} + 3$: For $\ell = 2^{r-1} + 3$, (3) yields $b = 2^{k-r+2}(2^{r-2} + 1) - 2a - 1$. When $a = 0 \mod (4)$, $b = 3 \mod (4)$, since $r \geq 3$ and $k > r$. So, b has 1 in the 1st bit position. Hence, by Observation 6 $\binom{2^k-3}{a,b,c} = 0$

mod (2). Next, From (1) and (2), we get $c = a - 2^{k-r+2} - 2$. Hence, for $a = 1 \mod (4), c = 3 \mod (4)$, which, by Observation 6, implies $\binom{2^k-3}{a,b,c} = 0 \mod (2)$. Again using Observation 6, $\binom{2^k-3}{a,b,c} = 0 \mod (2)$ for $a = 2$, or $3 \mod (4)$.

Hence, considering the above cases, we get that the coefficient of the term with exponent $2^k - 1$ in the expansion of $f^{2^k-3} \mod x^{2^k} + x$ is $\alpha^{2^k-2^{k-r+2}-3}(1 + \sum_{i=2}^{k-r+1} \alpha^{2^i})$. Hence, if $1 + \sum_{i=2}^{k-r+1} \alpha^{2^i} \neq 0$ then $x^{2^r+1} + x^{2^{r-1}+1} + x, 3 \leq r < k$, is not a PP of $\mathbb{F}_{2^k}$. Otherwise, i.e., if

$$\sum_{i=2}^{k-r+1} \alpha^{2^i} = 1, \tag{4}$$

we consider the next case.

Case 2. f^{2^k-4} : Similar to equations (1), (2), and (3) from the previous case, we get from the expansion of f^{2^k-4} the following set of equations.

$$a + b + c = 2^k - 4 \tag{5}$$
$$(2^r + 1)a + (2^{r-1} + 1)b + c = \ell(2^k - 1) \tag{6}$$
$$2^r a + 2^{r-1} b = 2^k(\ell - 1) - (\ell - 4) \tag{7}$$

As in the previous case, when we write $\binom{2^k-4}{a,b,c}$, we mean values of a, b, c that satisfy (5), (6) (and thereby (7)) for some ℓ which is clear from the context. Here we have the following observation.

Observation 7. *0th bit and 1st bit of $2^k - 4$ are zero. So, if any of $a, b, c \in \{1, 2, 3\} \mod (4)$, then following Corollary 1 $\binom{2^k-4}{a,b,c} = 0 \mod (2)$.*

Next, following similar considerations as in Case 1, from (7) we get for this case $\ell \in \{4, 2^{r-1} + 4\}$. Now, for $\ell = 2^{r-1} + 4$, $b = 2^{k-r+1}(2^{r-1} + 3) - 2a - 1$. Since, $k > r$, $b \in \{1, 3\} \mod (4)$, which implies, by Observation 7, $\binom{2^k-4}{a,b,c} = 0 \mod (2)$. So, we are left with the $\ell = 4$ case, and consider its following subcases.

Subcase 2.1. $\mathrm{wt}(a) \leq 1$: In this case $a = 0$, or $a = 2^i, 0 \leq i \leq k - r + 1$ (upper bound on i follows from (7)). Now, if $i \in \{0, 1\}$ then following Observation 7, $\binom{2^k-4}{a,b,c} = 0 \mod (2)$. Also, for $i = k - r + 1$, $b = 2^{k-r+1}$. So, both a and b have 1 in $(k - r + 1)$th bit position, which again implies $\binom{2^k-4}{a,b,c} = 0 \mod (2)$ for $i = k - r + 1$. For the remaining values of i we show the bit patterns of a, b, c in Table 3. In Table 4, we illustrate the case for $k = 11, r = 4, i = 5$.

From Table 3 it is clear that $\binom{2^k-4}{a,b,c} = 1 \mod (2)$ for these $k - r$ values of a.

Subcase 2.2. $\mathrm{wt}(a) > 1$: Let the first $t (t \geq 1)$ consecutive bits of a be 1, i.e., $a = \sum_{j=i_1-t+1}^{i_1} 2^j + \sum_{j=0}^{i_2} a_j 2^j$, where $i_1 \leq k - r + 1, i_2 \leq i_1 - t - 1, a_j \in \{0, 1\}, 0 \leq j \leq i_2$, and if $t = 1$ then at least one a_j is non-zero. Next, we consider the following subcases.

