Journal of Mathematical Research with Applications
Mar., 2023, Vol. 43, No. 2, pp. 166–174
DOI:10.3770/j.issn:2095-2651.2023.02.005
Http://jmre.dlut.edu.cn

Permutation Polynomials of $x^{1+\frac{q-1}{m}}+ax$

Danyao WU[1,*], **Pingzhi YUAN**[2]

1. *School of Computer Science and Technology, Dongguan University of Technology, Guangdong* 523808*, P. R. China;*
2. *School of Mathematics, South China Normal University, Guangdong* 510631*, P. R. China*

Abstract Let m be a positive integer and F_{q^r} be a finite field with the characteristic of p. We prove that if $p>m^2-m$ and $q\equiv 1 \pmod m$, the polynomial $x^{1+\frac{q-1}{m}}+ax$ $(a\neq 0)$ is not a permutation polynomial over F_{q^r} $(r\geq 2)$. And we verify that if $q\equiv 1 \pmod 7$ and $p\neq 2,3$, then the polynomial $x^{1+\frac{q-1}{7}}+ax$ $(a\neq 0)$ is not a permutation polynomial over F_{q^r} $(r\geq 2)$.

Keywords polynomial; permutation polynomial; finite field

MR(2020) Subject Classification 11T06; 12E10

1. Introduction

Let q be a prime power, F_q be the finite field of order q, and $F_q[x]$ be the ring of polynomials in a single indeterminate x over F_q. A polynomial $f(x)\in F_q[x]$ is called a permutation polynomial of F_q if it induces a one-to-one map from F_q to itself. These polynomials first arose in work of Betti [1] and Hermite [2] as a way to represent permutations. A general theory was developed by Hermite [2] and Dickson [3], with many subsequent developments by Carlitz and others.

The simplest class of nonconstant polynomials are the monomials x^n with $n>0$, and one easily checks that x^n permutes F_q if and only if n is coprime to $q-1$. However, the question of whether binomials are permutation polynomials or not is much more mysterious. Given $f(x)=x^m+ax^n\in F_q[x]$ with $0<n<m<q$ and $a\neq 0$, Hou [4] told us that there exist integers r, t, $d>0$ with $\gcd(t,q-1)=1$ and $d|(q-1)$ such that $f(x^t)\equiv x^r(x^{(q-1)/d}+a) \pmod{x^q-x}$. Therefore, if a binomial in a statement is assumed to be of the form $x^r(x^{(q-1)/d}+a)$, no generality is lost. Carlitz and Wells [5] relied on a bound on the Weil sum of a multiplicative character of F_q (see [6]) to prove that for fixed integers $d>1$ and $c>0$, when q is sufficiently large and satisfies the conditions $d|(q-1)$ and $\gcd(c,q-1)=1$, there exists $a\neq 0$ such that $x^r(x^{(q-1)/d}+a)^k$ is a permutation polynomial over F_q (Note that $k=1$, the polynomial is a binomial). Using the Hasse-Weil bound on the number of degree one places of an algebraic function field over F_q (see [7]), Masuda and Zieve [8] refined a result of Carlitz-Wells. They showed that if $q\geq 4$

Received November 10, 2021; Accepted November 25, 2022
Supported by the National Natural Science Foundation of China (Grant No. 12171163) and the Guangdong Basic and Applied Basic Research Foundation (Grant No. 2020A1515111090).

[*] Corresponding author

E-mail address: wudanyao111@163.com (Danyao WU); yuanpz@scnu.edu.cn (Pingzhi YUAN)

and $(q-1)/d > 2q(\log\log q)/\log q$, then there exists $a \neq 0$ such that $x^r(x^{(q-1)/d}+a)$ is a permutation polynomial over F_q. Moreover, they obtained an estimate for the number of a's with this property.

