The Number of Permutation Binomials Over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are Primes

A. Masuda, D. Panario* and Q. Wang*

School of Mathematics and Statistics, Carleton University
Ottawa, Ontario, K1S 5B6, Canada
{ariane,daniel,wang}@math.carleton.ca

Submitted: Feb 14, 2006; Accepted: Jul 12, 2006; Published: Aug 3, 2006
Mathematics Subject Classification: 11T06

Abstract

We give a characterization of permutation polynomials over a finite field based on their coefficients, similar to Hermite's Criterion. Then, we use this result to obtain a formula for the total number of monic permutation binomials of degree less than $4p$ over $\mathbb{F}_{4p+1}$, where p and $4p+1$ are primes, in terms of the numbers of three special types of permutation binomials. We also briefly discuss the case $q = 2p + 1$ with p and q primes.

1 Introduction

A polynomial $f(x)$ over a finite field $\mathbb{F}_q$ is called a *permutation polynomial* over $\mathbb{F}_q$ if the induced mapping $f : \mathbb{F}_q \to \mathbb{F}_q$ permutes the elements of $\mathbb{F}_q$. Permutation polynomials have been investigated since Hermite [7]. Accounts on these results can be found in Lidl and Niederreiter [13] (Chapter 7), Lidl and Mullen [10, 11], and Mullen [16]. In the last thirty years there has been a revival in the interest for permutation polynomials, in part due to their cryptographic applications; see [9, 12, 20, 21], for example.

In Section 2 we characterize permutation polynomials over a finite field based on their coefficients. This characterization is a variation of Hermite's Criterion ([13], Theorem 7.4).

Permutation binomials of specific types are studied by several authors; see [1, 2, 3, 4, 22, 24], for example. A recent application of permutation binomials for constructing Tuscan-ℓ arrays was given by Chu and Golomb [5]. We use our characterization to study the form and the number of monic permutation binomials over particular finite fields. We

*The second and the third authors are partially funded by NSERC of Canada.

describe monic permutation binomials over $\mathbb{F}_q$, when $q = 2p+1$ (in Section 3), and when $q = 4p + 1$ (in Section 4), where p, q are primes. Then we give a formula for the total number of monic permutation binomials of degree less than $q-1$, for the above values of q. We observe that it is conjectured that there exist infinitely many primes of the form $2p+1$ with p prime (Sophie-Germain primes), and of the form $4p+1$ with p prime [19]. Hence, these are interesting families of finite fields. The arguments we use in both cases are very similar. Since the case $q = 4p + 1$ involves more techniques, we concentrate on this case.

When $q = 4p + 1$, and p, q are primes, the formula mentioned above depends on N_1, N_2 and N_3, which are the numbers of permutation binomials of the form $x(x^p + a)$, $x^3(x^p + a)$ and $x^n(x^{2^i s} + a)$ of degree less than $q - 1$ over $\mathbb{F}_q$, with $a \neq 0$, $i \geq 1$ and $\gcd(s, 2p) = 1$, respectively. We indicate how to compute N_1 and N_2, by using a simple computer program based on Lemma 9. We conjecture that $N_3 = 0$. Finally, we provide the number of monic permutation binomials of a *given* degree m less than $q-1$ over $\mathbb{F}_q$, in terms of N_1, N_2 and $N_{3,m}$, where $N_{3,m}$ is the number of permutation binomials of the form $x^n(x^{2^i s} + a)$ over $\mathbb{F}_q$ with $a \neq 0$, $m = n + 2^i s$, $i \geq 1$ and $\gcd(s, 2p) = 1$. If one proves that $N_3 = 0$ then obviously $N_{3,m} = 0$ for any m less than $q - 1$. We remark that the number of permutation polynomials of a given degree is an open problem in [10]. Das in [6] provides an expression for this number when the finite field $\mathbb{F}_p$ is prime and the degree is $p-2$. In Section 5 we compute some values of N_1, N_2 and N_3, for small values of q, and thus, we obtain the total number of monic permutation binomials for those finite fields. We also briefly comment on some related open problems.

The following identity is used in this paper several times with no reference: if q is a prime, we have $\binom{q-1}{j} \equiv (-1)^j \pmod{q}$ for $j \in \mathbb{Z}$ and $0 \leq j \leq q-1$ ([13], Exercise 1.11).

2 A characterization of permutation polynomials

In this section we assume q is a prime power. The following theorem gives a characterization of permutation polynomials over $\mathbb{F}_q$ based on their coefficients. Our criterion is based on $q-1$ identities involving the coefficients of the polynomial. Without loss of generality, we assume that the degree of the polynomial is less than $q - 1$. We use the convention that $0^0 = 1$.

Theorem 1 *Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in \mathbb{F}_q[x]$ be a polynomial of degree m less than $q-1$. Then, $f(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if*

$$\sum_{(A_1,\ldots,A_m)\in S_N} \frac{N!}{A_1!\cdots A_m!} a_1^{A_1}\cdots a_m^{A_m} = \begin{cases} 0, & \text{if } N = 1,\ldots,q-2, \\ 1, & \text{if } N = q-1, \end{cases}$$

where $S_N = \{(A_1,\ldots,A_m) \in \mathbb{Z}^m\colon A_1 + \cdots + A_m = N, A_1 + 2A_2 + \cdots + mA_m \equiv 0 \pmod{q-1}, A_i \geq 0$ for all $i, 1 \leq i \leq m,$ and $A_i = 0$ whenever $a_i = 0\}$.

