MATHEMATICA MONTISNIGRI
Vol LVI (2023)

SPECIFIC PERMUTATION POLYNOMIALS OVER FINITE FIELDS

BELHOUT BOUSALMI

Department of Mathematics, Higher Normal School of Laghouat, Box 4033, Algeria
EDPNL & HM Laboratory of ENS-Kouba, Box 92 Algiers, Algeria
Corresponding author. E-mail: belhout23@gmail.com

DOI: 10.20948/mathmontis-2023-56-2

Summary. We give sufficient conditions for polynomials of special forms to be permutation polynomials over finite field. More specifically, we construct several explicit classes of permutation polynomials from these forms over finite fields. We also present from these polynomials a new family of complete permutation polynomials.

1 INTRODUCTION

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 know that any finite field $\mathbb{F}_q$ is commutative and that its multiplicative group $\mathbb{F}_q^*$ is cyclic. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial of $\mathbb{F}_q$ if its associated polynomial mapping $f: x \mapsto f(x)$ from $\mathbb{F}_q$ to itself is a bijection. A polynomial $f \in \mathbb{F}_q[X]$ is called a complete permutation polynomial if both polynomials $f(X)$ and $f(X) + X$ are permutation polynomials of $\mathbb{F}_q$.

The study of permutation polynomials started with Hermite (1863) [1], for prime fields $\mathbb{F}_p$ and later to Dickson (1897) [2, 3] for general finite fields $\mathbb{F}_q$. Permutation polynomials have important applications in cryptography, coding theory, combinatorial designs (see [4], [5] and [6]) and motivation comes from the study of permutation groups [7]. Also other areas of mathematics and engineering.

The construction of new classes of permutation polynomials is an interesting subject of study. Indeed we find in the papers of Lidl and Mullen [8, 9] some interesting open problems 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 permutation polynomials that are known [10]. In general, it is not easy to construct them.

In this paper, we have studied two families of composite polynomials over a finite field $\mathbb{F}_q$ of the form

$$X^r f\left(X^{\frac{q-1}{4}}\right), \text{ such that } r \in \mathbb{N}^*, q \equiv 1 \pmod 4 \text{ and } f \in \mathbb{F}_q[X].$$

Throughout this article, we denote (n, m) the greatest common divisor of any two integers n and m.

- The first family for $f(X) = X^3 + \delta X^2 + \delta^2 X + \delta^3 + 1$ with δ is a fourth root of unity in $\mathbb{F}_q$, and in this case we have the polynomial $X^r f\left(X^{\frac{q-1}{4}}\right)$ is a permutation of $\mathbb{F}_q$ if $(r, q-1) = 1$ and $(4\delta^3 + 1)^{\frac{q-1}{4}} = 1$ in $\mathbb{F}_q$.

2020 Mathematics Subject Classification: 12E05, 12E20, 12E30 .
Key words and Phrases: Finite fields, Permutation polynomials, Complete permutation polynomials.

- The second family for $g(X) = X^3 + X^2 + X + \gamma$, in this case the polynomial $X^r g\left(X^{\frac{q-1}{4}}\right)$ is a permutation of $\mathbb{F}_q$ if $(r, q-1) = 1$ and $\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{q-1}{4}} = 1$ in $\mathbb{F}_q$. And it is a complete permutation polynomial for special values of r, q and γ.

2 MAIN RESULTS

In this paper we prove the following results.

Theorem 2.1 Let $\mathbb{F}_q$ be a finite field containing q elements, such that $q \equiv 1 \pmod 4$, and let r be a positive integer, where $(r, q-1) = 1$. We have the following results

1. For every δ a fourth root of unity in $\mathbb{F}_q$ such that $(4\delta^3 + 1)^{\frac{q-1}{4}} = 1$ in $\mathbb{F}_q$, the polynomial

$$f(X) = X^r\left(X^{\frac{3(q-1)}{4}} + \delta X^{\frac{q-1}{2}} + \delta^2 X^{\frac{q-1}{4}} + \delta^3 + 1\right)$$

is a permutation polynomial of $\mathbb{F}_q$.

2. For any $\gamma \in \mathbb{F}_q \backslash \{1, -3\}$ such that $\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{q-1}{4}} = 1$ in $\mathbb{F}_q$, the polynomial

$$g(X) = X^r\left(X^{\frac{3(q-1)}{4}} + X^{\frac{q-1}{2}} + X^{\frac{q-1}{4}} + \gamma\right)$$

is a permutation polynomial of $\mathbb{F}_q$.