From the nonexistence perspective, Niederreiter and Robinson [9] used Riemann Hypothesis for curves over finite fields to verify that x^m+ax $(a \neq 0)$ is not a permutation polynomial over F_q if $q \geq (m^2-4m+6)^2$. Turnwald [10] improved this result by considering Weil's bound [11] for the number of F_q-rational points on the curve $(f(x)-f(y))/(x-y)$. He proved that $f(x)=x^m+ax^n$ with $m > n > 0$ and $a \neq 0$ is not a permutation polynomial over F_q if $q > (m-2)^2+4m-4$ and $m \neq np^i$; here, p denotes the characteristic of F_q. There are some results on binomial $x^{1+\frac{q-1}{m}}+ax$ $(q \equiv 1 \pmod{m})$ over F_{q^r}. For $r=1$, Carlitz [5] showed that for sufficiently large q there exists $a \in F_q^*$ for which $x^{1+\frac{q-1}{m}}+ax$ is a permutation polynomial over F_q. For $r \geq 2$, Carlitz [12] proved that the binomial $x^{1+\frac{q-1}{2}}+ax$ (q odd, $a \neq 0$) cannot be a permutation polynomial of F_{q^r}, and he raised the same question for $x^{1+\frac{q-1}{3}}+ax$ $(q \equiv 1 \pmod{3}, a \neq 0)$. Wan [13] answered Carlitz's question in the case $p \neq 2$. Kim and Lee [14] proved that $x^{1+\frac{q-1}{5}}+ax$ $(q \equiv 1 \pmod{5}, a \neq 0)$ cannot be a permutation polynomial of F_{q^r} for $p \neq 2$. Then they also conjectured that the polynomial $x^{1+\frac{q-1}{7}}+ax$ $(q \equiv 1 \pmod{7}, a \neq 0)$ is not a permutation polynomial over F_{q^r}. More generally, one may consider $x^{1+\frac{q-1}{m}}+ax \in F_{q^r}[x]$, where $q \equiv 1 \pmod{m}$, $m \geq 2$, $a \neq 0$. Clearly, if $m = \frac{q-1}{p^i-1}$, where $F_{p^i} \subset F_{q^r}$, then $x^{1+\frac{q-1}{m}}+ax = x^{p^i}+ax$, which is a permutation polynomial of F_{q^r} if and only if $(-a)^{(q^r-1)/(p^i-1)} \neq 1$. When $1+\frac{q-1}{m}$ is not a power of p, it is not known if the binomial can be a permutation polynomial of F_{q^r}.

In this paper, we give some properties of $x^{1+\frac{q-1}{m}}+ax$ $(a \neq 0)$ over $F_{q^r}[x]$ $(r \geq 2)$ and show that a polynomial of the form of $x^{1+\frac{q-1}{7}}+ax$ $(a \neq 0)$ is not a permutation polynomial of F_{q^r} $(r \geq 2)$, where $q \equiv 1 \pmod{7}$ and $p \neq 2, 3$.

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

2. Auxiliary results

We now present some auxiliary lemmas that will be needed in the sequel.

First, we give Hermite's criterion. The interest in this criterion is utilizing the degrees of the power of the polynomial to determine whether the one is permutation.

Lemma 2.1 ([15, Theorem 7.4]) *A polynomial $f(x) \in F_q[x]$ is permutation polynomial if and only if*

(1) For each i with $0 < i < q-1$, the reduction of $f^i(x)$ modulo x^q-x has degree less than $q-1$ and

(2) $f(x)$ has precisely one root in F_q.

Wan [13] established the following result about the binomial. Actually, Hermite's criterion can produce this outcome. For convenience of exposition of the Theorem 3.5, we still list here.

Lemma 2.2 ([13]) *Let $1 < k < q$, $q-1 = k([\frac{q-1}{k}]-t)+tk+j_0$, $0 \leq j_0 < k$, $0 \leq t < [\frac{q-1}{k}]$. Put $J = [\frac{q-1}{k}]-t+tk+j_0$ and suppose $p \nmid \binom{J}{tk+j_0}$. 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.