Proof. Without loss of generality, we assume $a_0 = 0$. Let $\alpha_0 = 0$, $\alpha_1 = 1, \ldots, \alpha_{q-1}$ be the distinct elements of $\mathbb{F}_q$. Clearly, $f(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q-1})$ are pairwise distinct. Lemma 7.3 in [13] implies that $f(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if

$$\sum_{i=1}^{q-1} f(\alpha_i)^N = \begin{cases} 0, & \text{if } N = 1, \ldots, q-2, \\ -1, & \text{if } N = q-1. \end{cases}$$

Since $f(\alpha_i) = a_1\alpha_i + \cdots + a_m\alpha_i^m$, we calculate

$$\sum_{i=1}^{q-1} f(\alpha_i)^N = \sum_{\substack{A_1+\cdots+A_m=N \\ A_i\in\mathbb{Z}, A_i\geq 0}} \frac{N!}{A_1!\cdots A_m!} a_1^{A_1}\cdots a_m^{A_m} \sum_{i=1}^{q-1} \alpha_i^{A_1+\cdots+mA_m}.$$

We note that if $A_1 + \cdots + mA_m = \ell(q-1) + r$, where $\ell, r \in \mathbb{Z}$, $0 \leq r \leq q-2$, then the distinct choices of α_i imply that

$$\sum_{i=1}^{q-1} \alpha_i^{A_1+\cdots+mA_m} = \sum_{i=1}^{q-1} \alpha_i^r = \begin{cases} -1, & \text{if } r = 0, \\ 0, & \text{if } r = 1, \ldots, q-2. \end{cases}$$

Hence,

$$\begin{aligned} \sum_{i=1}^{q-1} f(\alpha_i)^N &= \sum_{\substack{A_1+\cdots+A_m=N \\ A_1+\cdots+mA_m\equiv 0 \pmod{q-1} \\ A_i\in\mathbb{Z}, A_i\geq 0}} (-1)\frac{N!}{A_1!\cdots A_m!} a_1^{A_1}\cdots a_m^{A_m} \\ &= \begin{cases} 0, & \text{if } N = 1, \ldots, q-2, \\ -1, & \text{if } N = q-1. \end{cases} \end{aligned}$$

■

We remark that in S_N if $A_1 + 2A_2 + \cdots + mA_m = \ell(q-1)$ for some integer ℓ, then $1 \leq \ell \leq N$.

The above theorem is a generalization of a theorem by London and Ziegler [14], for prime finite fields. It provides a simple method for permutation binomial testing over $\mathbb{F}_q$. In this paper, by permutation binomial, we mean a monic polynomial of the form $x^m + ax^n$ where $a \neq 0$ and $0 < n < m < q-1$.

Corollary 2 *Let $f(x) = x^m + ax^n \in \mathbb{F}_q[x]$ with $a \neq 0$, $q \geq 3$ and $0 < n < m < q-1$. Then, $f(x)$ is a permutation binomial over $\mathbb{F}_q$ if and only if*

$$\sum_{A\in S_N} \binom{N}{A} a^{N-A} = \begin{cases} 0, & \text{if } N = 1, \ldots, q-2, \\ 1, & \text{if } N = q-1, \end{cases}$$

where

$$S_N = \left\{ A \in \mathbb{Z} \colon A = \frac{\ell(q-1) - nN}{m-n} \text{ where } \ell \in \mathbb{Z} \text{ and } 0 \leq A \leq N \right\}.$$

A consequence of Corollary 2 is that permutation binomials do not exist over some finite fields.

Corollary 3 *If $q-1$ is a Mersenne prime, then there is no permutation binomial with degree less than $q-1$ over $\mathbb{F}_q$.*

Proof. Suppose that $f(x) = x^m + ax^n$ is a permutation binomial over $\mathbb{F}_q$ where $a \neq 0$, $0 < n < m < q-1$ and $q-1$ is a Mersenne prime. It follows from Corollary 2 that, for $N = q-1$, the only possible integer values of $A = \frac{(\ell-n)(q-1)}{m-n}$ are 0 and $q-1$. Thus, $\binom{q-1}{0}a^{q-1} + \binom{q-1}{q-1}a^0 = 2 \neq 1$. ■

For example, there is no permutation binomial over $\mathbb{F}_3, \mathbb{F}_8, \mathbb{F}_{32}, \mathbb{F}_{128}, \mathbb{F}_{8192}, \ldots$.

Now we use Corollary 2 to obtain a result on the non-existence of certain permutation binomials over prime finite fields $\mathbb{F}_{2^k r+1}$, where $k \geq 1$ and r is an odd integer greater than 1.

Lemma 4 *Let $q = 2^k r + 1$ where q is prime, r is an odd integer greater than 1 and $k \geq 1$. There is no permutation binomial over $\mathbb{F}_q$ of the form $x^m + ax^n$ with $a \neq 0$, $0 < n < m < q-1$, $m - n = 2^i s$, i an integer ≥ 1, s an odd integer, $\gcd(s, r) = 1$, in the following two situations:*
(i) $1 \leq i < k$ and $m \leq 2^{k-i} r$,
(ii) $k < i$ and $m \leq r$.

Proof. (i) Suppose we have a permutation binomial $x^m + ax^n$ with $m - n = 2^i s$ and $1 \leq i < k$, s an odd integer such that $\gcd(s, r) = 1$ and $m \leq 2^{k-i} r$. Let us consider $N = st_0 < q-1$ where t_0 is a positive integer of the form $2^i d$. We investigate the possible integer values of $A = \frac{2^k r\ell - nN}{2^i s}$ such that $0 \leq A \leq N$. Since $\gcd(s, 2r) = 1$, we look for all possible multiples of $2^k rs$ within the interval $I = [nst_0, st_0(n + 2^i s)]$. Let d be the smallest positive integer such that the interval I contains a multiple of $2^k rs$. In order to prove the existence of such d, we consider two cases.