Theorem 2.2 Let $q = 5^{4m}, (m \geq 1)$ and let r be a positive integer, where $(r, q-1) = 1$. Then we have

1. the polynomial $f(X) = X^r\left(X^{\frac{3(q-1)}{4}} + \delta X^{\frac{q-1}{2}} + \delta^2 X^{\frac{q-1}{4}} + \delta^3 + 1\right)$ is a permutation polynomial of $\mathbb{F}_q$ for all $\delta \in \mathbb{F}_5 \backslash \{0, 1\}$.
2. the polynomial $g(X) = X^r\left(X^{\frac{3(q-1)}{4}} + X^{\frac{q-1}{2}} + X^{\frac{q-1}{4}} + \gamma\right)$ is a permutation polynomial of $\mathbb{F}_q$ for all $\gamma \in \mathbb{F}_5 \backslash \{1, 2\}$.

Using Theorem 2.1 and Theorem 2.2 we obtain the following two corollaries.

Corollary 2.3 Let p be a prime number, such that $p \equiv 1 \pmod 4$ and $p \geq 7$, we set $q = p^{4m}, m \geq 1$. Then the polynomial

$$X^r\left(X^{\frac{3(q-1)}{4}} + X^{\frac{q-1}{2}} + X^{\frac{q-1}{4}} + 2\right)$$

is a permutation polynomial of $\mathbb{F}_q$.

Corollary 2.4 For every odd positive integer r, the polynomial

$$f(X) = X^{r+6} + X^{r+4} + X^{r+2} + 2X^r$$

is a permutation polynomial of $\mathbb{F}_9$.

3 LEMMAS

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

Lemma 3.1 Let p be a prime number, x be a integer, and let m be a positive integer. Then

$$x^{p^m} \equiv x \pmod{p}.$$

Proof. According to Fermat's little theorem, we have $x^p \equiv x \pmod{p}$. And by recurrence, we get $x^{p^m} \equiv x \pmod{p}$, for all positive integer m.

Lemma 3.2 Let m and x be positive integers. And let p be a prime number, such that $p \equiv 1 \pmod 4$ and $p \nmid x$. Then we have

$$x^{\frac{p^{4m}-1}{4}} \equiv 1 \pmod{p}.$$

Proof. For $m \geq 1$, we have

$$p^{4m} - 1 = (p-1)(1+p+p^2+p^3)(1+p^4+p^8+\cdots+p^{4m-4}).$$

Since $1+p+p^2+p^3 \equiv 0 \pmod 4$. Then by Fermat's little theorem, we find

$$x^{\frac{p^{4m}-1}{4}} = (x^{p-1})^{(1+p^4+p^8+\cdots+p^{4m-4})\left(\frac{1+p+p^2+p^3}{4}\right)} \equiv 1 \pmod{p}.$$

4 PROOFS OF MAIN RESULTS

Proof of theorem 2.1 We prove the first part of the Theorem 2.1. 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 $b^r\left(b^{\frac{3(q-1)}{4}} + \delta b^{\frac{q-1}{2}} + \delta^2 b^{\frac{q-1}{4}} + \delta^3 + 1\right) = 0$. Suppose $b \neq 0$, then $b^{\frac{3(q-1)}{4}} + \delta b^{\frac{q-1}{2}} + \delta^2 b^{\frac{q-1}{4}} + \delta^3 + 1 = 0$. Put $\omega = b^{\frac{q-1}{4}}$, then we have

$$\omega^3 + \delta\omega^2 + \delta^2\omega + \delta^3 + 1 = 0. \tag{4.1}$$

And we also have $\omega^4 = b^{q-1} = 1$, it means that ω is a fourth root of unity. This is equivalent to

$$(\omega = \delta) \text{ or } (\omega^3 + \delta\omega^2 + \delta^2\omega + \delta^3 = 0).$$

If $\omega = \delta$, by equation 4.1, we have $4\delta^3 + 1 = 0$, which contradicts the condition $(4\delta^3 + 1)^{\frac{q-1}{4}} = 1$. If $\omega \neq \delta$, by equation 4.1, we find that $1 = 0$ it is a contradiction $(q \geq 2)$. Then $b = 0 = a$. Now we suppose that $ab \neq 0$, and we put $\theta = a^{\frac{q-1}{4}}$ and $\omega = b^{\frac{q-1}{4}}$ then $\theta^4 = \omega^4 = \delta^4 = 1$. By symmetry, we have just the following three cases:

Case 1: If $\theta = \omega = \delta$. From equation $f(a) = f(b)$, we get:
$a^r(4\delta^3 + 1) = b^r(4\delta^3 + 1)$, hence $(\frac{a}{b})^r = 1$. Then the order l of the element $\frac{a}{b}$ in the multiplicative group $\mathbb{F}_q^*$ divides $(r, q-1)$, and by the condition $(r, q-1) = 1$, we obtain $l = 1$. Therefore $a = b$.