To determine p being not a divisor of $\binom{J}{tk+j_0}$ in Lemma 2.2 and the coefficients of the expansion of $f^i(x)$ in Lemma 2.1, we require the following two lemmas.

Lemma 2.3 ([16]) *Let p be a prime and*

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

be representations of m and k to the basis p, where $0 \leq m_i,\ k_i \leq p-1$. Then

$$\binom{m}{k} \equiv \prod_{i=0}^{l} \binom{m_i}{k_i} \pmod{p}.$$

Let $\upsilon_p(n)$ be the exponent of the highest power of p that divides n. Furthermore, we denote by $\lfloor t \rfloor$ the greatest integer $\leq t$.

Lemma 2.4 ([15, Lemma 6.39]) *For any nonnegative integer n and any prime p we have*

$$\upsilon_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor = \frac{n - s_n}{p-1},$$

where s_n is the sum of digits in the representation of n to the base p.

At last, we list the relationship between the degree of permutation binomials and the order of the finite field.

Lemma 2.5 ([10]) *If there is a permutation polynomial of F_q of the form $x^s + ax^t$, where $s > t > 0$ and $a \in F_q^*$, then either $\frac{s}{t}$ is a power of p or $q \leq (s-2)^4 + 4s - 4$.*

3. Main results

We discuss whether $x^{1+\frac{q-1}{m}} + ax$ is a permutation polynomial over F_{q^r} or not. We know that if $m = \frac{q-1}{p^t-1}$ with t being a divisor of n, we have that

$$x^{1+\frac{q-1}{m}} + ax = x^{p^t} + ax$$

is a p-polynomial over F_{q^r}. Then $x^{p^t} + ax$ is a permutation polynomial over F_{q^r} if and only if $-a$ is not a (p^t-1)th power of an element of $F_{q^r}^*$. If $m \neq \frac{q-1}{p^t-1}$ with t being a divisor of n and $r \geq 4$, we have that $1 + \frac{q-1}{m}$ is not a power of p and

$$q^r > (1 + \frac{q-1}{m} - 2)^4 + 4(1 + \frac{q-1}{m}) - 4.$$

By Lemma 2.5, $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ is not a permutation polynomial over F_{q^r}.

Therefore, for $m \neq \frac{q-1}{p^t-1}$ with t being a divisor of n, we only need to consider the cases $r = 2$ and $r = 3$.

Kim and Lee [14] gave the following properties of $x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ over F_{q^r} $(r = 2, 3)$.

Proposition 3.1 ([14]) *$x^{1+\frac{q-1}{m}} + ax$ $(a \neq 0)$ is not a permutation polynomial over F_{q^2} if*

$p > m^2-m$ and $q > m^3-2m^2-m+1$ with $m \geq 3$.

Proposition 3.2 ([14]) *$x^{1+\frac{q-1}{m}}+ax$ ($a \neq 0$) 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 $m \geq 3$.*

Here, we give an alternative proof to the above Propositions. In all proofs, techniques used here are different from the ones used in [14]. As a result, condition $q > m^3-2m^2-m+1$ of Proposition 3.1 and condition $q > m+(m-1)(m(m-1)^2-1)$ of Proposition 3.2 are deleted.

Theorem 3.3 *For a prime power q and a positive integer m with $q \equiv 1 \pmod{m}$, the polynomial $x^{1+\frac{q-1}{m}}+ax$ ($a \neq 0$) is not a permutation binomial over F_{q^2}, if p satisfies one of the following conditions:*

(i) $p > m^2-m$;

(ii) $p < m^2-m < p^2$ and $t+m \leq p$, where t is the least nonnegative residue of m^2-2m modulo p.

