EXPLICIT CLASSES OF PERMUTATION AND COMPLETE PERMUTATION POLYNOMIALS OVER FINITE FIELDS

Abdelmejid Bayad, Belhout Bousalmi, Abdallah Derbal

Advanced Studies in Contemporary Mathematics
31 (2021), No. 1, pp. 89 – 98

www.jangjeon.or.kr
http://dx.doi.org/10.17777/ascm2021.31.1.89

EXPLICIT CLASSES OF PERMUTATION AND COMPLETE PERMUTATION POLYNOMIALS OVER FINITE FIELDS

BELHOUT BOUSALMI, ABDELMEJID BAYAD, AND ABDALLAH DERBAL

Abstract. Let q be a power of prime number p, such that

$$q \equiv 1(\mathrm{mod}3).$$

We investigate the following two families of polynomials

$$X^r(X^{2(q-1)/3} + \delta X^{(q-1)/3} + \delta^2 + 1),\ X^r(X^{2(q-1)/3} + X^{(q-1)/3} + \gamma)$$

where δ and γ belong to finite field $\mathbb{F}_q$. From these families, we find new classes of permutation polynomials (PP) and complete permutation polynomials (CPP) to the finite field $\mathbb{F}_q$.

1. Introduction and preliminaries

Let p be a prime number and let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of p. We set $q = p^n$ for some positive integer n. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if its associated polynomial mapping $f : x \to f(x)$ from $\mathbb{F}_q$ to itself is a bijection. A polynomial $f \in \mathbb{F}_q[X]$ is called a complete permutation polynomial (CPP) if both polynomial mapping $x \to f(x)$ and $x \to x + f(x)$ are permutation polynomials of $\mathbb{F}_q$.

The study of permutation polynomials started in 1863 with Hermite [5] for prime fields $\mathbb{F}_p$ and later by Dickson (1897) [2] for a general finite fields $\mathbb{F}_q$. There are two main reasons for the study (PP) and (CPP) of finite fields. First, (PP) over finite fields $\mathbb{F}_q$ become of remarkable interest in the construction of cryptographic systems for the secure transmission of data, coding theory and combinatorial design theory. See [7, 8, 9]. The second main motivation comes from the study of permutation groups [17].

The articles of Lidl and Mullen [10, 11] listed some open problems of interest and one of them is to find new classes of permutation polynomials of $\mathbb{F}_q$. In fact there are only a few classes of (PP) and (CPP) that are known. In general, it is not easy to construct (PP) and (CPP) of finite fields. For example, there is no known deterministic polynomial time algorithm to test whether a given polynomial is a permutation polynomial, though a probabilistic polynomial time solution has just been obtained by Von zur Gathen [4]. There are only three major known classes of (PP). The first

Key words and phrases. Finite fields, Permutation polynomials, Complete permutation polynomials.

class consists of Chebyshev-Dickson (PP). The Dickson polynomials of the first kind are given by

$$D_k(X,a)=\sum_{j=0}^{[k/2]}\frac{k}{k-j}\binom{k-j}{j}(-a)^jX^{k-2j},\quad \text{where } a\in\mathbb{F}_q.$$

These polynomials are (PP) of $\mathbb{F}_q$ if and only if $(k,q^2-1)=1$ and form a group under composition and have applications in public key cryptosystems. See [12, Theorem 7.16].

The second class consists of permutational linearized polynomials of the form $L(x)=\sum_{i=0}^{n}a_ix^{p^i}$ is a (PP) of $\mathbb{F}_q$ if and only if 0 is the unique root of L in $\mathbb{F}_q$. This class also forms a group, that so-called Betti-Mathieu group. It is isomorphic to the group $GL_n(\mathbb{F}_p)$ of nonsingular matrices, where $q=p^n$. See [12, p.362-390] and [15, Prop. 2.6, p.37].

The third class consists of (PP) of the form $X^rf(X^{\frac{q-1}{d}})$, where d is a divisor of $q-1$, wihich is introduced by Dickson and Rogers [3]. This class forms a group $G(d,q)$ under composition and this group is isomorphic to a generalized wreath product $G(d,q)\simeq G\rtimes H$, where $G=\mathbb{Z}/\frac{q-1}{d}\mathbb{Z}$ and $H=S_d$ (see [17, p.157-159]).

In general, it is very difficult to construct (PP). See [1, 4, 6, 8, 10, 11]. The following equivalent statements provide ideas which used to prove that a given polynomial is a (PP).

