Finite Fields and Their Applications 17 (2011) 105–112

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Specific permutation polynomials over finite fields

José E. Marcos *,[1]

Departamento de Algebra, Geometría y Topología, Facultad de Ciencias, Universidad de Valladolid, 47005 Valladolid, Spain

ARTICLE INFO

Article history:
Received 31 July 2008
Revised 6 February 2009
Accepted 12 February 2009
Available online 26 February 2009
Communicated by Rudolf Lidl

Keywords:
Finite field
Permutation polynomial
Complete mapping

ABSTRACT

We present new classes of permutation polynomials over finite fields. If q is the order of the finite field, some of these polynomials have the form $x^r f(x^{(q-1)/d})$, where $d|(q-1)$. We also present some permutation polynomials involving the trace function, which plays an additive role analogous to $x^{(q-1)/d}$. Finally, we present a generalization involving other symmetric functions of $x, x^p, \ldots, x^{q/p}$.

1. Introduction

In this paper, p represents a prime number, $q = p^n$ a prime power, $\mathbb{F}_q$ the finite field of order q, and $\mathbb{F}_q^*$ its multiplicative group. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial over $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ to itself.

In recent years, there has been significant progress in finding new permutation polynomials: see, for instance, [1,2,4,6,7,9,13,16,18–20].

In Section 2, we study a new class of permutation polynomials of the form $x^r f(x^{(q-1)/d})$. Our result is closely related with the results in [20], and partially with [1,8,12,16,19].

In Section 3, we study permutation polynomials involving the trace function. We are able to deduce the permutation behaviour of a polynomial in $\mathbb{F}_q[x]$ from a simpler polynomial in $\mathbb{F}_p[x]$. Our main result is

Theorem 1. *Let $L(x) = a_0x + a_1x^p + \cdots + a_{n-1}x^{p^{n-1}} \in \mathbb{F}_p[x]$ be a linearized polynomial which permutes $\mathbb{F}_{p^n}$. Let $h(x) \in \mathbb{F}_p[x]$, let $\gamma \in \mathbb{F}_{p^n}$, and let $k = \mathrm{Tr}(\gamma) \in \mathbb{F}_p$. The polynomial*

$$f(x) = L(x) + \gamma h\big(\mathrm{Tr}(x)\big)$$

* Fax: +34 983423013.
E-mail address: marcosje@agt.uva.es.

[1] Partially supported by Grant no. VA067A05, Junta Castilla y León.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.02.004

permutes $\mathbb{F}_{p^n}$ *if and only if the polynomial*

$$(a_0 + a_1 + \cdots + a_{n-1})x + kh(x)$$

permutes $\mathbb{F}_p$.

This result provides a class of permutation polynomials involving linearized polynomials and the trace polynomial, but note that our polynomials are not linearized in general. In these permutation polynomials, the trace function plays an additive role analogous to the multiplicative role of $x^{(q-1)/d}$ in the polynomials of the form $x^r f(x^{(q-1)/d})$. In Section 4, we obtain other permutation polynomials involving other symmetric functions of $x, x^p, \ldots, x^{q/p}$.

2. A class of specific permutation polynomials

In this section we present a new class of permutation polynomials of the form $x^r f(x^{(q-1)/d}) \in \mathbb{F}_q[x]$, where $d|(q-1)$. Wan and Lidl [14] studied permutation polynomials of this form. They gave a general criterion [14, Theorem 1.2] to determine whether a polynomial of the above form induces a permutation on $\mathbb{F}_q$. This criterion has been used in [7,8]. Recently, Park and Lee [13, Theorem 2.3] have given a similar criterion, which is simpler and more applicable. See also [19,20, Lemma 2.1] for a shorter proof and some applications. Let μ_d denote the set of dth roots of unity in $\mathbb{F}_q$.

Lemma 2 *(Park and Lee, Zieve). Let* $d, r > 0$ *with* $d|(q-1)$, *and let* $h(x) \in \mathbb{F}_q[x]$. *Then* $f(x) = x^r h(x^{(q-1)/d})$ *permutes* $\mathbb{F}_q$ *if and only if the following two conditions hold*:

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

Condition (1) is also present in [14, Theorem 1.2]. Notice that, if $\gcd(r, (q-1)/d) = s > 1$, then $f(x) = g(x^s)$. Since x^s is not a permutation in $\mathbb{F}_q$, neither is $f(x)$.

