Comm. Korean Math. Soc. **10** (1995), No. 4, pp. 823–829

PERMUTATION POLYNOMIALS OF THE TYPE $x^{1+\frac{q-1}{m}} + ax$

SEOG YOUNG KIM AND JUNE BOK LEE

ABSTRACT. In this paper, we prove that $x^{1+\frac{q-1}{5}} + ax$ $(a \neq 0)$ is not a permutation polynomial over F_{q^r} $(r \geq 2)$ and we show some properties of $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ over F_{q^r} $(r \geq 2)$.

1. Introduction

Let F_q denote the finite field of order $q = p^n$, p a prime number. A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial of F_q if $f(x)$ induces a 1-1 map of F_q onto itself.

In 1962, Carlitz[1] proved that the polynomial $x^{1+\frac{q-1}{2}} + ax(a \neq 0)$ is not a permutation polynomial over any field F_{q^r} $(r \geq 2)$. Then he rasied the question of whether the same conclusion is also held for the polynomial $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ with $m \geq 3$. In 1987, Daqing Wan[2] gave an answer to this question in the case $p \neq 2$, $m = 3$.

In this paper, we give an answer to question for $p \neq 2$, $m = 5$, and we will discuss some facts about $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$, where $q \equiv 1 \pmod{m}$.

In the following we assume that $q = p^n$, p a prime unless stated otherwise.

LEMMA 1.1 ([2]). *Let $1 < k < q$, $q - 1 = k([\frac{q-1}{k}] - t) + tk + j, 0 \leq j < k$, $0 \leq t < [\frac{q-1}{k}]$. Put $J = [\frac{q-1}{k}] - t + tk + j$ and suppose $p \nmid \binom{J}{tk+j}$. If $q - 1 > (k-1, q-1)((t+1)k - 1)$, then $f(x) = x^k + ax(a \neq 0)$ is not a permutation polynomial over F_q.*

Received May 20, 1995. Revised June 26, 1995.
1991 AMS Subject Classification: 11T06.
Key words and phrases: Finite Fields, Permutation Polynomial.

THEOREM 1.2 ([4]). *Let $1 < k < q$, k be not a power of p, $q \geqq (k^2 - 4k + 6)^2$, then $x^k + ax$ $(a \neq 0)$ is not a permutation polynomial over F_q.*

THEOREM 1.3 ([5]). *Let p be a prime number, and*

$$m = \sum_{i=0}^{l} m_i p^i \quad \text{and} \quad k = \sum_{i=0}^{l} k_i p^i$$

be representations of m and k to the basis p, that is, $0 \leq m_i,\ k_i < p$. Then

$$\binom{m}{k} = \prod_{i=0}^{l} \binom{m_i}{k_i} \quad \text{mod } p.$$

THEOREM 1.4 ([3]). *If k is a divisor of $q-1$, then there is no permutation polynomial of degree k over F_q .*

2. Results

We discuss whether or not $x^{1+\frac{q-1}{m}} + ax$ is a permutation polynomial over F_{q^r} $(r \geq 2)$. First, we know that if $r \geq 4$ then $x^{1+\frac{q-1}{m}} + ax\,(a \neq 0)$ is not a permutation polynomial over F_{q^r} because of the following and Theorem 1.2;

$$\left(\left(1+\frac{q-1}{m}\right)^2 - 4\left(1+\frac{q-1}{m}\right)+6\right)^2 \leq \left(\frac{q-m-1}{m}+\sqrt{2}\right)^4$$
$$\leq \left(\frac{q+m-1}{m}\right)^4 < q^r \text{ for } r \geq 4.$$

Thus, we need only consider the cases $r = 2$ and $r = 3$.

THEOREM 2.1. *$x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ is not a permutation polynomial over F_{q^2} if $p > m^2 - m$ and $q > m^3 - 2m^2 - m + 1$ with $m \geq 3$.*

PROOF. Let $k = \frac{q+m-1}{m}$. Since $q \geq m^3 - 2m^2 - m + 1$, $\left[\frac{q^2-1}{k}\right] = mq + (m - m^2)$. Then

$$\begin{aligned} q^2 - 1 &= k\left(\left[\frac{q^2-1}{k}\right] - t\right) + tk + j \\ &= k(mq + (m - m^2) - t) + tk + j \\ &= q^2 - (m-1)^2 + j, \quad \text{where } j = (m-1)^2 - 1. \end{aligned}$$