Subsubcase 2.2.1. $i_1 \leq k - r$: Note that $b = 2^{k-r+2} + 2^{k-r+1} - 2a$, i.e., $b = 2^{k-r+1} + (2^{k-r+2} - 2a)$. Now, from the analysis of the Subsubcase 1.1.1 ($\mathsf{wt(a)} > 1$) of Case 1, we have that both a and $2^{k-r+2} - 2a$ has 1 in the uth bit position, where $u \leq i_1 \leq k - r$. Then it is easy to see that

Table 3

Values		Bit positions with 1
$a = 0$, $b = 2^{k-r+2} + 2^{k-r+1}$, $c = 2^k - 2^{k-r+2} - 2^{k-r+1} - 4$	a	$\emptyset$
	b	$\{k-r+2, k-r+1\}$
	c	$\{u \mid 2 \le u \le k-r,$ $k-r+3 \le u \le k-1\}$
$a = 2^i$, $b = 2^{k-r+2} + 2^{k-r+1} - 2^{i+1}$, $c = 2^k - 2^{k-r+2} - 2^{k-r+1} + 2^i - 4$ $(2 \le i \le k-r)$	a	$\{i\}$
	b	$\{u \mid u = k-r+2,$ $i+1 \le u \le k-r\}$
	c	$\{u \mid 2 \le u \le i-1,$ $u = k-r+1,$ $k-r+3 \le u \le k-1\}$

Table 4

Value	Bit representation
$2^k - 4 = 2^{11} - 4$	1 1 1 1 1 1 1 1 1 1 0 0
$a = 2^5$	0 0 0 0 0 0 1 0 0 0 0 0
$b = 2^9 + 2^8 - 2^6$	0 0 1 0 1 1 0 0 0 0 0 0
$c = 2^{10} + 2^8 + 2^5 - 4$	0 1 0 1 0 0 0 1 1 1 0 0

both a and $2^{k-r+2} + 2^{k-r+1} - 2a$ has 1 in the same uth bit position. So, following Corollary 1, $\binom{2^k-4}{a,b,c} = 0 \mod (2)$ in this case.

Subsubcase 2.2.2. $i_1 = k - r + 1$: We consider the following two possibilities.

(**i**) $\mathrm{wt}(a - 2^{k-r+1}) \ge 2$: So, $b = 2^{k-r+2} + 2^{k-r+1} - 2a = 2^{k-r+1} - 2a'$, where $a' = a - 2^{k-r+1}$, and $\mathrm{wt}(a') \ge 2$. Let $a' = 2^j + \sum_{s=0}^{j-1} a_s 2^s$, $a_s \in \{0, 1\}$, and at least one $a_s = 1$. It is clear that $j \le k - r - 1$, for otherwise $b < 0$. But, this is equivalent to the Subsubcase 1.1.1 ($\mathsf{wt(a)} > 1$) of Case 1, which implies a' and b has 1 in the same uth bit position for some $u \le k - r - 1$. This in turn implies a and b has 1 in the same (as the previous) uth bit position. Hence, we get that $\binom{2^k-4}{a,b,c} = 0 \mod (2)$ in this case as well.

(**ii**) $\mathrm{wt}(a - 2^{k-r+1}) = 1$: Let us assume that $a = 2^{k-r+1} + 2^j$, where $2 \le j \le k - r$. In Table 5, we consider bit patterns of a, b, c for this case. Bit patterns from Table 5 imply that for these $k - r - 1$ values of j $\binom{2^k-4}{a,b,c} = 1 \mod (2)$.