For $d \geqslant 2$, we denote

$$h_d(x) = x^{d-1} + x^{d-2} + \cdots + x + 1 \in \mathbb{F}_q[x].$$

Theorem 3. *Let* $3 \leqslant d < q-1$ *satisfy* $d|(q-1)$, $u \geqslant 1$, *and* $0 \leqslant k \leqslant d-1$. *Let* $b \in \mathbb{F}_q$. *The polynomial*

$$g(x) = x^u \left(h_d\left(x^{(q-1)/d}\right) + bx^{k(q-1)/d}\right) \in \mathbb{F}_q[x]$$

is a permutation polynomial if and only if the following four conditions hold:

(1) $b \neq 0$, $d + b \neq 0$ *in* $\mathbb{F}_q$.
(2) $\gcd(u, (q-1)/d) = 1$.
(3) $\gcd(u + k(q-1)/d, d) = 1$.
(4) $(d+b)/b$ *is a* d*th power in* $\mathbb{F}_q$.

Proof. According to Lemma 2, we consider the polynomial

$$\lambda(x) = x^u \left(h_d(x) + bx^k\right)^{(q-1)/d}.$$

The polynomial $g(x)$ is a permutation polynomial if and only if the polynomial $\lambda(x)$ permutes μ_d, the set of dth roots of unity in $\mathbb{F}_q$. Let $\omega \in \mathbb{F}_q$ be a primitive dth root of unity, and so $\mu_d = \{1, \omega, \omega^2, \ldots, \omega^{d-1}\}$.

First assume that the four conditions are satisfied. For each $1 \leqslant i \leqslant d-1$ we have that

$$\lambda(\omega^i) = \omega^{iu}\left(b\omega^{ik}\right)^{(q-1)/d} = b^{(q-1)/d}\left(\omega^i\right)^{u+k(q-1)/d}.$$

By condition (3), we have that the cardinal $\#\{\lambda(\omega^i)\colon\ 1 \leqslant i \leqslant d-1\} = d-1$. On the other side, we have that

$$\lambda(1) = (d+b)^{(q-1)/d}.$$

If $\lambda(1) = \lambda(\omega^i)$ for certain $1 \leqslant i \leqslant d-1$, we get equality

$$\left(\frac{d+b}{b}\right)^{(q-1)/d} = \left(\omega^i\right)^{u+k(q-1)/d}.$$

By condition (4), we have that $((d+b)/b)^{(q-1)/d} = 1$, and by condition (3), we have that $1 \neq (\omega^i)^{u+k(q-1)/d}$, which is a contradiction. Thus, $\lambda(1) \neq \lambda(\omega^i)$. Therefore, $\lambda(x)$ induces a permutation on the set μ_d.

Now we show that the conditions (1)–(4) are necessary for $g(x)$ to be a permutation polynomial. Condition (2) is necessary by Lemma 2. If $b = 0$, then $g(\omega) = 0 = g(0)$. If $d + b = 0$, then $g(1) = 0 = g(0)$.

If $\gcd(u + k(q-1)/d, d) = s > 1$, then $1 < 1 + d/s < d$, and $\lambda(\omega) = \lambda(\omega^{1+d/s})$. Thus, $\lambda(x)$ does not permute μ_d.

Finally, if conditions (1)–(3) are satisfied, but $(d+b)/b$ is not a dth power in $\mathbb{F}_q$, we have that

$$\left(\frac{d+b}{b}\right)^{(q-1)/d} = \omega^h, \quad 1 \leqslant h \leqslant d-1.$$

There exists $1 \leqslant i \leqslant d-1$ such that $h \equiv i(k(q-1)/d + u) \pmod{d}$. Thus

$$\left(\frac{d+b}{b}\right)^{(q-1)/d} = \left(\omega^i\right)^{k(q-1)/d+u},$$

and therefore, $\lambda(1) = (d+b)^{(q-1)/d} = \lambda(\omega^i)$. That is, $\lambda(x)$ does not permute μ_d. □

The above theorem can also be proved using [3, Theorem 4.1], or applying [17, Theorem 1].