Theorem 1. *(*[6, Theorem 1.1, p.83]*) For $f\in\mathbb{F}_q[X]$, the following statements are equivalent.*

1. *f is a PP of $\mathbb{F}_q$.*
2. *For each $y\in\mathbb{F}_q$, the equation $f(x)=y$ has at least one solution $x\in\mathbb{F}_q$.*
3. *For each $y\in\mathbb{F}_q$, the equation $f(x)=y$ has at most one solution $x\in\mathbb{F}_q$.*
4. *For all $a\in\mathbb{F}_q^*$,*

$$\sum_{x\in\mathbb{F}_q}\zeta_p^{Tr_{q/p}(af(x))}=0, \text{where } p=char\mathbb{F}_q \text{ and } \zeta_p=e^{2\pi i/p}.$$

5. *(Hermite's criterion)*

$$\sum_{x\in\mathbb{F}_q}f(x)^s=\begin{cases}0 \ \ if \ \ 0\le s\le q-2\\ -1 \ \ if \ \ s=q-1.\end{cases}$$

6. *The polynomial $(f(X)-f(Y))/(X-Y)\in\mathbb{F}_q[X,\ Y]$ has no roots $(x,\ y)\in\mathbb{F}_q^2$ with $x\neq y$.*

Note that for the third class of (PP) of the form $X^r f(X^{\frac{q-1}{d}})$, we quote from [6, Theorem 2.2, p.85] and references therein the following simple criteria.

Theorem 2. *Let d and r be positive integers with $d \mid q-1$. Let $f(X) = X^r h(X^{\frac{q-1}{d}})$, where $h \in \mathbb{F}_q[X]$. Then, f is a (PP) of $\mathbb{F}_q$ if and only if*

(1) *$gcd(r, \frac{q-1}{d}) = 1$ and*
(2) *$X^r h(X)^{\frac{q-1}{d}}$ permutes μ_d.*

Theorem 2 is equivalent to the criterion for polynomial given by Wan-Lidl [17]. Let us recall this criteiron. Let $d \mid q-1$ and g be a fixed primitive root of $\mathbb{F}_q$. Let $\omega = g^{(q-1)/d}$ be a primitive d-th root of unity in $\mathbb{F}_q$. Define a multiplicative character ψ with values in $\mathbb{Z}/d\mathbb{Z}$ sush that for all $a \in \mathbb{F}_q^*$,

$$\psi(a) \equiv Ind_g(a) \pmod{d},$$

where $Ind_g(a)$ is the residue class b mod $(q-1)$ such that $a = g^b$. It is clear that ψ satisfies

$$a^{(q-1)/d} = \omega^{\psi(a)}.$$

With this definition, we have the following criterion.
Criterion of Wan and Lidl. *Let g be a primitive element of $\mathbb{F}_q$ and $\omega = g^{(q-1)/d}$ be a primitive d-th root of unity in $\mathbb{F}_q$. Then the polynomial $h(X) = X^r f(X^{(q-1)/d})$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied*

(a) $(r, \frac{q-1}{d}) = 1$,
(b) $f(\omega^i) \neq 0$, *for all* $0 \leq i < d$,
(c) $\psi\left(\frac{f(\omega^i)}{f(\omega^j)}\right) \not\equiv r(j-i) \pmod{d}$, *for all* $0 \leq i < j < d$.

This result unifies and generalizes several classes of permutation polynomials. But the difficulty lies with explicit definition to the polynomial h that satisfies the conditions of the previous criterion, this is due to the difficulty of the determination of a primitive element of $\mathbb{F}_q$, especially for the big values of q, and by other side the choice of the polynomial f which satisfies both conditions (b) and (c).

Due to the importance of polynomials of the form $X^r f(X^{(q-1)/d})$, in this paper we find and study two new classes of permutation polynomials of the forms: $X^r(X^{\frac{2(q-1)}{3}} + \delta X^{\frac{q-1}{3}} + \delta^2 + 1)$, and $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + \gamma)$ of $\mathbb{F}_q$, and we extract from the second form two classes of complete permutation polynomials of $\mathbb{F}_q$.

2. Main results

In this paper we prove the following results.