- If $s = 1$, let $d = 2^{k-i-1} r$. Then $d > 1$, $N = 2^{k-1} r < q-1$, and the length $|I| = 2^i t_0 = 2^{2i} d = 2^{k+i-1} r \geq 2^k r$. Hence I contains a multiple of $2^k r$.
- If $s > 1$, let $d = \lfloor \frac{2^{k-i} r}{s} \rfloor$. We note that $d \geq 1$; otherwise, we would have $q - 1 = 2^k r < 2^i s = m - n$. Moreover, $N = 2^i ds < 2^k r = q-1$. Since $t_0 \geq 2d > \frac{2^{k-i} r}{s}$, we also deduce that $|I| = 2^i s^2 t_0 > 2^k rs$.

In any event suppose $2^k rs\ell_0$ is the least such multiple in I, and let $A_0 = \frac{2^k rs\ell_0 - nN}{2^i s}$. We claim that there is no other multiple of $2^k rs$ in I. In fact, if there were two multiples of $2^k rs$ in I then $2^k rs(\ell_0 + 1) \leq st_0(n + 2^i s)$, i.e.

$$2^k r(\ell_0 + 1) \leq t_0 m. \tag{1}$$

If $d = 1$ then, by using that $m \leq 2^{k-i} r$, we obtain

$$t_0 m = 2^i m < 2^i m + 2^k r\ell_0 < 2^k r(\ell_0 + 1),$$

which is a contradiction to (1). So we can assume that $d > 1$. Let $N' = N - 2^i s$. Then $1 \le N' < q-1$, and

$$A' = \frac{2^k rs\ell_0 - nN'}{2^i s} = A_0 + n \tag{2}$$

is an integer. The minimality of d and the conditions on Corollary 2 imply that $N' < A_0 + n$. In this case we get from (2) that

$$t_0 m < 2^k r\ell_0 + 2^i m.$$

The hypothesis $m \le 2^{k-i} r$ leads to $t_0 m < 2^k r(\ell_0 + 1)$ contradicting (1).

(ii) Now let us suppose $x^m + ax^n$ is a permutation binomial with $m - n = 2^i s$, $k < i$, $m \le r$ and s an odd integer such that $\gcd(s, r) = 1$. We write $m - n = 2^{k+j} s$ with $j \ge 1$. So $m - n < q - 1$ implies that $2^j s < r$. Let us consider $N = st_0 < q - 1$ with t_0 of the form $2^{k+j} d$, for some positive integer d. We investigate the possible integer values of $A = \frac{2^k r\ell - nN}{2^{k+j} s}$ such that $0 \le A \le N$. Since $\gcd(s, 2r) = 1$, we look for all possible multiples of $2^{k+j} rs$ within the interval $I = [nst_0, st_0(n + 2^{k+j} s)]$. Let d be the smallest positive integer such that the interval I contains a multiple of $2^{k+j} rs$. Such a d exists. Indeed, we can choose $d = \lfloor \frac{r}{2^j s} \rfloor$. We note that $d \ge 2$, because $m - n = 2^{k+j} s < m \le r$ implies that $2 \le 2^k \le \frac{r}{2^j s}$. Moreover, $N = 2^{k+j} ds < \frac{2^{k+j} rs}{2^j s} = q - 1$. Since $t_0 \ge 2d > \frac{r}{2^j s}$, we deduce that the length of I is

$$\begin{aligned} |I| = 2^{2(k+j)} s^2 d &\ge 2^{(1+j)+(k+j)} s^2 d = 2d(2^{k+2j} s^2) \\ &> \frac{r}{2^j s}(2^{k+2j} s^2) = 2^{k+j} rs. \end{aligned}$$

Thus there is a multiple of $2^{k+j} rs$ in I. Suppose $2^{k+j} rs\ell_0$ is the least such multiple in I, and let $A_0 = \frac{2^{k+j} rs\ell_0 - nN}{2^{k+j} s}$. We claim that there is no other multiple of $2^{k+j} rs$ in I. In fact, if there were two multiples of $2^{k+j} rs$ in I then $2^{k+j} rs(\ell_0 + 1) \le st_0(n + 2^{k+j} s)$, i.e.

$$2^{k+j} r(\ell_0 + 1) \le t_0 m. \tag{3}$$

If $d = 1$ then, by using that $m \le r$, we obtain

$$t_0 m = 2^{k+j} m < 2^{k+j} m + 2^{k+j} r\ell_0 < 2^{k+j} r(\ell_0 + 1),$$

which is a contradiction to (3). So we can assume that $d > 1$. Let $N' = N - 2^{k+j} s$. Then we have $1 \le N' < q - 1$ and

$$A' = \frac{2^{k+j} rs\ell_0 - nN'}{2^{k+j} s} = A_0 + n \tag{4}$$

is an integer. The minimality of d and the conditions on Corollary 2 imply that $N' < A_0 + n$. In this case we get from (4) that

$$t_0 m < 2^{k+j} r\ell_0 + 2^{k+j} m.$$

The hypothesis $m \le r$ leads to $t_0 m < 2^{k+j} r(\ell_0 + 1)$ which is a contradiction to (3). ■

We note that if either $1 \le i < k$ and $m > 2^{k-i} r$, or $k = i$, or $k < i$ and $m > r$, then permutation binomials over $\mathbb{F}_q$ may exist. As an example, in $\mathbb{F}_{97}[x]$, there are permutations binomials such as $x^{35} + 3x^3$ and $x^{65} + 93x$ showing that it is possible to have $m - n$ equals 32 and 64.

3 Permutation binomials over $\mathbb{F}_{2p+1}$ where p and $2p+1$ are primes

In this section, we briefly discuss the following result concerning permutation binomials over $\mathbb{F}_q$ where $q = 2p+1$, and p, q are primes. We note that other descriptions of permutation binomials over those fields when $p \mid m-n$ can be found in [17] and [23].