If b and $d+b$ are non-zero dth powers in $\mathbb{F}_q$, the above theorem is an immediate consequence of [20, Corollary 2.2].

Remark. If d is prime and $u \in d\mathbb{Z}$, then condition (2) implies condition (3).

Remark. If $d = 3$, we get a result included in [8, Theorem 5]. If $d = 3$ and $b = -1$, we obtain [16, Theorem 1].

Remark. If $d = 5$, $k = 4$, and $b = -1$, we get a result included in [1, Theorem 5.4].

If we put $d = 2$ in the above theorem, the four conditions are sufficient for $g(x)$ to be a permutation polynomial, but they are not necessary. The following result [15], [14, Corollary 1.5] shows this fact.

Proposition 4. *Let $q \equiv 3 \pmod 4$. The polynomial $g(x) = x^2(x^{(q-1)/2} + 1 + b) \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if $(1+b)^2 - 1$ is not a square in $\mathbb{F}_q$, if and only if $(2+b)/b$ is not a square in $\mathbb{F}_q$.*

Proof. An immediate consequence of Lemma 2. □

Example. Let $d=4$, $b=-1$, $k=0$, and $u=1$. We assume that $3\neq 0$ in $\mathbb{F}_q$ and $4|(q-1)$. Then

$$g(x)=x\big(x^{3(q-1)/4}+x^{2(q-1)/4}+x^{(q-1)/4}\big)\in\mathbb{F}_q[x]$$

is a permutation polynomial if and only if -3 is a fourth power in $\mathbb{F}_q$. In particular, $g(x)$ induces a permutation in $\mathbb{F}_p$ for the primes $p=37$, 61, 157, 193, 313, 349, 373, ...

Example. Let $d=6$, $b=-3$, $k=0$, and $u=1$. Let p be a prime such that $12|(p-1)$. Then

$$g(x)=x\big(x^{5(p-1)/6}+x^{4(p-1)/6}+x^{3(p-1)/6}+x^{2(p-1)/6}+x^{(p-1)/6}-2\big)\in\mathbb{F}_p[x]$$

is a permutation polynomial.

We fix a finite field $\mathbb{F}_q$ and a number $d\geqslant 3$ such that $d|(q-1)$. It is possible to extend the previous theorem to characterize the permutation polynomials among the polynomials of the form

$$x^u\big(h_d\big(x^{(q-1)/d}\big)+bx^{k(q-1)/d}\big)^s\big(h_d\big(x^{(q-1)/d}\big)+cx^{l(q-1)/d}\big)^t\in\mathbb{F}_q[x],$$
$$b,c\in\mathbb{F}_q,\ 0\leqslant k,l\leqslant d-1,\ s,t\in\mathbb{Z}.$$

It is also possible to include more factors of the same kind. Instead of writing such a general result, we present a concrete example of the type of result that can be proved.

Proposition 5. *Let $\mathbb{F}_q$ be a finite field such that $5|(q-1)$ and $4\neq 0$ in $\mathbb{F}_q$. The polynomial*

$$g(x)=x^5\big(h_5\big(x^{(q-1)/5}\big)-x^{4(q-1)/5}\big)\big(h_5\big(x^{(q-1)/5}\big)-x^{3(q-1)/5}\big)\in\mathbb{F}_q[x]$$

permutes the field $\mathbb{F}_q$ if and only if $\gcd(5,(q-1)/5)=1$ and 4 is a fifth power in $\mathbb{F}_q$.

Proof. Completely analogous to that of Theorem 3. □

3. Permutation polynomials related with the trace function

We use $\mathrm{Tr}(x)$ to denote the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and also to denote the corresponding polynomial, i.e.,

$$\mathrm{Tr}(x)=x+x^p+x^{p^2}+\cdots+x^{p^{n-1}}.$$

Throughout this section we shall assume that $n>1$. The trace function has been used to produce permutation polynomials on finite fields in [4,6,18]. In this section we provide new classes of permutation polynomials involving the trace function.

Let $L(x)=a_0x+a_1x^p+a_2x^{p^2}+\cdots+a_{n-1}x^{p^{n-1}}\in\mathbb{F}_p[x]$ be a linearized polynomial. We shall use the following trivial fact in the sequel.