So, considering the above possibilities, we conclude that the coefficient of the term with exponent $4(2^k - 1)$ in the expansion of f^{2^k-4} is

$$\alpha^{2^k - 2^{k-r+2} - 2^{k-r+1} - 4}(1 + \sum_{i=2}^{k-r} \alpha^{2^i}) + \alpha^{2^k - 2^{k-r+2} - 4} \sum_{i=2}^{k-r} \alpha^{2^i} \tag{8}$$

Now, by employing (4) and simplifying we get that the above expression equals $\alpha^{2^k - 2^{k-r+2} + 2^{k-r+1} - 4}$, which is non-zero. From earlier discussion, coefficient of

Table 5

Values		Bit positions with 1
$a = 2^{k-r+1} + 2^j$, $b = 2^{k-r+1} - 2^{j+1}$, $c = 2^k - 2^{k-r+2} + 2^j - 4$ $(2 \le j \le k-r)$	a	$\{j, k-r+1\}$
	b	$\{u \mid j+1 \le u \le k-r\}$
	c	$\{u \mid 2 \le u \le j-1,$ $k-r+2 \le u \le k-1\}$

the term with exponent $(2^{r-1}+4)(2^k-1)$ in the expansion of f^{2^k-4} is 0. So, the coefficient of the term with exponent 2^k-1 in the expansion of $f^{2^k-4} \mod x^{2^k} + x$ is clearly non-zero. □

2.2 Proof of Theorem 1

Proof. We apply Theorem 5 by setting $Q(x) = x(x^{\frac{2^n-1}{2^k-1}} + a)$. Since $s = 1$ in this case, so condition (i) of Theorem 5 is satisfied. Next, observe that condition (ii) of Theorem 5 is satisfied if and only if $a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k}$. So, $Q(x)$ is a PP if and only if condition (iii) of Theorem 5 is satisfied for $a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k}$.

Let α be a primitive element of $\mathbb{F}_{2^n}$, then $\beta = \alpha^{\frac{2^n-1}{2^k-1}}$ be a primitive element of $\mathbb{F}_{2^k}$. So, for all $0 \le i < j < 2^k - 1$, $\quad Q(\alpha^i)^{\frac{2^n-1}{2^k-1}} \ne Q(\alpha^j)^{\frac{2^n-1}{2^k-1}}$ is equivalent to the condition

$$\beta^i(\beta^i + a)^{\frac{2^n-1}{2^k-1}} \ne \beta^j(\beta^j + a)^{\frac{2^n-1}{2^k-1}}, \text{ for } a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k} \text{ and } i \ne j.$$

For $a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k}$, the above condition implies $x(x+a)^{\frac{2^n-1}{2^k-1}}$ is a PP of $\mathbb{F}_{2^k}$. Hence, $Q(x)$ is a PP of $\mathbb{F}_{2^n}$ if and only if $x(x+a)^{\frac{2^n-1}{2^k-1}}$ is a PP of $\mathbb{F}_{2^k}$ for $a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k}$. Now, for k odd, $a \in \mathbb{F}^*_{2^{2k}} \setminus \mathbb{F}^*_{2^k}$ can be written as $a = bw + cw^2$, where $b, c \in \mathbb{F}_{2^k}, b \ne c$, and $w \in \mathbb{F}^*_4 \setminus \{1\}$, i.e., $w^2 + w + 1 = 0$. So,

$$\begin{aligned}
x(x+a)^{\frac{2^n-1}{2^k-1}} &= x(x+bw+cw^2)^{\frac{2^{2^rk}-1}{2^k-1}} \\
&= x(x+bw+cw^2)^{2^{(2^r-1)k}+2^{(2^r-2)k}+\cdots+1} \\
&= x(x+bw+cw^2)^{2^{(2^r-1)k}}(x+bw+cw^2)^{2^{(2^r-2)k}}\ldots(x+bw+cw^2) \\
&= x(x+bw^2+cw)(x+bw+cw^2)\ldots(x+bw^2+cw)(x+bw+cw^2) \\
&= x(x^2+(b+c)x+b^2+c^2+bc)\ldots(x^2+(b+c)x+b^2+c^2+bc) \\
&= (b+c)^{2^r}\left(x^{2^r+1} + x^{2^{r-1}+1} + \left(\frac{b^2+c^2+bc}{b^2+c^2}\right)^{2^{r-1}} x\right) \\
&\quad \text{by the transformation } x \mapsto (b+c)x.
\end{aligned}$$