Proposition 5 *Suppose $q = 2p+1$ where p and q are odd primes. Then, any monic permutation binomial of degree less than $q-1$ over $\mathbb{F}_q$ with $p \mid m-n$ is of the form $x^{2j+1}(x^p+a)$ or $x^{2j}(x^p+a^{-1})$, where $a^2 \neq 1$ and a satisfies $\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{p-2k-1} = 0$. Moreover, let M be the number of permutation binomials of the form $x^n(x^{2^i s}+a)$ with $a \neq 0$, $0 < n < n+2^i s < q-1$, $\gcd(s,2p) = 1$, and either $i = 1$, or $i > 1$ and $p < n+2^i s < 2p$. The number of monic permutation binomials with degree less than $q-1$ over $\mathbb{F}_q$ is $(p-1)^2 + M$.*

Proof. Let us assume that $x^n(x^p+a)$ is a permutation binomial over $\mathbb{F}_q$ with $a \neq 0$ and $0 < n < p$. There are $p-1$ possible values for n. We consider all possible integer solutions of $A = \frac{2p\ell - nN}{p}$ within the range from 0 to N, for each $1 \leq N \leq 2p$. We have that A is an integer if and only if $p \mid N$. Thus, it is enough to consider $N = p$ and $2p$.

We start with $N = 2p$. In this case, $A = 2(\ell - n)$ consists of all even numbers from 0 to $2p$. Thus,

$$\sum_{k=0}^{p}\binom{2p}{2k}a^{2(p-k)} = 1.$$

Since $\binom{2p}{2k} = 1$, we have that $\sum_{k=0}^{p} a^{2(p-k)} = 1$, which is equivalent to $a^2 \neq 1$.

When $N = p$, $A = 2\ell - n$. Clearly, if n is odd (respectively, even) then A is odd (respectively, even). So, we have

$$\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{p-2k-1} = 0 \quad \text{for } n \text{ odd}, \tag{5}$$

and

$$\sum_{k=0}^{(p-1)/2}\binom{p}{2k}a^{p-2k} = 0 \quad \text{for } n \text{ even}. \tag{6}$$

Since $a \neq -1$, if a satisfies (5) then a does not satisfy (6). However, a^{-1} satisfies (6), because

$$\begin{aligned}\sum_{k=0}^{(p-1)/2}\binom{p}{2k}(a^{-1})^{p-2k} &= a^{-p}\sum_{k=0}^{(p-1)/2}\binom{p}{p-2k}a^{2k}\\ &= a^{-p}\sum_{k=0}^{(p-1)/2}\binom{p}{2k+1}a^{p-2k-1} = 0.\end{aligned}$$

Conversely, if a satisfies (6) then a does not satisfy (5), but a^{-1} satisfies (5). Since $(1+a)^p = \pm 1$ and $(1-a)^p = \pm 1$, we have either

$$(1+a)^p - (1-a)^p = 0 \quad \text{or} \quad (1+a)^p + (1-a)^p = 0.$$

Hence, there are $p-1$ nonzero a's satisfying (5) or (6) for each n. The number of monic permutation binomials of degree less than $q-1$ over $\mathbb{F}_q$, when $m-n=p$, is $(p-1)^2$. The rest of the proof is obtained from the fact that $\gcd(m-n, q-1) = 1$ [15] and Lemma 4. ■

An exhaustive search based on Corollary 2 for small values of $q = 2p+1$ with p, q primes indicates that M is zero.

4 Permutation binomials over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes

In this section we concentrate on the case $q = 4p+1$ with p, q primes. We use Corollary 2 repeatedly with no reference.

Lemma 6 *Let $q = 4p+1$ where p and q are primes. There is no permutation binomial over $\mathbb{F}_q$ of the form $x^m + ax^n$ with $a \neq 0$, $0 < n < m < q-1$ and $m-n=2$.*

Proof. Suppose such permutation binomial exists. We observe that n must be odd; otherwise, we would have m and n even. Let $N = 2p$. Then $A = p(2\ell - n)$ is a multiple of p. Since $0 \leq A \leq 2p$, the only possibility for A is p. In this case we must have $\binom{2p}{p} a^p = 0$ contradicting that $a \neq 0$. ■

Lemma 7 *Let $q = 4p+1$ where p and q are primes. There is no permutation binomial over $\mathbb{F}_q$ of the form $x^m + ax^n$ with $a \neq 0$, $0 < n < m < q-1$ and $m-n = 2s$, where s is odd and $p < s < 2p$.*

Proof. Suppose such permutation binomial over $\mathbb{F}_q$ exists. Let $N = 2s$. So $N < 4p$ and $A = \frac{2p\ell}{s} - n$. The conditions on s imply that A is an integer if and only if ℓ is a multiple of s. Suppose $\ell = s\overline{\ell}$. Since $1 \leq \ell \leq N$, $\overline{\ell}$ must be 1 or 2. On the other hand, the condition $0 \leq A \leq N$ implies that $\frac{n}{2p} \leq \overline{\ell} \leq \frac{2s+n}{2p}$. Let I be the interval $(\frac{n}{2p}, \frac{2s+n}{2p})$. The length of I is $\frac{s}{p}$. Since $p < s < 2p$, we have that $1 < \frac{s}{p} < 2$. Furthermore, we notice that $n = m - 2s < 4p - 2p = 2p$. Thus, $\frac{n}{2p} < 1 < \frac{2s+n}{2p} < 2$, and $\overline{\ell} = 1$. Hence, I contains only one integer A such that $0 \leq A \leq N$. Thus, $\binom{2s}{A} a^{2s-A} = 0$ contradicting that $a \neq 0$. ■

By combining the fact that $\gcd(m-n, q-1) \neq 1$ [15] and Lemmas 4, 6, and 7, we now summarize the possible values of $m-n$.