Theorem 3. *Let $\mathbb{F}_q$ be a finite field containing q elements, such that $q \equiv 1 \pmod 3$, and r be a positive integer, where $(r, q-1) = 1$. We have the following results*

1. *For every δ cubic root of unity in $\mathbb{F}_q$ such that $(3\delta^2+1)^{\frac{q-1}{3}} = 1$ in $\mathbb{F}_q$, the polynomial*
$$f(X) = X^r(X^{\frac{2(q-1)}{3}} + \delta X^{\frac{q-1}{3}} + \delta^2 + 1)$$
is a permutation polynomial of $\mathbb{F}_q$.
2. *For any $\gamma \in \mathbb{F}_q \backslash \{1, -2\}$ such that $\left(\frac{\gamma+2}{\gamma-1}\right)^{\frac{q-1}{3}} = 1$ in $\mathbb{F}_q$, the polynomial*
$$f(X) = X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + \gamma)$$
is a permutation polynomial of $\mathbb{F}_q$.

Theorem 4. *Let $\mathbb{F}_q$ be a finite field of characteristic p containing q elements, and r be a positive integer, where $(r, q-1) = 1$.*

1. *If $q \equiv 1 \pmod 6$, then the polynomial $X^r\left(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + \frac{p-1}{2}\right)$ is a permutation polynomial of $\mathbb{F}_q$.*
2. *If $p \equiv 1 \pmod 3$, and $q = p^{3k}$, $(k \geq 1)$. Then the polynomial $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + 2)$ is a permutation polynomial of $\mathbb{F}_q$.*
3. *If $p \geq 5$, $p \equiv -1 \pmod 3$ and $q = p^{2k}$ $(k \geq 1)$. Then the polynomial $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + 2)$ is a permutation polynomial of $\mathbb{F}_q$.*

Using Theorem 3 and Theorem 4, we obtain the following two corollaries.

Corollary 2.1. *Let $q = 2^{6k}$ $(k \geq 1)$, and r be a positive integer, where $(r, q-1) = 1$. Then there exists δ in $\mathbb{F}_q^*$, such that the polynomials $X^r(X^{2(\frac{q-1}{3})} + \delta X^{\frac{q-1}{3}} + \delta)$ and $X^r(X^{2(\frac{q-1}{3})} + \delta^2 X^{\frac{q-1}{3}} + \delta^2)$ are permutation polynomials of $\mathbb{F}_q$.*

Corollary 2.2. *Let p be a prime number, $p \geq 5$. We set $q = p^{2k}$ if $p \equiv -1 \pmod 3$ or $q = p^{k(p-1)}$. Then the polynomials $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}})$ and $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} - 1)$ are permutation polynomials of $\mathbb{F}_q$, where $(r, q-1) = 1$.*

3. Key Lemmas

Before we proceed to the proof of our main results, we present the following elementary lemmas.

Lemma 3.1. *Let p a prime number, x be a integer, and u be a positive integer. Then $x^{p^u} \equiv x \pmod p$.*

Proof. According to Fermat's little theorem, we have $x^p \equiv x \pmod p$. And by recurrence, we get $x^{p^u} \equiv x \pmod p$, for all $u \geq 1$. □

Lemma 3.2. *Let $q \equiv 1 \pmod 3$, and the polynomial $f(X) = X^2 + X + 1 \in \mathbb{F}_q[X]$. Then f has two distinct roots in $\mathbb{F}_q$.*

Proof. Let g be a primitive element of $\mathbb{F}_q$. By putting $\delta = g^{\frac{q-1}{3}}$, we find that $\delta^3 = 1$ and $\delta \neq 1$, then $\delta^2 + \delta + 1 = 0$. Therefore δ is root of the polynomial f in $\mathbb{F}_q$. It is clear that δ^2 is the second root and $\delta^2 \neq 1, \delta$. □

Lemma 3.3. *Let p a prime number, u be a positive integer and x be a integer number, such that $p \nmid x$. Then*

$$\begin{cases} x^{\frac{p^{3u}-1}{3}} \equiv 1 \pmod p & \text{if } p \equiv 1 \pmod 3 \\ x^{\frac{p^{2u}-1}{3}} \equiv 1 \pmod p & \text{if } p \equiv -1 \pmod 3 \end{cases}$$