Case 2: If $\theta = \delta$ and $\omega \neq \delta$. From equation $f(a) = f(b)$, we get: $a^r(4\delta^3 + 1) = b^r$, hence $(\frac{b}{a})^r = 4\delta^3 + 1$. Then we deduce that

$$\left(\frac{b^{\frac{q-1}{4}}}{a^{\frac{q-1}{4}}}\right)^r = (4\delta^3 + 1)^{\frac{q-1}{4}} = 1.$$

Then we have $(\frac{\omega}{\theta})^r = (\frac{\omega}{\delta})^r = 1$, hence the order l of $\frac{\omega}{\delta}$ in $\mathbb{F}_q^*$ divides $(r, q-1)$, Since $\omega \neq \delta$, then $l \geq 2$, therefore $(r, q-1) \geq 2$, which contradicts the condition $(r, q-1) = 1$.

Case 3: If $\theta \neq \delta$ and $\omega \neq \delta$. We have $\theta^3 + \delta\theta^2 + \delta^2\theta + \delta^3 = \omega^3 + \delta\omega^2 + \delta^2\omega + \delta^3 = 0$. By the equation $f(a) = f(b)$, we get: $a^r = b^r$ hence $(\frac{a}{b})^r = 1$, we deduce from the condition $(r, q-1) = 1$ that $a = b$. The proof of the first part of the Theorem 2.1 is finished.

To prove the second part of the Theorem 2.1, we follow the same method that we used to prove the first result. So it suffices to prove that the induced map g is injective on $\mathbb{F}_q$. Suppose that $g(a) = g(b)$ for some elements a and b of $\mathbb{F}_q$. If $a = 0$, then $b^r\left(b^{\frac{3(q-1)}{4}} + b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + \gamma\right) = 0$. Suppose $b \neq 0$, then $b^{\frac{3(q-1)}{4}} + b^{\frac{q-1}{2}} + b^{\frac{q-1}{4}} + \gamma = 0$. Put $\omega = b^{\frac{q-1}{4}}$, then

$$\omega^3 + \omega^2 + \omega + \gamma = 0. \tag{4.2}$$

And we have $\omega^4 = b^{q-1} = 1$, ω is a fourty root of unity. This is equivalent to

$$(\omega = 1) \text{ or } (\omega^3 + \omega^2 + \omega + 1 = 0).$$

Then by the equation 4.2, we obtain $(\gamma = -3)$ or $(\gamma = 1)$ which contradicts the hypothesis of the Theorem 2.1. Then $b = 0 = a$.

Now we suppose that $ab \neq 0$. We put $\theta = a^{\frac{q-1}{4}}$ and $\omega = b^{\frac{q-1}{4}}$ then $\theta^4 = \omega^4 = 1$. By symmetry, we get the only following three cases:

Case 1: If $\theta = \omega = 1$. By equation $g(a) = g(b)$, we have $(\gamma + 3)a^r = (\gamma + 3)b^r$, 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 find that $l = 1$. hence $a = b$.

Case 2: If $\theta = 1$ and $\omega \neq 1$. From equation $g(a) = g(b)$, we get: $(\gamma + 3)a^r = (\gamma - 1)b^r$, hence $\left(\frac{b}{a}\right)^r = \frac{\gamma+3}{\gamma-1}$. Then we deduce that

$$\left(\frac{b^{\frac{q-1}{4}}}{a^{\frac{q-1}{4}}}\right)^r = \left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{q-1}{4}} = 1.$$

Then we have $\omega^r = 1$. Since $\omega \neq 1$, then the order of $\omega \geq 2$, it implies that $(r, q-1) \geq 2$ which contradicts the condition $(r, q-1) = 1$.