Let $J = \left[\frac{q^2-1}{k}\right] - t + tk + j$. Then

$$\begin{aligned} J &= mq + (m - m^2) - t + t\left(\frac{q+m-1}{m}\right) + (m-1)^2 - 1 \\ &= mq - m + t\frac{q-1}{m}, \\ tk + j &= t\left(\frac{q+m-1}{m}\right) + (m-1)^2 - 1 \\ &= t\left(\frac{q+m-1}{m}\right) + m^2 - 2m. \end{aligned}$$

Take $t = 0$, then

$$\begin{aligned} J &= mq - m \\ &= (m-1)q + (p-1)\frac{q}{p} + \cdots + (p-1)p + p - m, \\ tk + j &= m^2 - 2m. \end{aligned}$$

Since $p > m^2 - m$, $\binom{J}{tk+j} \not\equiv 0 \mod p$ by Theorem 1.3. Note that $q^2 - 1 > (\frac{q-1}{m})(\frac{q-1}{m}) = (\frac{q-1}{m})^2$. Now, Lemma 1.1. can be applied. □

By the same method of the proof of Theorem 2.1 we can prove the following:

THEOREM 2.2. $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ *is not a permutation polynomial over* F_{q^3} *if* $p > m^2 - m$, *and* $q > m + (m-1)(m(m-1)^2 - 1)$ *with* $m \geq 3$.

Theorem 2.1 and 2.2 have a lower bound of p. Thus we can not say that $x^{1+\frac{q-1}{m}} + ax$ is not a permutation polynomial over F_{q^r} for each m. However when $m = 5$, we can say that $x^{1+\frac{q-1}{m}} + ax$ is not a permutation polynomial over $F_{q^r} (r \geq 2)$ for all $p \neq 2$, $q \equiv 1 \pmod{m}$.

THEOREM 2.3. *Let $q \equiv 1 \pmod 5$, $p \neq 2$, then $x^{1+\frac{q-1}{5}} + ax$ $(a \neq 0)$ is not a permutation polynomial over any finite field F_{q^r} $(r \geq 2)$.*

We need some Lemmas to prove Theorem 2.3.

LEMMA 2.4. *Let $p = 17$ or 19, $q > 71$, then*

$$\binom{6q-6}{q+19} \not\equiv 0 \mod p.$$

PROOF. We have

$$\begin{aligned} 6q - 6 &= 5q + (p-1)\frac{q}{p} + \cdots + (p-1)p + p - 6, \\ q + 19 &= q + 17 + 2 \quad \text{for} \quad p = 17 \\ \text{or} \quad q + 19 &= q + 19 \quad \text{for} \quad p = 19. \end{aligned}$$

Then by Theorem 1.3, we obtain

$$\binom{6q-6}{q+19} \equiv \binom{5}{1}\binom{p-1}{1}\binom{p-6}{2} \not\equiv 0 \mod p \quad \text{if} \quad p = 17$$

and

$$\binom{6q-6}{q+19} \equiv \binom{5}{1}\binom{p-1}{1} \not\equiv 0 \mod p \quad \text{if} \quad p = 19. \quad \square$$

LEMMA 2.5. *Let $p = 3$, $q > 71$, then*

$$\binom{8q-8}{3q+27} \not\equiv 0 \mod p.$$

PROOF. This follows from Theorem 1.3. $\square$

LEMMA 2.6. *Let $p = 17$, $q > 321$, then*

$$\binom{5q^2-3q-2}{17q+3} \not\equiv 0 \mod p.$$

PROOF. We have

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

Then by Theorem 1.3, we have

$$\binom{5q^2-3q-2}{17q+3}\equiv\binom{p-1}{1}\binom{p-2}{3}\not\equiv 0 \mod p \text{ for } p=17. \quad \square$$

Similarly, we can prove the following two lemmas.

LEMMA 2.7. *Let* $p\neq 3,17,19$, *and* $q>321$, *then*

$$\binom{5q^2-4q-1}{16q-1}\not\equiv 0 \mod p.$$

LEMMA 2.8. *Let* $p=3$ *or* 19, $q\geq 321$, *then*

$$\binom{5q^2-q-4}{19q+11}\not\equiv 0 \mod p.$$

PROOF. of Theorem 2.3: We already showed that if $r\geq 4$, then the Theorem holds.