Proof. For $u \geq 1$, we have by Fermat's little theorem

$$\begin{cases} x^{\frac{p^{3u}-1}{3}} = \left(x^{p-1}\right)^{\left(\frac{p^2+p+1}{3}\right)(1+p^3+p^6+\cdots+p^{3u-3})} \equiv 1 \pmod p \text{ if } p \equiv 1 \pmod 3 \\ x^{\frac{p^{2u}-1}{3}} = \left(x^{p-1}\right)^{\left(\frac{p+1}{3}\right)(1+p^2+p^4+\cdots+p^{2u-2})} \equiv 1 \pmod p \text{ if } p \equiv -1 \pmod 3. \end{cases}$$

Then we get our desired result. □

4. Proofs of main results

4.1. Proof of theorem 3.

We prove Theorem 3. It suffices to prove that the induced map f is injective on $\mathbb{F}_q$. Suppose that $f(a) = f(b)$ for some elements a and b of $\mathbb{F}_q$. If $a = 0$, then $b^r(b^{2(\frac{q-1}{3})} + \delta b^{\frac{q-1}{3}} + \delta^2 + 1) = 0$. Suppose $b \neq 0$, then $b^{2(\frac{q-1}{3})} + \delta b^{\frac{q-1}{3}} + \delta^2 + 1 = 0$. Put $\omega = b^{\frac{q-1}{3}}$, then

$$\omega^2 + \delta\omega + \delta^2 + 1 = 0 \tag{4.1}$$

and we have $\omega^3 = b^{q-1} = 1$, ω is a cubic root of unity. This is equivalent to $\{(\omega = \delta) \text{ or } (\omega^2 + \delta\omega + \delta^2 = 0)\}$. If $\omega = \delta$, then $3\delta^2 + 1 = 0$, which contradicts the condition $(3\delta^2 + 1)^{\frac{q-1}{3}} = 1$. If $\omega \neq \delta$, by equation (4.1), we have $1 = 0$ which is a contradiction ($q \geqslant 2$). Then $b = 0 = a$.

Now we suppose that $ab \neq 0$, and we put $\theta = a^{\frac{q-1}{3}}$, then $\theta^3 = 1 = \delta^3$. By symmetry, we have just the following three cases:

1. If $\theta = \omega = \delta$. From equation $f(a) = f(b)$ we get: $(3\delta^2 + 1)a^r = (3\delta^2 + 1)b^r$. Hence $\left(\frac{a}{b}\right)^r = 1$. Then the order l of $\frac{a}{b}$ in $\mathbb{F}_q^*$ divides $(r, q-1)$, and by the condition $(r, q-1) = 1$, we have $l = 1$. Therefore $a = b$.
2. If $\theta = \delta$ and $\omega \neq \delta$. From equation $f(a) = f(b)$ we get: $(3\delta^2+1)a^r = b^r$, and hence $\left(\frac{b}{a}\right)^r = 3\delta^2 + 1$. Then we deduce that

$$\left(\frac{b^{\frac{q-1}{3}}}{a^{\frac{q-1}{3}}}\right)^r = \left(3\delta^2 + 1\right)^{\frac{q-1}{3}} = 1.$$

Then we have $\left(\frac{\omega}{\delta}\right)^r = 1$, this implies that the order l of $(\frac{\omega}{\delta})$ in $\mathbb{F}_q^*$ divides $(r, q-1)$,. On the other hand $\omega \neq \delta$, then $l \geqslant 2$, therefore $(r, q-1) \geqslant 2$, which contradicts the condition $(r, q-1) = 1$.

3. If $\theta \neq \delta$ and $\omega \neq \delta$, then $\theta^2 + \delta\theta + \delta^2 = \omega^2 + \delta\omega + \delta^2 = 0$. The equation $f(a) = f(b)$ gives that $a^r = b^r$, hence $\left(\frac{a}{b}\right)^r = 1$. We then deduce from the condition $(r, q-1) = 1$ that $a = b$.

To prove the second part of the Theorem 3, we follow the same method that we used to prove the first one below. So it suffices to prove that the induced map f is injective on $\mathbb{F}_q$. Suppose that $f(a) = f(b)$ for some elements a and b of $\mathbb{F}_q$. If $a = 0$, then $b^r(b^{2(\frac{q-1}{3})} + b^{\frac{q-1}{3}} + \gamma) = 0$. Suppose $b \neq 0$, then $b^{2(\frac{q-1}{3})} + b^{\frac{q-1}{3}} + \gamma = 0$. Put $\omega = b^{\frac{q-1}{3}}$, then $\omega^2 + \omega + \gamma = 0$, and we have $\omega^3 = b^{q-1} = 1$, ω is a cubic root of unity. This is equivalent to $\{(\omega = 1)$ or $(\omega^2 + \omega + 1 = 0)\}$. We then get $\gamma = -2$ or $\gamma = 1$, which is a contradiction. Then $b = 0 = a$.