Proposition 8 *Let $q = 4p + 1$ where p and q are primes. If $x^m + ax^n$ is a permutation binomial over $\mathbb{F}_q$ with $a \neq 0$ and $0 < n < m < q - 1$, then the possible values of $m - n$ are*

$$m - n = \begin{cases} 2s; & \text{where } s > 1, (s, 2p) = 1, \text{ and } 2p < m < n + 2p, \\ 4s; & \text{where } (s, 2p) = 1, \\ 2^i s; & \text{where } i > 2, (s, 2p) = 1, \text{ and } m > p, \\ cp, & \text{if } c = 1, 2 \text{ or } 3. \end{cases}$$

Next we analyze the case when p divides $m - n$.

Lemma 9 *Suppose $q = 4p + 1$ where p and q are primes. If $f(x) = x^m + ax^n$ is a permutation binomial over $\mathbb{F}_q$ with $a \neq 0$, $0 < n < m < q - 1$ and $p \mid m - n$, then $f(x)$ has one of the following forms:*

(1) $x^j(x^p + a)$, *where $0 < j < 3p$, a is such that $a^4 \neq 1$ and, for each $1 \leq c \leq 3$,*

$$\sum_{t=\lceil cj/4 \rceil}^{\lfloor c(p+j)/4 \rfloor} \binom{cp}{4t - cj} a^{c(p+j)-4t} = 0;$$

(2) $x^{2j+1}(x^{2p} + a)$, *where $0 \leq j < p$, a is such that $a^2 \neq 1$ and*

$$\sum_{t=0}^{p-1} \binom{2p}{2t + 1} a^{2(p-t)-1} = 0;$$

(3) $x^j(x^{3p} + a)$, *where $0 < j < p$, a is such that $a^4 \neq 1$ and, for each $1 \leq c \leq 3$,*

$$\sum_{t=\lceil -cj/4 \rceil}^{\lfloor c(p-j)/4 \rfloor} \binom{cp}{4t + cj} a^{c(p-j)-4t} = 0.$$

Proof. The possible values for $m - n$ are p, $2p$ and $3p$. In each case, A is an integer only if $p \mid N$. Cases 1 and 3 follow immediately from Corollary 2 by analyzing the possible values of A.

Suppose $m - n = 2p$. If n is even then m is even, and in this case $f(x)$ is not a permutation binomial. Thus, n must be odd. This eliminates the cases $N = p$ and $N = 3p$, as there is no integer $A = \frac{4p\ell - nN}{2p}$. If $N = 4p$, we get

$$\sum_{t=0}^{2p} \binom{4p}{2t} a^{4p-2t} = 1,$$

which implies $a^2 \neq 1$. If $N = 2p$, then $A = 2\ell - n$ is odd. Hence, we have the condition $\sum_{t=0}^{p-1} \binom{2p}{2t + 1} a^{2(p-t)-1} = 0.$ ■

After this research was done, we learned that Park in [18] has proved a more general version of Lemma 9. His proof is a direct application of Hermite's Criterion while ours is based on Corollary 2.

The next lemma will be essential for the purpose of counting.

Lemma 10 *Let $q = 4p+1$ where p and q are primes, $p > 3$, n be an odd positive integer with $n \equiv i \pmod 4$, $a \neq 0$, and $c = 1$, 2 or 3. If $\gcd(n, q-1) = 1$ then $f(x) = x^n(x^{cp}+a)$ is a permutation binomial over $\mathbb{F}_q$ if and only if $g(x) = x^i(x^{cp}+a)$ is a permutation binomial over $\mathbb{F}_q$. If $\gcd(n, q-1) \neq 1$, then there is no permutation binomial of the form $x^n(x^p+a)$.*

Proof. Suppose that $\gcd(n, q-1) = 1$ and $f(x)$ is a permutation binomial over $\mathbb{F}_q$. Let us prove that $g(x)$ is onto. For $s \in \mathbb{F}_q^*$ fixed, there exists $r \in \mathbb{F}_q^*$ such that $f(r) = s$. We recall that $i = 1$ or 3, and $p \neq 3$. Hence x^i is a permutation monomial over $\mathbb{F}_q$. Let $t \in \mathbb{F}_q^*$ be such that $t^i = r^n$. We claim that $t^{cp} = r^{cp}$. In fact, if $n - i = 4k$ for some integer k then $r^{(n-i)cp} = r^{4kcp} = 1$. Thus, $r^{cpn} = r^{cpi}$, and $t^{cpi} = r^{cpi}$ implies that $t^{cp} = r^{cp}$. Hence, $g(t) = s$, i.e. $g(x)$ is a permutation binomial over $\mathbb{F}_q$. The proof of the converse part follows similarly.

When $\gcd(n, q-1) \neq 1$, p divides n, since n is odd. Furthermore, the degree of the binomial is smaller than $4p$. So, n must be p. But, if $x^p(x^p+a)$ is a permutation binomial over $\mathbb{F}_q$, then so is $y^2 + ay$. This is a contradiction. ■

It is convenient to establish the following notation.

Definition 11 *Let $q = 4p+1$ with p, q primes. Two binomials $x^{4k+i}(x^d+a)$ and $x^{4k+j}(x^d+a^{-1})$ are said to be* paired permutation binomials *over $\mathbb{F}_q$, when $x^{4k+i}(x^d+a)$ is a permutation binomial over $\mathbb{F}_q$ if and only if $x^{4k+j}(x^d+a^{-1})$ is a permutation binomial over $\mathbb{F}_q$. In this case, we denote the paired permutation binomials by (i, j, d).*

The following theorem entails that, when p divides $m - n$, all permutation binomials occur in pairs over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes.

Theorem 12 *Let $q = 4p+1$ where p and q are primes. The following are paired permutation binomials over $\mathbb{F}_q$:*

(i) $(1,2,p)$, $(3,4,p)$, $(1,4,3p)$, $(2,3,3p)$, *if* $p \equiv 1 \pmod 4$*;*

(ii) $(1,4,p)$, $(2,3,p)$, $(1,2,3p)$, $(3,4,3p)$, *if* $p \equiv -1 \pmod 4$*;*

(iii) $(1,3,2p)$.