Lemma 6. *Let $L(x)=a_0x+a_1x^p+\cdots+a_{n-1}x^{p^{n-1}}\in\mathbb{F}_p[x]$ be a linearized polynomial, and let $\mathrm{Tr}(x)=x+x^p+\cdots+x^{p^{n-1}}$ be the trace polynomial. Then, for each $\alpha\in\mathbb{F}_{p^n}$, we have*

$$L\big(\mathrm{Tr}(\alpha)\big)=\mathrm{Tr}\big(L(\alpha)\big)=(a_0+a_1+\cdots+a_{n-1})\,\mathrm{Tr}(\alpha).$$

We now prove the result stated in the introduction:

Proof of Theorem 1. Let $\alpha \in \mathbb{F}_{p^n}$, and let $i = \mathrm{Tr}(\alpha) \in \mathbb{F}_p$. Then $f(\alpha) = L(\alpha) + \gamma h(i)$. It is clear that $f(x)$ is injective on the set

$$T_i = \{\alpha \in \mathbb{F}_{p^n} : \mathrm{Tr}(\alpha) = i\}.$$

Now let $\beta \in \mathbb{F}_{p^n}$, and let $j = \mathrm{Tr}(\beta) \in \mathbb{F}_p$. We assume that $f(\alpha) = f(\beta)$, that is

$$L(\alpha) + \gamma h(i) = L(\beta) + \gamma h(j).$$

We apply the trace to both sides of the equality and we get

$$\mathrm{Tr}\big(L(\alpha)\big) + kh(i) = \mathrm{Tr}\big(L(\beta)\big) + kh(j).$$

Using Lemma 6, we obtain

$$(a_0 + a_1 + \cdots + a_{n-1})i + kh(i) = (a_0 + a_1 + \cdots + a_{n-1})j + kh(j).$$

By hypothesis, we have that $i = j$. Now using the fact that $f(x)$ is injective on T_i, we finally conclude that $\alpha = \beta$. For the converse, note that, if $(a_0 + a_1 + \cdots + a_n)x + kh(x)$ is not injective, then $f(x)$ applies two distinct sets T_i and T_j into a set T_a of the same type. □

Corollary 7. *Let $h(x) \in \mathbb{F}_p[x]$. The polynomial $f(x) = x + h(\mathrm{Tr}(x))$ permutes $\mathbb{F}_{p^n}$ if and only if the polynomial $x + nh(x)$ permutes $\mathbb{F}_p$.*

Example. Let $p \equiv 2 \pmod 3$, let $n \notin p\mathbb{Z}$, and let $h(x) = x^3 - x/n$. Then $f(x) = x + h(\mathrm{Tr}(x))$ permutes $\mathbb{F}_{p^n}$.

Corollary 8. *Let $h(x) \in \mathbb{F}_p[x]$ be any polynomial. Let $\gamma \in \mathbb{F}_{p^n}$ satisfy $\mathrm{Tr}(\gamma) = 0$. Then the polynomial $f(x) = x + \gamma h(\mathrm{Tr}(x))$ permutes $\mathbb{F}_{p^n}$.*

In the situation of the above corollary, note that

$$f^s(x) = \overbrace{f \circ f \circ \cdots \circ f}^{s \text{ times}}(x) = x + s\gamma h\big(\mathrm{Tr}(x)\big)$$

as functions on $\mathbb{F}_{p^n}$. Consequently, $f^p(x) = x$. In this situation, it is clear that $f(x) + ax$ is also a permutation polynomial for any $a \neq -1$, $a \in \mathbb{F}_p$. A permutation polynomial $g(x)$ is called a complete mapping polynomial if $g(x) + x$ is also a permutation polynomial, see [10,11]. Therefore, we have the following result:

Proposition 9. *If $p \neq 2$, the polynomial $f(x)$ in Corollary 8 is a complete mapping polynomial.*

We introduce another class of permutation polynomials similar to the previous one.