Now, we assume that $ab \neq 0$, and we put $\theta = a^{\frac{q-1}{3}}$, then $\theta^3 = 1$. By symmetry, we get the only following three cases:

1. If $\theta = \omega = 1$. By equation $f(a) = f(b)$, we have $(\gamma+2)a^r = (\gamma+2)b^r$, hence $\left(\frac{a}{b}\right)^r = 1$. Then the order l of $(\frac{a}{b})$ in $\mathbb{F}_q^*$ divides $(r, q-1)$, and by the condition $(r, q-1) = 1$, we have $l = 1$. hence $a = b$.
2. If $\theta = 1$ and $\omega \neq 1$. From equation $f(a) = f(b)$, we get: $(\gamma + 2)a^r = (\gamma - 1)b^r$, hence $\left(\frac{b}{a}\right)^r = \left(\frac{\gamma+2}{\gamma-1}\right)$. Then we deduce that

$$\left(\frac{b^{\frac{q-1}{3}}}{a^{\frac{q-1}{3}}}\right)^r = \left(\frac{\gamma+2}{\gamma-1}\right)^{\frac{q-1}{3}} = 1.$$

   Then we have $\omega^r = 1$. Since $\omega \neq 1$, then ω is a primitive cubic root of unity, therefore $3 \mid (r, q-1)$, which contradicts the condition $(r, q-1) = 1$.
3. If $\theta \neq 1$ and $\omega \neq 1$. The two elements θ and ω are primitives cubic roots of unity, then $\theta^2 + \theta = \omega^2 + \omega = -1$. By the equation $f(a) = f(b)$, we get: $(\gamma - 1)a^r = (\gamma - 1)b^r$, hence $\left(\frac{a}{b}\right)^r = 1$, we deduce from the condition $(r, q-1) = 1$ that $a = b$.

This gives our Theorem 3.

4.2. **Proof of theorem 4.**

1) If $q \equiv 1 \pmod 6$, here we have $p \neq 2$ and $p \neq 3$. By taking $\gamma = \frac{p-1}{2}$ in the second part of Theorem 3, then we obtain $\gamma \neq 1$ and $\gamma \neq -2$. It follows that

$$\left(\frac{\gamma+2}{\gamma-1}\right)^{\frac{q-1}{3}} = (-1)^{\frac{q-1}{3}} = 1.$$

Hence the condition of second part of Theorem 3 is satisfied. Therefore we deduce first part of the Theorem 4.

2) According to the Lemma 3.3, we have $4^{\frac{q-1}{3}} = 1$ in $\mathbb{F}_q$. Then by the Theorem 3, the polynomial $f(X) = X^r(X^{2(\frac{q-1}{3})} + X^{\frac{q-1}{3}} + 2)$ is a permutation polynomial of $\mathbb{F}_q$. This proves the second part of Theorem 4.
3) We prove the remaing case in the same way as the proof of the second result.

4.3. **Proof of Corollary 2.1.**
We have $q \equiv 1 \pmod 9$, so $3 \mid \frac{q-1}{3}$. From the Lemma 3.2 it exists $\delta \in \mathbb{F}_q^*$, such that $\delta \neq 1$ and $\delta^3 = 1$. Then we get $(3\delta^2+1)^{\frac{q-1}{3}} = \delta^{\frac{q-1}{3}} = 1$ and $(3\delta^4+1)^{\frac{q-1}{3}} = (\delta+1)^{\frac{q-1}{3}} = (\delta^2)^{\frac{q-1}{3}} = 1$. By the Theorem 1, we find that the polynomials $X^r(X^{2(\frac{q-1}{3})} + \delta X^{\frac{q-1}{3}} + \delta)$ and $X^r(X^{2(\frac{q-1}{3})} + \delta^2 X^{\frac{q-1}{3}} + \delta^2)$ are permutation polynomials of $\mathbb{F}_q$.