Moreover, all permutation binomials $x^m + ax^n$ over $\mathbb{F}_q$ with $p \mid m-n$ are described as one of the above types.

Proof. We first show in detail the cases (i) $(1,2,p)$ and (i) $(1,4,3p)$, since they are representatives of the technique used to prove the remaining cases in (i) and (ii). Then we prove (iii). Let us assume $p=4u+1$ for some positive integer u, and use Lemma 9. It is enough to consider $N=cp$ with $1\le c\le 4$. For $N=4p$, the equation on a reduces to the condition that $a^4\neq 1$. This is clearly equivalent to $(a^{-1})^4\neq 1$. Now, we fix c with $1\le c\le 3$.

Let us prove (i) $(1,2,p)$. We have $A=4\ell-nc$, and the range $0\le A\le cp$ implies that $\ell=c(k+1),\dots,c(k+u)$, for $n=4k+1$ and $n=4k+2$. We show that

$$\sum_{\ell=c(k+1)}^{c(k+u)}\binom{cp}{4\ell-c(4k+1)}a^{c(p+4k+1)-4\ell}=0$$

if and only if

$$\sum_{\ell=c(k+1)}^{c(k+u)}\binom{cp}{4\ell-c(4k+2)}(a^{-1})^{c(p+4k+2)-4\ell}=0.$$

In fact,

$$\begin{aligned}
&\sum_{\ell=c(k+1)}^{c(k+u)}\binom{cp}{4\ell-c(4k+2)}(a^{-1})^{c(p+4k+2)-4\ell}\\
=\;& a^{-cp}\sum_{\ell=c(k+1)}^{c(k+u)}\binom{cp}{4\ell-c(4k+2)}a^{4\ell-c(4k+2)}\\
=\;& a^{-cp}\sum_{\ell=c(k+1)}^{c(k+u)}\binom{cp}{4\ell-c(4k+1)}a^{c(p+4k+1)-4\ell},
\end{aligned}$$

where the last expression is obtained by changing the variable ℓ by $c(2k+1+u)-\ell$. The desired result follows as $a\neq 0$.

Next, let us prove (i) $(1,4,3p)$. By Lemma 9, we show that

$$\sum_{t=-ck}^{c(u-k)}\binom{cp}{4t+c(4k+1)}a^{c(p-4k-1)-4t}=0$$

if and only if

$$\sum_{t=-c(k+1)}^{c(u-k-1)}\binom{cp}{4t+c(4k+4)}(a^{-1})^{c(p-4k-4)-4t}=0.$$

This is equivalent to show that

$$\sum_{i=0}^{cu}\binom{cp}{4i+c}a^{c(p-1)-4i}=0\quad\Longleftrightarrow\quad\sum_{i=0}^{cu}\binom{cp}{4i}(a^{-1})^{cp-4i}=0.$$

By doing the change of variables i by $uc - i$, we obtain

$$\begin{aligned}\sum_{i=0}^{cu} \binom{cp}{4i} (a^{-1})^{cp-4i} &= a^{-cp} \sum_{i=0}^{cu} \binom{cp}{cp-4i} a^{4i} \\ &= a^{-cp} \sum_{i=0}^{cu} \binom{cp}{4i+c} a^{c(p-1)-4i}.\end{aligned}$$

Again, as $a \neq 0$, we are done.

Finally we show (iii). We observe that $A = \frac{4p\ell - nN}{2p}$ is an integer if and only if N is even. The case $N = 4p$ reduces to the trivial fact that $a^2 \neq 1$ is equivalent to $(a^{-1})^2 \neq 1$. For $N = 2p$, we need to prove that $\sum_{t=0}^{p-1} \binom{2p}{2t+1} a^{2(p-t)-1} = 0$ if and only if $\sum_{t=0}^{p-1} \binom{2p}{2t+1} (a^{-1})^{2(p-t)-1} = 0$. Indeed, this follows from

$$\begin{aligned}(1+a)^{2p} - (1-a)^{2p} = 0 \iff& (a^{-1}+1)^{2p} - (a^{-1}-1)^{2p} = 0 \\ \iff& (1+a^{-1})^{2p} - (1-a^{-1})^{2p} = 0.\end{aligned}$$

■

Theorem 12 reduces the problem of counting all monic permutation binomials of degree up to $q-1$ over $\mathbb{F}_q$ to the counting of three specific types of permutation binomials, as shown in the next theorem.

Theorem 13 *Suppose $q = 4p+1$ where $p > 3$ and q are primes. Let N_1 and N_2 be the numbers of permutation binomials over $\mathbb{F}_q$ of the form $x(x^p + a)$ and $x^3(x^p + a)$ of degree less than $q-1$, respectively, where $a \neq 0$. Let N_3 be the number of permutation binomials over $\mathbb{F}_q$ of the form $x^n(x^{2^i s} + a)$ with degree less than $q-1$, $i \geq 1$, $\gcd(s, 2p) = 1$ and $a \neq 0$. The total number of monic permutation binomials over $\mathbb{F}_q$ of degree less than $q-1$ is $2(p-1)(p-1+N_1+N_2)+N_3$.*

Proof. We prove the case $p \equiv 1 \pmod 4$, and the other case follows in a similar fashion. Suppose $p = 4u+1$ for some positive integer u. When $p \mid (m-n)$, we partition the permutation binomials that we want to count into three disjoint groups according to Theorem 12. The number of binomials in each one of these groups provides one term appearing in $2(p-1)(p-1+N_1+N_2)$. With respect to N_3, Proposition 8 contains details about which permutation binomials may contribute to N_3 exactly.