Proof In Lemma 2.1, let $i = mq-m$. Then it will suffice to show that the reduction of

$$(x^{1+\frac{q-1}{m}}+ax)^{mq-m} \pmod{x^{q^2}-x}$$

has degree q^2-1. Now

$$\begin{aligned}(x^{1+\frac{q-1}{m}}+ax)^{mq-m} &= \sum_{j=0}^{mq-m}\binom{mq-m}{j}a^j x^{(1+\frac{q-1}{m})(mq-m-j)+j}\\ &= \sum_{j=0}^{mq-m}\binom{mq-m}{j}a^j x^{q^2-1+(m-2)(q-1)-\frac{q-1}{m}\cdot j}.\end{aligned}$$

For $j > m(m-2)$, the corresponding exponent of x are $\leq q^2-2$. For $j < m(m-2)$, the corresponding exponent of x are easily seen to be $\geq q^2$ and $\leq 2q^2-3$, so that after reduction of these terms $\pmod{x^{q^2}-x}$ we get monomials of degree $\leq q^2-2$. The only remaining term is the one for $j = m(m-2)$-namely,

$$\binom{mq-m}{m^2-2m}a^{m^2-2m}x^{q^2-1}.$$

It suffices then to prove that the binomial coefficient above is not divisible by the characteristic p of F_q. If s_n is as defined above in Lemma 2.4, then $p > m^2-m$ implies that

$$s_{mq-m} = s_{mq-(m^2-m)} + s_{m^2-2m},$$

hence Lemma 2.4 yields

$$\upsilon_p\left(\binom{mq-m}{m^2-2m}\right) = \frac{1}{p-1}\left(s_{mq-(m^2-m)}+s_{m^2-2m}-s_{mq-m}\right) = 0,$$

which is the desired fact. □

By the same method of the proof of Theorem 3.3, we can prove the following theorem. For convenience of description below, we still give proof.

Theorem 3.4 *Let $q \equiv 1 \pmod{m}$. The polynomial $x^{1+\frac{q-1}{m}}+ax$ ($a \neq 0$) is not a permutation* *binomial over F_{q^3}, if p satisfies one of the following conditions:*

(i) $p > m^2 - m$;

(ii) $p < m^2 - m < p^2$ *and* $t + m \le p$, *where t is the least nonnegative residue of $m^2 - 2m$ modulo p.*

Proof In Lemma 2.1, let $i = mq^2 - (m-1)q - 1$. Then it will suffice to show that the reduction of

$$(x^{1+\frac{q-1}{m}} + ax)^{mq^2-(m-1)q-1} \pmod{x^{q^3} - x}$$

has degree $q^3 - 1$. Now

$$\begin{aligned}&(x^{1+\frac{q-1}{m}} + ax)^{mq^2-(m-1)q-1}\\ &\quad= \sum_{j=0}^{mq^2-(m-1)q-1} \binom{mq^2-(m-1)q-1}{j} a^j x^{(1+\frac{q-1}{m})[mq^2-(m-1)q-1-j]+j}\\ &\quad= \sum_{j=0}^{mq^2-(m-1)q-1} \binom{mq^2-(m-1)q-1}{j} a^j x^{q^3-1+[(m-1)^2q-1-j]\cdot\frac{q-1}{m}}.\end{aligned}$$

For $j > (m-1)^2q - 1$, the corresponding exponent of x are $\le q^3 - 2$. For $j < (m-1)^2q - 1$, the corresponding exponent of x are easily seen to be $\ge q^2$ and $\le 2q^3 - 3$, so that after reduction of these terms $\pmod{x^{q^2} - x}$ we get monomials of degree $\le q^3 - 2$. The only remaining term is the one for $j = (m-1)^2q - 1$-namely,

$$\binom{mq^2-(m-1)q-1}{(m-1)^2q-1} a^{(m-1)^2q-1} x^{q^3-1}.$$

It suffices then to prove that the binomial coefficient above is not divisible by the characteristic p of F_q. If s_n is defined as above in Lemma 2.4, then $p > m^2 - m$ implies that