4.4. **Proof of Corollary 2.2.**
If $q = p^{k(p-1)}$, we can write $q-1 = (p-1)(1+p+p^2+\cdots+p^{k(p-1)-1})$. By Lemma 3.1, we have

$$\begin{aligned} 2^{\left(1+p+\cdots+p^{k(p-1)-1}\right)} &\equiv (2^{p-1})^k (\mod p) \\ &\equiv 1 (\mod p). \end{aligned}$$

Since $p \geqslant 5$ then $p-1$ is even and $(6,p) = 1$. So by Euler's theorem we get $p^{k(p-1)} \equiv 1 \pmod 6$. We deduce that $3 \mid p-1$ or $3 \mid 1+p+\cdots+p^{k(p-1)-1}$.
• If $3 \mid p-1$ then

$$2^{\frac{q-1}{3}} = \left(2^{1+p+\cdots+p^{k(p-1)-1}}\right)^{\frac{p-1}{3}} \equiv 1 \pmod p.$$

• If $3 \mid 1+p+\cdots+p^{k(p-1)-1}$ then

$$2^{\frac{q-1}{3}} = \left(2^{p-1}\right)^{\left(\frac{1+p+\cdots+p^{k(p-1)-1}}{3}\right)} \equiv 1 \pmod p.$$

Now if $p \equiv -1 \pmod 3$ and $q = p^{2k}$, then it is clear that $(3, p-1) = 1$ and $q \equiv 1 \pmod 6$, hence we deduce that $\frac{q-1}{3(p-1)} \in \mathbb{N}^*$. By Fermat's little theorem, we have

$$2^{\frac{q-1}{3}} = \left(2^{p-1}\right)^{\left(\frac{q-1}{3(p-1)}\right)} \equiv 1 \pmod p.$$

Then we conclude in both cases that $2^{\frac{q-1}{3}} = 1$ in $\mathbb{F}_q$.
By taking $\gamma = 0$ or $\gamma = -1$ in the second part of Theorem 3, we get $\left(\frac{\gamma+2}{\gamma-1}\right)^{\frac{q-1}{3}} = 1$, then we find that both polynomials $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}})$ and $X^r(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} - 1)$ are permutation polynomials of $\mathbb{F}_q$.

5. New classes of complete permutation polynomials

For $r = 1$ and thanks to Theorems 3 and 4, we extract two new families of (CPP) over finite fields. This is formulated in the following theorems.

Theorem 5. *Let $q = 7^{3u}$ and u be any positive integer. Then we have the polynomial $f(x) = X^{1+\frac{2(q-1)}{3}} + X^{1+\frac{q-1}{3}} + 2X$ is a complete permutation polynomial of $\mathbb{F}_q$.*

Proof. We can write

$$\begin{aligned} f(x) &= X^{1+\frac{2(q-1)}{3}} + X^{1+\frac{q-1}{3}} + 2X \\ &= X(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + 2). \end{aligned}$$

And we have $f(X) + X = X(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} + 3)$, thanks to Theorem 4 (with $p = 7$ and $q = 7^{3u}$), we find that both polynomials $f(X)$ and $f(X)+X$ are permutation polynomials of $\mathbb{F}_{7^{3u}}$. Then we get our desired result. □

Theorem 6. *Let p be a prime number, $p \geq 5$. We set $q = p^{2k}$ if $p \equiv -1 \pmod 3$ or $q = p^{k(p-1)}$. Then the polynomial $f(X) = X^{1+\frac{2(q-1)}{3}} + X^{1+\frac{q-1}{3}} - X$ is a complete permutation polynomial of $\mathbb{F}_q$.*

Proof. We have

$$\begin{aligned} f(X) &= X^{1+\frac{2(q-1)}{3}} + X^{1+\frac{q-1}{3}} - X \\ &= X(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}} - 1) \end{aligned}$$

and we can see that $f(X) + X = X(X^{\frac{2(q-1)}{3}} + X^{\frac{q-1}{3}})$, thanks to Corollary 2.2 (with $\gamma = 0$ or $\gamma = -1$) , we find that both polynomials $f(X)$ and $f(X) + X$ are permutation polynomials of $\mathbb{F}_q$. Then the polynomial $f(X) = X^{1+\frac{2(q-1)}{3}} + X^{1+\frac{q-2}{3}} - X$ is a complete permutation polynomial of $\mathbb{F}_q$. □

6. Examples

In the following we give many interesting (PP) and (CPP) polynomials for some finite fields.