Now assume that $r=2$. If $q>71$, then

$$\begin{aligned} q^2-1 &> \frac{q-1}{5}\left(16\left(\frac{q+4}{5}\right)-1\right)\\ &> \frac{q-1}{5}\left(6\left(\frac{q+4}{5}\right)-1\right)\\ &> \frac{q-1}{5}\left(\frac{q+4}{5}-1\right).\end{aligned}$$

and

$$\begin{aligned} q^2-1 &= \frac{q+4}{5}\left(\left[\frac{q^2-1}{k}\right]-t\right)+t\left(\frac{q+4}{5}\right)+j, \text{ where } k=\frac{q+4}{5}\\ &= q^2-16+j.\end{aligned}$$

Then $j = 15$, $J = 5q-5+t(\frac{q-1}{5})$, and $tk+j = t(\frac{q+4}{5})+15$ in Lemma 1.1. We take $t = 0$, and so $J = 5q-5$, $tk+j = 15$. According to Theorem 1.3,

$$\binom{j}{tk+j} \equiv \binom{5q-5}{15} \not\equiv 0 \mod p.$$

if $q > 71$ and $p \neq 3, 17, 19$, so in this csae our result follows. If $p = 3$, $q > 71$, then we can take $t = 15$ and Lemma 2.5 implies it. If $p = 17$ or 19, $q > 71$, then we can take $t = 5$ and Lemma 2.4 implies it. If $q = 41$ or 61, then we can take $t = 0$ and Lemma 1.1 implies it. If $q = 11$ or 31, then Theorem 1.2 implies it. If $q = 71$, then $k = 1 + \frac{q-1}{5} = 15$ and k divides $q^2 - 1 = 5040$ and so Theorem 1.4 can be applied.

Assume that $r = 3$. If $q \leq 321$, then when $k = 1+\frac{q-1}{5}$, $(k^2-4k+6)^2 \leq q^3$, and by Theorem 1.2, our result follows. Let $q > 321$, then

$$\begin{aligned} q^3 - 1 &> \frac{q-1}{5}\left(95\left(\frac{q+4}{5}\right) - 1\right) \\ &> \frac{q-1}{5}\left(80\left(\frac{q+4}{5}\right) - 1\right). \end{aligned}$$

Now $q^3 - 1 = \frac{q+4}{5}(5(q^2-4q+16)-1) + \frac{q+4}{5} - 65$, $j = \frac{q+4}{5} - 65$. If $p \neq 3, 17, 19$, then taking $t = 79$

$$\begin{aligned} J &= 5(q^2 - 4q + 16) - 1 + \frac{q+4}{5} - 65 - t + t\left(\frac{q+4}{5}\right) \\ &= 5q^2 - 20q + 14 - t + (t+1)\frac{q+4}{5} \\ &= 5q^2 - 4q - 1, \\ tk + j &= t\left(\frac{q+4}{5}\right) + \frac{q+4}{5} - 65 \\ &= 16q - 1. \end{aligned}$$

According to Lemma 2.7,

$$\binom{J}{tk+j} \equiv \binom{5q^2-4q-1}{16q-1} \not\equiv 0 \mod p.$$

Hence Lemma1.1 shows that $f(x)$ is not a permutation polynomial over F_{q^r}. If $p=3$ or 19, taking $t=94$, then $J=5q^2-q-4$, $tk+j=19q+11$. By Lemma 2.8, it can be proved. If $p=17$, taking $t=84$, then $J=5q^2-3q-2$, $tk+j=17q+3$. By Lemma 2.6, it can be proved. Thus Theorem 2.3 is proved completely. □

Though $x^{1+\frac{q-1}{m}}+ax$ is not a permutation polynomial over $F_{q^r}(r\geq 2)$ for $m=2,3$, and 5, we can not say that it does hold for $m=4$. However, if $p\neq 2,3,5$, then it is true for $m=4$. And because 2, 3, and 5 are prime numbers, we may assume that it is true for $m=7$ or another prime numbers, but it is still unproved.

References

1. Carlitz, L., *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc **68** (1962), 120-122.
2. D. Wan, *Permutation Polynomial over Finite Fields*, Acta Mathematica Sinica, New Series **3** (1987), 1-5.
3. Lidl, R. & Neiderreiter, H., *Finite Fields,*, Encyclopedia Math. Appl. **20** Addison-Wesley (1983), Chap 7.
4. Neiderreiter, H. & Robinson, K. H., *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser.A **33** (1982), 197-212.
5. Van Lint, L. H., *Introduction to Coding Theory*, Springer-Verlag, New York, 1982.

Department of Mathematics
Yonsei University
Seoul,120-749, Korea