$$s_{mq^2-(m-1)q-1} = s_{(m-1)^2q-1} + s_{mq^2-(m^2-m+1)},$$

hence Lemma 2.4 yields

$$\begin{aligned}&\upsilon_p\left(\binom{mq^2-(m-1)q-1}{(m-1)^2q-1}\right)\\ &\quad= \frac{1}{p-1}(s_{(m-1)^2q-1} + s_{mq^2-(m^2-m+1)} - s_{mq^2-(m-1)q-1}) = 0,\end{aligned}$$

which is the desired fact. □

Now we discuss the permutation behavior of polynomial of $x^{1+\frac{q-1}{7}} + ax$ $(a \ne 0)$ over F_{q^r} $(r \ge 2)$, where $q \equiv 1 \pmod 7$ and $p \ne 2, 3$, and give the following theorem.

Theorem 3.5 *Let $q \equiv 1 \pmod 7$, $p \ne 2, 3$. Then the polynomial $x^{1+\frac{q-1}{7}} + ax$ $(a \ne 0)$ is not a permutation polynomial over F_{q^r} $(r \ge 2)$.*

We need some lemmas to prove Theorem 3.5.

Lemma 3.6 *Let $p = 5$ and q be a power of p with $q \equiv 1 \pmod 7$. Then*

$$\binom{7q-7}{35} \not\equiv 0 \pmod p.$$

Proof For $p=5$, we have

$$7q-7=pq+q+(p-1)\frac{q}{p}+\cdots+(p-1)p^2+(p-2)p+(p-2) \text{ and } 35=25+10.$$

Then by Lemma 2.3, we obtain

$$\binom{7q-7}{35}\equiv\binom{4}{1}\binom{3}{2}\binom{3}{0}\not\equiv 0 \pmod 5.$$

We are done. □

Lemma 3.7 *Let* $p\in\{13,19,37,41\}$ *and* q *be a power of* p *with* $q\equiv 1 \pmod 7$. *Then*

$$\binom{8q-8}{q+41}\not\equiv 0 \pmod p.$$

Proof We have

$$8q-8=7q+(p-1)\frac{q}{p}+(p-1)\frac{q}{p^2}+\cdots+(p-1)p+(p-8)$$

for $p>8$ and

$$q+41=q+3\times 13+2=q+2\times 19+3=q+37+4.$$

Then by Lemma 2.3, we get

$$\binom{8q-8}{q+41}\equiv\binom{7}{1}\binom{12}{3}\binom{5}{2}\not\equiv 0 \pmod{13},$$
$$\binom{8q-8}{q+41}\equiv\binom{7}{1}\binom{18}{2}\binom{11}{3}\not\equiv 0 \pmod{19},$$
$$\binom{8q-8}{q+41}\equiv\binom{7}{1}\binom{36}{1}\binom{29}{4}\not\equiv 0 \pmod{37},$$
$$\binom{8q-8}{q+41}\equiv\binom{7}{1}\binom{40}{1}\binom{33}{0}\not\equiv 0 \pmod{41}.$$

We are done. □

Lemma 3.8 *Let* $p\in\{5,37\}$ *and* q *be a power of* p. *Then*

$$\binom{7q^2-5q-2}{37q+5}\not\equiv 0 \pmod p.$$

Proof We have

$$\begin{aligned}7q^2-5q-2=&6q^2+(p-1)\frac{q^2}{p}+\cdots+(p-1)pq+(p-6)q+\\&(p-1)\frac{q}{p}+\cdots+(p-1)p+(p-2),\end{aligned}$$

for $p=37$, or

$$\begin{aligned}7q^2-5q-2=&pq^2+q^2+(p-1)\frac{q^2}{p}+\cdots+(p-1)p^2q+\\&(p-2)pq+(p-1)q+\cdots+(p-1)p+(p-2),\end{aligned}$$

for $p=5$ and

$$37q+5=25q+10q+2q+5.$$

Then by Lemma 2.3, we obtain

$$\binom{7q^2-5q-2}{37q+5} \equiv \binom{4}{1}\binom{3}{2}\binom{4}{2}\binom{4}{1} \not\equiv 0 \pmod 5,$$

$$\binom{7q^2-5q-2}{37q+5} \equiv \binom{36}{1}\binom{35}{5} \not\equiv 0 \pmod{37}.$$

We are done. □

Similarly, we can prove the following three lemmas.