6.1. **Example 1.** Thanks to Theorems 3, 4, 5, and 6 we obtain

- **a)** the binomials $X^{17} + X^9$, $X^{21} + X^{13}$, $X^{23} + X^{15}$, and $X^{27} + X^{19}$ are permutation polynomials of $\mathbb{F}_{25}$.
- **b)** the trinomial $X^r(X^{\frac{2(7^u-1)}{3}} + 2X^{\frac{7^u-1}{3}} + 5)$ is a permutation polynomial of $\mathbb{F}_{7^u}$, where $(r, 7^u - 1) = 1$.
- **c)** the trinomial $X^r(X^{\frac{2(13^u-1)}{3}} + X^{\frac{13^u-1}{3}} + 6)$ is a permutation polynomial of $\mathbb{F}_{13^u}$, where $(r, 13^u - 1) = 1$.
- **d)** the trinomial $X^{17} + X^9 - X$ is a complete permutation polynomials of $\mathbb{F}_{25}$.
- **e)** the trinomial $X^{229} + X^{115} + 2X$ is a complete permutation polynomials of $\mathbb{F}_{343}$.

6.2. **Example 2.** We have $\mathbb{F}_{16} \simeq \frac{\mathbb{F}_2[X]}{<p(X)>}$, where $p(X) = X^4 + X^3 + X^2 + X + 1$ is an irreducible polynomial in the ring $\mathbb{F}_2[X]$. Then the field $\mathbb{F}_{16}$ contains a root α of the polynomial $p(X)$, and it is clear that $\alpha \neq 1$. Put $\gamma = \frac{\alpha}{\alpha-1}$, then we have

$$\left(\frac{\gamma}{\gamma-1}\right)^5 = \alpha^5 = 1.$$

Hence, by Theorem 3, we find that the trinomial $f(X) = X^r(X^{10} + X^5 + \gamma)$ is a permutation polynomial of $\mathbb{F}_{16}$, where $(r, 15) = 1$. And we have the polynomial $X^{11} + X^6 + \gamma X$ is a complete permutation polynomials of $\mathbb{F}_{16}$.

References

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

[2] L. E. Dickson, *The analytic representation of substitutions on a prime power of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65-120, 161-183.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, Teubner (1901), New York, Dover (1958).

[4] J. Von zur Gathen, *Tests for permutation polynomials*, J. Comput, **20** (1991), 591-602.

[5] C. Hermite, *Sur les fonctions de sept lettres,* C. R. Acad. Sci-Paris **. 57** (1863), 750-757.

[6] X. D. Hou, *Permutation polynomials over finite fieds-A survey of recent advances*, Finite Fields Appl. **32** (2015) 82-119.

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

[8] R. Lidl, W. B. Mullen, *A note on polynomials and functions in algebraic cryptography*, Ars Combin **17A** (1977) 76-92.

[9] R.Lidl, H. Niederreiter , *Introduction to Finite Fields and their Applications* , Cambridge University Press Cambridge, 1986.

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

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

[12] R. Lidl and H. Niederreiter, *Finite Fields.* Cambridge University Press, second edition, 1997.

[13] G.L. Mullen, D. Panario (Eds.), *Handbook of Finite Fields*, CRC Press, Boca Raton, 2013.

[14] H. Niederreiter, K H. Robinson, *Complete mappings of finite fields.* J Aust Math Soc Ser A, 1982, 2: 197-212

[15] C. Small, *Arithmetic of Finite Fields,* CRC Press, 24 avr. 1991 - 240 pages.

[16] J. K. Strayer, *Elementary Number Theory,* PWS Publishing Company, Boston, 1994.

[17] D. Q. Wan, R. Lidl, *Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure,* Monatsh. Math. **112** (2) (1991), 149-163.

Belhout BOUSALMI

Département de Mathématiques et Laboratoire d'Equations aux Dérivées Partielles Non linéaires et Histoire des Mathématiques, Ecole Normale Supérieure, B.P. 92, Vieux Kouba, Alger, Algérie.

E-mail address: belhout23@gmail.com

Abdelmejid BAYAD
Université Paris-Saclay, Laboratoire de Mathématiques et Modélisation d'Evry (UMR 8071), 23 Boulevard de France, 91037 Evry cedex, France.
E-mail address: abdelmejid.bayad@univ-evry.fr

Abdallah DERBAL
Département de Mathématiques et Laboratoire d'Equations aux Dérivées Partielles Non linéaires et Histoire des Mathématiques, Ecole Normale Supérieure, B.P. 92, Vieux Kouba, Alger, Algérie.
E-mail address: abderbal@yahoo.fr