Note that since $b, c \in \mathbb{F}_{2^k}$, $\left(\frac{b^2+c^2+bc}{b^2+c^2}\right)^{2^{r-1}} \in \mathbb{F}_{2^k}$. Next, applying Theorem 2 on the polynomial $x^{2^r+1} + x^{2^{r-1}+1} + \left(\frac{b^2+c^2+bc}{b^2+c^2}\right)^{2^{r-1}} x$, we get that $x(x+a)^{\frac{2^n-1}{2^k-1}}$ is a PP of $\mathbb{F}_{2^k}$ if and only if (1) $r = 1, 2$ and (2) $\frac{b^2+c^2+bc}{b^2+c^2} = 1$. Now, condition (2) is equivalent to b or c (but not both) $= 0$, which is equivalent to $a \in w\mathbb{F}^*_{2^k} \cup w^2\mathbb{F}^*_{2^k}$. □

Acknowledgment

The authors thank the anonymous reviewers for their valuable comments.

References

1. L. Carlitz, Some theorems on permutation polynomials, Bull. Amer. Math. Soc. vol 68 (2), pp. 120–122, 1962.
2. L. Carlitz and C. Wells, The number of solutions of a special system of equations in a finite field, Acta Arithmetica, vol 12, pp. 77–84, 1966.
3. P. Charpin and G. M. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}^*$, *Siam J. Disc. Math.*, vol 22 (2), pp. 650–665, 2008.
4. S.D. Cohen, and M.D. Fried, Lenstra's Proof of the Carlitz-Wan Conjecture on Exceptional Polynomials: An Elementary Version, Finite Fields and Their Applications, vol 1 (3), pp. 372–375, 1995.
5. L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math., vol 11, pp. 65–120, 1896.
6. A. B. Evans. Orthomorphism graphs of groups, Lecture Notes in Mathematics, vol 1535, Springer, Berlin, 1992.
7. Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields and Their Applications, vol 13, pp. 58–70, 2007.
8. R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications. vol. 20, second edition, Cambridge University Press, 1997.
9. A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields. Trans. of the American Mathematical Society. vol 361 (8), pp 4169–4180, 2009.
10. H. Niederreiter and K. H. Robinson, Complete mappings of finite fields. J. Australian Math. Soc. Ser. A, vol 33, pp. 197–212, 1982.
11. H. Niederreiter and A. Winterhof, Cyclotomic $\mathscr{R}$-orthomorphisms of finite fields. Discrete Math, vol 295, pp. 161–171, 2005.
12. D. Q. Wan and R. Lidl. Permutation polynomials of the form $x^r f(x^{\frac{q-1}{m}})$ and their group structure. *Monatsh. Math.*, Vol 112 (2), pp. 149–163, 1991.
13. S. Sarkar, S. Bhattacharya, and A. Çeşmelioğlu On Some Permutation Binomials of the Form $x^{\frac{2^n-1}{k}+1} + ax$ over $\mathbb{F}_{2^n}$: Existence and Count, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol 7369, pp. 236–246, 2012.
14. R. Shaheen and A. Winterhof, Permutation of finite fields for check digit systems., Designs, Codes, and Cryptography, vol 57 (3), pp. 361–371, 2010.
15. G. Turnwald, Permutation polynomials of binomial type. Contributions to General Algebra, vol 6, pp. 281-286, 1988.
16. Daqing Wan, A generalization of the Carlitz conjecture, Finite Fields, Coding Theory, and Advances in Communications and Computing, Lecture Notes in Pure and Appl. Math., vol 141, pp. 431âĂŞ-432, 1993.
17. Daqing Wan, Gary L. Mullen, and Peter Jau-Shyong Shiue, The number of permutation polynomials of the form $f(x) + cx$ over a finite field. Proceedings of the Edinburgh Mathematical Society (Series 2), vol 38, pp. 133-149, 1993.
18. A. Winterhof, Generalizations of complete mappings of finite fields and some applications, Journal of Symbolic Computation, vol 64, pp. 42–52, 2014.
19. Gaofei Wu, Nian Li, Tor Helleseth, and Yuqing Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, Finite Fields and Their Applications, vol 28, pp. 148-165, 2014.