Case 3: If $\theta \neq 1$ and $\omega \neq 1$. Then we have $\theta^3 + \theta^2 + \theta = \omega^3 + \omega^2 + \omega = -1$. By the equation $g(a) = g(b)$, we get: $(\gamma - 1)a^r = (\gamma - 1)b^r$ hence $(\frac{a}{b})^r = 1$, we deduce from the

condition $(r, q-1)=1$ that $a=b$. The proof of the theorem 2.1 is complete.

Proof of theorem 2.2

1. Let $\delta \in \mathbb{F}_5 \backslash \{0,1\}$, then $\delta^4=1$ and $\delta^3 \neq 1$. We have

$$(4\delta^3+1)^{\frac{q-1}{4}}=(1-\delta^3)^{\frac{5^{4m}-1}{4}}=(1-\delta^3)^{1+5+5^2+\cdots+5^{(4m-1)}}.$$

By the Lemma 3.1, we have

$$(1-\delta^3)^{1+5+5^2+\cdots+5^{(4m-1)}}=(1-\delta^3)^{4m}.$$

Since $1-\delta^3$ is an element of $\mathbb{F}_5^*$, then by Fermat's little theorem we have $(1-\delta^3)^{4m}=1$, hence we deduce that $(4\delta^3+1)^{\frac{q-1}{4}}=1$. Then δ satisfies the conditions of the first part of Theorem 2.1. Therefore the polynomial $f(X)$ is a permutation polynomial of $\mathbb{F}_q$.

2. Let $\gamma \in \mathbb{F}_5 \backslash \{1,2\}$. We show that γ satisfies the condition of the second part of Theorem 2.1. We have

$$\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{q-1}{4}}=\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{5^{4m}-1}{4}}=\left(\frac{\gamma+3}{\gamma-1}\right)^{1+5+5^2+\cdots+5^{(4m-1)}}.$$

Since $\frac{\gamma+3}{\gamma-1}$ is an element of $\mathbb{F}_5^*$, then from the lemma 3.1, we have

$$\left(\frac{\gamma+3}{\gamma-1}\right)^{1+5+5^2+\cdots+5^{(4m-1)}}=\left(\frac{\gamma+3}{\gamma-1}\right)^{4m}=1.$$

Thus the polynomial $g(X)$ is a permutation polynomial of $\mathbb{F}_q$. This completes the proof of the theorem.

Proof of corollary 2.3 By taking $\delta=1$ and $q=p^{4m}$ in the first part of Theorem 2.1, and according to the lemma 3.2, we get

$$(4\delta^3+1)^{\frac{q-1}{4}}=5^{\frac{p^{4m}-1}{4}}=1.$$

Then we have the polynomial $X^r\left(X^{\frac{3(q-1)}{4}}+X^{\frac{q-1}{2}}+X^{\frac{q-1}{4}}+2\right)$ is a permutation polynomial of $\mathbb{F}_q$.

Proof of corollary 2.4 We can write

$$f(X)=X^{r+6}+X^{r+4}+X^{r+2}+2X^r$$
$$=X^r(X^{\frac{3(9-1)}{4}}+X^{\frac{9-1}{2}}+X^{\frac{9-1}{4}}+2).$$

Since r is an odd positive integer, then $(r,2^3)=1$. And by taking $\gamma=2$ and $q=3^2$ in the second part of theorem 2.1, we get $\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{q-1}{4}}=2^2=1$ hence we find that the polynomial $f(X)=X^{r+6}+X^{r+4}+X^{r+2}+2X^r$ is a permutation polynomial of $\mathbb{F}_9$.

5 A NEW FAMILY OF COMPLETE PERMUTATION POLYNOMIALS

For $r = 1$ and thanks to Theorem 2.2, we extract a new family of complete permutation polynomials over finite fields. This is formulated in the following theorem.

Theorem 5.1 Let $q = p^{4m}, (m \geq 1)$. Then the polynomial

$$f(X) = X^{1+\frac{3(q-1)}{4}} + X^{1+\frac{q-1}{2}} + X^{1+\frac{q-1}{4}} + 3X$$

is a complete permutation polynomial of $\mathbb{F}_q$.