Let the first group be formed by permutation binomials of the form $x^{2i+1}(x^{2p}+a)$ with $i \geq 0$. Since these polynomials must have degree less than $4p$, and $x^p(x^{2p}+a)$ is not a permutation binomial over $\mathbb{F}_q$, we have $p-1$ possible values for i. By Theorem 12, we have that each permutation binomial $x^{4k+1}(x^{2p}+a)$ is associated to the permutation binomial $x^{4k+3}(x^{2p}+a^{-1})$. Hence, according to Lemma 10, it is enough to count the number of permutation binomials of the form $x(x^{2p}+a)$. To do this, we notice that the equation $x^{2p} = 1$ has $2p$ solutions, including ± 1. Furthermore, since $a \neq \pm 1$ and $\frac{1+a}{1-a} \neq \pm 1$, the equation

$$\left(\frac{1+a}{1-a}\right)^{2p} = 1$$

has exactly $2p-2$ solutions. This equation is equivalent to $(1+a)^{2p}-(1-a)^{2p}=0$, that is,

$$\sum_{t=0}^{p-1}\binom{2p}{2t+1}a^{2(p-t)-1}=0.$$

By Lemma 9, we conclude that there are $2p-2$ permutation binomials of the form $x(x^{2p}+a)$, and thus, there are $2(p-1)^2$ permutation binomials in the first group.

The second group consists of permutation binomials of the forms $x^{4k+1}(x^p+a)$, $x^{4k+2}(x^p+a^{-1})$, $x^{4\ell+3}(x^{3p}+a)$, and $x^{4\ell+2}(x^{3p}+a^{-1})$. They are all associated to $x(x^p+a)$. This correspondence is due to Lemma 10, Theorem 12, and the fact that $x^{4\ell+3}(x^{3p}+a)$ is a composition of $x^{4k+1}(x^p+a)$ and x^3. Taking into account that we are only considering binomials of degree less than $4p$, and that there is no permutation binomial of the form $x^p(x^p+a)$ over $\mathbb{F}_q$, it is clear that the number of such possible k's is $3u$, and that the number of such possible ℓ's is u. Hence, we have $2N_1(p-1)$ as the total of permutation binomials in the second group.

The third group is formed by permutation binomials of the forms $x^{4k+3}(x^p+a)$, $x^{4k+4}(x^p+a^{-1})$, $x^{4\ell+1}(x^{3p}+a)$, and $x^{4\ell+4}(x^{3p}+a^{-1})$. They are all associated to $x^3(x^p+a)$. By similar arguments, this group has a total of $2N_2(p-1)$ permutation binomials. ■

In Section 5 we present some values of N_1, N_2 and N_3. The outputs lead us to conjecture that $N_3=0$ for any finite field $\mathbb{F}_q$ with $q=4p+1$ and p, q primes.

Another application of Theorem 12 provides the number of monic permutation binomials of a *given degree* m over $\mathbb{F}_q$ in terms of N_1, N_2 and another amount to be defined as $N_{3,m}$.

Theorem 14 *Let $q=4p+1$ where $p>3$ and q are primes. Let N_1 and N_2 be the numbers of permutation binomials of the form $x(x^p+a)$ and $x^3(x^p+a)$ of degree less than $q-1$, respectively, where $a\neq 0$. Let $N_{3,m}$ be the number of permutation binomials over $\mathbb{F}_q$ of the form $x^n(x^{2^is}+a)$ with degree m less than $q-1$, $\gcd(s,2p)=1$, $i\geq 1$ and $a\neq 0$. If $p\mid(m-n)$ and $m=p$, $2p$ or $3p$, then there is no permutation binomial of degree m over $\mathbb{F}_q$. For each other value of m, the number of monic permutation binomials of degree m over $\mathbb{F}_q$ is the sum of $N_{3,m}$ and the corresponding entry in the following table:*

(1) If $p<m<2p$ then

(mod 4)	$m\equiv 1$	$m\equiv 2$	$m\equiv 3$	$m\equiv 4$
$p\equiv 1$	N_2	N_1	N_1	N_2
$p\equiv -1$	N_2	N_2	N_1	N_1

(2) If $2p<m<3p$ then

(mod 4)	$m\equiv 1$	$m\equiv 2$	$m\equiv 3$	$m\equiv 4$
$p\equiv 1$	$2(p-1)+N_2$	N_1	$2(p-1)+N_1$	N_2
$p\equiv -1$	$2(p-1)+N_2$	N_2	$2(p-1)+N_1$	N_1

(3) If $3p < m < 4p$ then

(mod 4)	$m \equiv 1$	$m \equiv 2$	$m \equiv 3$	$m \equiv 4$
$p \equiv 1$	$2(p-1) + N_1 + N_2$	$2N_1$	$2(p-1) + N_1 + N_2$	$2N_2$
$p \equiv -1$	$2(p-1) + N_1 + N_2$	$2N_2$	$2(p-1) + N_1 + N_2$	$2N_1$

Proof. We only prove one of the cases since the proofs of the remaining cases are similar. Suppose $3p < m < 4p$ with $p \equiv 1 \pmod 4$ and $m \equiv 1 \pmod 4$. There are three types of monic permutation binomials of degree m over $\mathbb{F}_q$, namely, $x^{m-p}(x^p + a)$, $x^{m-2p}(x^{2p}+a)$, and $x^{m-3p}(x^{3p}+a)$. By Lemma 9 or the proof of Theorem 13, the number of permutation binomials of second type is $2(p-1)$. We use Lemma 10 and Theorem 12 to count the number of permutation binomials for the other types. For the first one, since $m - p \equiv 4 \pmod 4$, the number of such permutation binomials is N_2. The number of permutation binomials of the third type is N_1, as $m - 3p \equiv 2 \pmod 4$. Therefore, the number of permutation binomials of degree m over $\mathbb{F}_q$ is $2(p-1) + N_1 + N_2 + N_{3,m}$. ■

We should emphasize again that it might be that $N_{3,m} = 0$ for each m less than $q-1$.