Lemma 3.9 *Let $p = 13$ and q be a power of p. Then*

$$\binom{7q^2-3q-4}{39q+17} \not\equiv 0 \pmod{13}.$$

Lemma 3.10 *Let $p = 19$ and q be a power of p. Then*

$$\binom{7q^2-4q-3}{38q+11} \not\equiv 0 \pmod{19}.$$

Lemma 3.11 *Let $p = 41$ and q be a power of p. Then*

$$\binom{7q^2-q-6}{41q+29} \not\equiv 0 \pmod{41}.$$

At last, we give a lemma to explain that if $p \neq 2, 3$, then $1 + (q-1)/7$ is not a power of p.

Lemma 3.12 *Let $1 + (q-1)/7$ be a power of p. Then $p = 2$ or 3.*

Proof Since $1 + (q-1)/7$ is a power of p, there exists a positive integer t such that

$$1 + (q-1)/7 = p^t$$

or

$$7(p^t - 1) = q - 1.$$

We have

$$7p^t - 6 = q,$$

which implies that $p|6$. We get $p = 2$ or 3 by p being a prime. □

Now we show Theorem 3.5.

Proof We already showed that if $p \neq 2, 3$, then $1 + (q-1)/7$ is not a power of p by Lemma 3.12 and for $r \geq 4$, Theorem 3.5 holds. We only need to consider the cases $r = 2$ and $r = 3$.

Assume that $r = 2$. By Theorem 3.3, we need only consider $p \in \{5, 13, 19, 37, 41\}$. Now

$$q^2 - 1 > \frac{q-1}{7}(8 \cdot \frac{q+6}{7} - 1) > (\frac{q-1}{7})^2$$

and we have

$$q^2 - 1 = \frac{q+6}{7} \cdot 7(q-6) + 35.$$

If $p = 5$, we can take $t = 0$ in Lemma 2.2. Then

$$J = 7q - 7, \quad tk + j_0 = 35.$$

According to Lemma 3.6,

$$\binom{7q-7}{35} \not\equiv 0 \pmod{p}.$$

By Lemma 2.2, it can be proved. If $p \in \{13, 19, 37, 41\}$, taking $t = 7$, we have

$$J = 8q - 8, \quad tk + j_0 = q + 41.$$

According to Lemma 3.7,

$$\binom{8q-8}{q+41} \not\equiv 0 \pmod{p}.$$

Lemma 2.2 implies it.

Assume that $r = 3$. By Theorem 3.4, we need only consider $p < 7^2 - 7$. Now

$$\begin{aligned} q^3 - 1 &> \frac{q-1}{7}(286 \cdot \frac{q+6}{7} - 1) > \frac{q-1}{7}(273 \cdot \frac{q+6}{7} - 1) \\ &> \frac{q-1}{7}(266 \cdot \frac{q+6}{7} - 1) > \frac{q-1}{7}(259 \cdot \frac{q+6}{7} - 1) \end{aligned}$$

and

$$q^3 - 1 = \frac{q+6}{7}(7(q^2 - 6q + 36) - 1) + \frac{q+6}{7} - 217.$$

If $p \in \{5, 37\}$ and $\frac{q+6}{7} - 217 \geq 0$, then we have $q > p^2$. Taking $t = 258$, we have

$$J = 7q^2 - 5q - 2, \quad tk + j_0 = 37q + 5.$$

By Lemma 3.8, we have

$$\binom{7q^2-5q-2}{37q+5} \not\equiv 0 \pmod{p}.$$

By Lemma 2.2, it can be proved.