Proof. We have

$$\begin{aligned} f(X) &= X^{1+\frac{3(q-1)}{4}} + X^{1+\frac{q-1}{2}} + X^{1+\frac{q-1}{4}} + 3X \\ &= X(X^{\frac{3(q-1)}{4}} + X^{\frac{q-1}{2}} + X^{\frac{q-1}{4}} + 3). \end{aligned}$$

And we have $f(X) + X = X(X^{\frac{3(q-1)}{4}} + X^{\frac{q-1}{2}} + X^{\frac{q-1}{4}} + 4)$, thanks to Theorem 2.2 (with $\gamma = 3$ and $\gamma = 4$), we find that both polynomials $f(X)$ and $f(X) + X$ are permutation polynomials of $\mathbb{F}_{5^{4m}}$. Then we get our desired result.

6 EXAMPLES

In the following we give many interesting permutation and complete permutation polynomials over some finite fields.

Examples 6.1

a) The polynomials $X^{469} + 3X^{313} - X^{157} + 3X, X^{469} + 2X^{313} - X^{157} - X$ and $X^{469} - X^{313} + X^{157}$ are permutation polynomials of $\mathbb{F}_{54}$.

b) The polynomial $X^7 + 3X^5 - X^3 + 2X$ is a permutation polynomial of $\mathbb{F}_9$, and that it represents the transposition (1 2).

c) The polynomial $X^r\left(X^{\frac{3(13^{4m}-1)}{4}} + X^{\frac{13^{4m}-1}{2}} + X^{\frac{13^{4m}-1}{4}} + 2\right)$ is a permutation polynomial of $\mathbb{F}_{13^{4m}}$, where $(r, 13^{4m} - 1) = 1$ with $m \geq 1$.

d) The polynomial $X^{469} + X^{313} + X^{157} + 3X$ is a complete permutation polynomial of $\mathbb{F}_{5^4}$.

Examples 6.2 Let α be a primitive element of $\mathbb{F}_{49}$. By putting $\beta = \alpha^4$ we get that $\beta^{12} = 1$. And it is clear that $\beta \neq 1$ and $\beta \neq -3$. Set $\gamma = \frac{\beta+3}{\beta-1}$, then we have

$$\left(\frac{\gamma+3}{\gamma-1}\right)^{\frac{49-1}{4}} = \beta^{12} = 1.$$

Therefore we find that the polynomial $X^r(X^{36} + X^{24} + X^{12} + \gamma)$ is a permutation polynomial of $\mathbb{F}_{49}$, where $(r, 48) = 1$.

7 CONCLUSION

In this paper, we have introduced and studied the following two classes of polynomials $h(X) = X^r f\left(X^{\frac{q-1}{4}}\right)$ and $t(X) = X^r g\left(X^{\frac{q-1}{4}}\right)$ such that $f(X) = X^3 + \delta X^2 + \delta^2 X + \delta^3 + 1$ and $g(X) = X^3 + X^2 + X + \gamma$, where δ and γ belong to finite field $\mathbb{F}_q$. From these classes, we determine new families of permutation and complete permutation polynomials of $\mathbb{F}_q$.

In the next work, we will try to generalize our results from the present paper, so we will study the class of composite polynomials over a finite field $\mathbb{F}_q$ of the form

$$X^r f\left(X^{\frac{q-1}{d}}\right), \text{ such that } r, d \in \mathbb{N}^* \ (d \geq 2),\ q \equiv 1 \pmod{d} \text{ and } f \in \mathbb{F}_q[\mathrm{X}].$$

Acknowledgements: The author would like to thank the anonymous referees for their careful reading that will lead to the final version of this manuscript.

REFERENCES

[1] C. Hermite, "Sur les fonctions de sept lettres", *C. R. Acad. Sci-Paris*, **57**, 750-757 (1863).
[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**, 65-120, 161-183 (1897).
[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, Teubner (1901), New York, Dover (1958).
[4] J. Levine, J. V. Brawley, "Some cryptographic applications of permutation polynomials", *Cryp- tologia*, **1**, 76-92 (1977).
[5] R. Lidl, W. B. Mullen, "A note on polynomials and functions in algebraic cryptography", *Ars Combin*, **17**, 76-92 A (1977).
[6] R.Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press Cambridge, (1986).
[7] D. Q. Wan, R. Lidl, "Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure", *Monatsh. Math*, **112**, 149-163 (2) (1991).
[8] R. Lidl, G.L. Mullen, "When does a polynomial over a finite field permute the elements of the field", *Amer. Math. Monthly*, **95**, 243-246 (1988).
[9] R. Lidl, G.L. Mullen, "When does a polynomial over a finite field permute the elements of the field", *Amer. Math. Monthly*, **100**, 71-74 (1993).
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, second edition (1997).

Received, July 27, 2022