5 Conclusions

In this section we discuss some problems for further research. The following table gives some values of N_1, N_2 and N_3, which are defined in Theorem 13, and thus the total number of monic permutation binomials of degree less than $q-1$ over $\mathbb{F}_q$, for each q less than 1000 of the form $4p+1$, where p and q are primes. The amounts N_1 and N_2 are easily obtained by using a simple and efficient computer program implied by Lemma 9. Unfortunately they do not seem to suggest a general formula. We observe that from Lemma 9 it is also easy to see that N_1 and N_2 are multiples of 4, and that a trivial upper bound for both of them is $p-2$, if $p \equiv 1 \pmod 4$, and p, if $p \equiv -1 \pmod 4$. Although we do not have enough information about N_3, the data strongly suggest that it might be zero (similarly, M might be zero too for the case $2p+1$). It would be interesting to obtain a closed formula for N_1, N_2 and N_3. In this case, Theorem 13 would provide an exact formula for the number of monic permutation binomials of degree up to $q-1$ over $\mathbb{F}_q$, for $q = 4p+1$ and p, q primes. Similarly, we would obtain an exact formula for the number of monic permutation binomials of a given degree up to $q-1$ over $\mathbb{F}_q$ for $q = 4p+1$, and p, q primes, using Theorem 14.

In the following table the total number of permutation binomials was computed in two different ways. On the one hand we used Theorem 13 and the computations of N_1, N_2 and N_3 commented above. On the other hand we did an exhaustive search of permutation binomials for those finite fields.

There are some other natural extensions of this work such as the characterization and counting of permutation binomials over $\mathbb{F}_q$ with $q = 2^k p + 1$, $k \geq 3$, and p, q primes; the study of permutation binomials over an arbitrary prime and a non-prime field, and permutation trinomials over a finite field (see [8]). For these problems, Theorem 1 can be an important tool as well as several techniques in this paper.

q	p	N_1	N_2	N_3	Total
13	3	0	0	0	8
29	7	4	0	0	120
53	13	0	4	0	384
149	37	16	16	0	4896
173	43	20	20	0	6888
269	67	36	24	0	16632
293	73	28	28	0	18432
317	79	12	32	0	19032
389	97	48	36	0	34560
509	127	40	40	0	51912
557	139	56	32	0	62376
653	163	52	72	0	92664
773	193	64	60	0	121344
797	199	72	88	0	141768

Acknowledgments

The authors would like to thank the referee for many helpful comments.

References

[1] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proceedings of the American Mathematical Society* **134** (2006), no 1, 15-22.

[2] A. Akbary and Q. Wang, On some permutation polynomials over finite fields, *International Journal of Mathematics and Mathematical Sciences* **16** (2005), 2631-2640.

[3] L. Carlitz, Some theorems on permutation polynomials, *Bulletin of the American Mathematical Society* **68** (1962), 120-122.

[4] W. Chou, Binomial permutations of finite fields, *Bulletin of the Australian Mathematical Society* **38** (1988), 325-327.

[5] W. Chu and S. W. Golomb, Circular Tuscan-k arrays from permutation binomials, *Journal of Combinatorial Theory (Series A)* **97** (2002), 195-202.

[6] P. Das, The number of permutation polynomials of a given degree over a finite field, *Finite Fields and Their Applications* **8** (2002), 1-13.

[7] C. Hermite, Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris, **57** (1863), 750-757; *Oeuvres*, vol. 2, 280-288, Gauthier-Villars, Paris, 1908.

[8] J. B. Lee and Y. H. Park, Some permuting trinomials over finite fields, *Acta Mathematica Scientia (English Ed.)* **17** (1997), 250-254.

[9] J. Levine and J. V. Brawley, Some cryptographic applications of permutation polynomials, *Cryptologia* **1** (1977), 76-92.

[10] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *American Mathematical Monthly* **95** (1988), 243-246.

[11] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *American Mathematical Monthly* **100** (1993), 71-74.

[12] R. Lidl and W. B. Müller, Permutation polynomials in RSA-cryptosystems, *Proc. CRYPTO 83*, (D. Chaum Ed.), 293-301, Plenum, New York, 1984

[13] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge University Press, 1997.

[14] D. London and Z. Ziegler, Functions over the residue field modulo a prime, *Journal of the Australian Mathematical Society* **7** (1967), 410-416.

[15] R. Mollin and C. Small, On permutation polynomials over finite fields, *International Journal of Mathematics and Mathematical Sciences* **10** (1987), 535-543.

[16] G. L. Mullen, Permutation polynomials over finite fields, *Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, NV, 1991)*, 131-151, Lecture Notes in Pure and Appl. Math., **141**, Dekker, New York, 1993.

[17] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *Journal of the Australian Mathematical Society (Series A)* **33** (1982), 197-212.

[18] H. G. Park, On certain binomials over a finite field, *Journal of Applied Mathematics and Computing* **18** (2005), 679-684.

[19] P. Ribenboim, "The Book of Prime Number Records", Springer-Verlag, 1988.

[20] R. L. Rivest, Permutation polynomials modulo 2^w, *Finite Fields and Their Applications* **7** (2001), 287-292.

[21] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, The RC6 block cipher, *available on-line at* http://theory.lcs.mit.edu/∼rivest/rc6.pdf

[22] D. Wan, Permutation polynomials over finite fields, *Acta Mathematica Sinica (New Series)* **3** (1987), 1-5.

[23] D. Wan, Permutation binomials over finite fields, *Acta Mathematica Sinica (New Series)* **10** (1994), 30-35.

[24] L. Wang, On permutation polynomials, *Finite Fields and Their Applications* **8** (2002), 311-322.