If $p = 13$ and $\frac{q+6}{7} - 217 \geq 0$, we can take $t = 272$. Then

$$J = 7q^2 - 3q - 4, \quad tk + j_0 = 39q + 17.$$

By Lemma 3.9, we have

$$\binom{7q^2-3q-4}{39q+17} \not\equiv 0 \pmod{13}.$$

By Lemma 2.2, it can be proved.

If $p \in \{5, 13, 37\}$ and $\frac{q+6}{7} - 217 \leq 0$, then we only need to consider $q = 13^2$ since $q \equiv 1 \pmod{7}$. Thus, Lemma 2.5 can be applied.

If $p = 19$, we can take $t = 265$. Then

$$J = 7q^2 - 4q - 3, \quad tk + j_0 = 38q + 11.$$

By Lemma 3.10, we have

$$\binom{7q^2-4q-3}{38q+11} \not\equiv 0 \pmod{19}.$$

By Lemma 2.2, it can be proved.

If $p = 41$, we can take $t = 286$. Then

$$J = 7q^2 - q - 6, \quad tk + j_0 = 41q + 29.$$

By Lemma 3.11, we have

$$\binom{7q^2-q-6}{41q+29} \not\equiv 0 \pmod{41}.$$

By Lemma 2.2, it can be proved.

Thus Theorem 3.5 is proved completely. □

Acknowledgements We thank the referees for their time and comments.

References

[1] E. BETTI. *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*. Ann. Sci. Mat. Fis., 1851, **2**: 5–19.

[2] CH. HERMITE. *Sur les fonctions de sept lettres*. C. R. Acad. Sci. Pairs., 1863, **57**: 750–757.

[3] L. E. DICKSON. *The analytic represenntation of substitutions on a power of a prime number of letters with a discussion of the linear group*. Ann. Mat., 1896-1897, **11**: 65–120.

[4] Xiangdong HOU. *A Survey of Permutation Binomials and Trinomials over Finite Fields*. Amer. Math. Soc., Providence, RI, 2015.

[5] L. CARLITZ, C. WELLS. *The number of solutions of a special system of equations in a finite field*. Acta. Math. Sinica (N.S.), 1966, **12**: 77–84.

[6] A. WEIL. *On the Riemann hypothesis in function fields*. Proc. Nat. Acad. Sci. U. S. A., 1941, **27**: 345–347.

[7] H. STICHTENOTH. *Algebraic Function Fields and Codes*. Universitext. Springer-Verlag, Berlin, 1993.

[8] A. M. MASUDA, M. E. ZIEVE. *Permutaiton binomials over finite fields*. Trans. Amer. Math. Soc., 2009, **361**: 4169–4180.

[9] H. NIEDERREITER, K. ROBINSON. *Complete mappings of finite fields*. J. Austral. Math. Soc. Ser. A, 1982, **33**(2): 197–212.

[10] G. TURNWALD. *Permutation Polynomials of Binomial Type*. Hölder-Pichler-Tempsky, Vienna, 1988.

[11] A. WEIL. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Inst. Math. Univ. Strasbourg 7, Hermann, Paris, 1948.

[12] L. CARLITZ. *Some theorems on permutation polynomials*. Bull. Amer. Math. Soc., 1962, **68**: 120–122.

[13] Daqing WAN. *Permutation polynomials over finite fields*. Acta Math. Sinica (N.S.), 1987, **3**(1): 1–5.

[14] S. Y. KIM, J. B. LEE. *Permutation polynomials of the type* $x^{1+((q-1)/m)}+ax$. Commun. Korean Math. Soc., 1995, **10**(4): 823–829.

[15] R. LIDL, H. NIEDERREITER. *Finite Fields*. Cambridge University Press, United Kingdom, 1997.

[16] E. LUCAS. *Théorie des fonctions numériques simplement périodiques*. American J. Math., 1878, **1**(2): 184–196.