Theorem 10. *Let $L(x) = a_0x + a_1x^p + \cdots + a_{n-1}x^{p^{n-1}} \in \mathbb{F}_p[x]$ be a linearized polynomial which permutes $\mathbb{F}_{p^n}$. Let $h(x) \in \mathbb{F}_p[x]$. Let $\gamma \in \mathbb{F}_{p^n}$, let $k = \mathrm{Tr}(\gamma) \in \mathbb{F}_p$, and let $b \in \mathbb{F}_p$. The polynomial*

$$f(x) = bL(x) + h\big(\mathrm{Tr}(x)\big)\big(L(x) + \gamma\big)$$

permutes $\mathbb{F}_{p^n}$ if and only if the following two conditions hold:

- $b + h(i) \neq 0$ *for all* $i \in \mathbb{F}_p$.
- *The polynomial* $g(x) = (b + h(x))(a_0 + a_1 + \cdots + a_{n-1})x + h(x)k$ *permutes* $\mathbb{F}_p$.

Proof. We assume that the two conditions hold. Let $\alpha \in \mathbb{F}_{p^n}$, and let $i = \mathrm{Tr}(\alpha) \in \mathbb{F}_p$. Then

$$f(\alpha) = \big(b + h(i)\big)L(\alpha) + h(i)\gamma.$$

Taking into account the first condition, we see that $f(x)$ is injective on the set

$$T_i = \big\{\alpha \in \mathbb{F}_{p^n} \colon \mathrm{Tr}(\alpha) = i\big\}.$$

Now let $\beta \in \mathbb{F}_{p^n}$, and let $j = \mathrm{Tr}(\beta) \in \mathbb{F}_p$. We assume that $f(\alpha) = f(\beta)$, that is,

$$\big(b + h(i)\big)L(\alpha) + h(i)\gamma = \big(b + h(j)\big)L(\beta) + h(j)\gamma.$$

We apply the trace to both sides of the equality and we get

$$\big(b + h(i)\big)\,\mathrm{Tr}\big(L(\alpha)\big) + h(i)k = \big(b + h(j)\big)\,\mathrm{Tr}\big(L(\beta)\big) + h(j)k.$$

Using Lemma 6, we obtain

$$\big(b + h(i)\big)(a_0 + a_1 + \cdots + a_{n-1})i + h(i)k = \big(b + h(j)\big)(a_0 + a_1 + \cdots + a_{n-1})j + h(j)k.$$

The second condition implies that $i = j$. Now using the fact that $f(x)$ is injective on T_i, we finally conclude that $\alpha = \beta$. For the converse, note that $f(x)$ maps each set T_i bijectively onto a set T_a of the same type. □

Remark. In the previous theorem, we can fix $b = 0$ or $\gamma = 0$, or $L(x) = x$, in order to produce easy examples.

Corollary 11. *Let* $h(x) \in \mathbb{F}_p[x]$. *The polynomial* $f(x) = xh(\mathrm{Tr}(x))$ *permutes* $\mathbb{F}_{p^n}$ *if and only if the following two conditions hold*:

- $h(0) \neq 0$.
- *The polynomial* $g(x) = xh(x)$ *permutes* $\mathbb{F}_p$.

Notice that the first condition above can be replaced with the following one: $h(i) \neq 0$ for all $i \in \mathbb{F}_p$.

Example. Let $p \equiv \pm 2 \pmod 5$. Let $h(x) = x^4 - 5x^2 + 5 \in \mathbb{F}_p[x]$. Then

$$xh(x) = x^5 - 5x^3 + 5x = D_5(x),$$

which is a Dickson polynomial. This polynomial permutes $\mathbb{F}_p$ for all primes $p \equiv \pm 2 \pmod 5$. Therefore, the polynomial

$$f(x) = x\big(\mathrm{Tr}(x)^4 - 5\,\mathrm{Tr}(x)^2 + 5\big)$$

permutes $\mathbb{F}_{p^n}$.

In the above results, we can replace the polynomial $h(x)$ by a rational function $R(x) \in \mathbb{F}_p(x)$ which satisfies the given requirements for $h(x)$. For instance, the Rédei function

$$R_3(x) = \frac{x^3 - 3x}{3x^2 - 1} \in \mathbb{F}_p(x)$$

permutes $\mathbb{F}_p$ if $p \equiv 5$ or 7 (mod 12), see [5]. By Corollary 11, we get that the function

$$f(x) = x\frac{\mathrm{Tr}(x)^2 - 3}{3\,\mathrm{Tr}(x)^2 - 1}$$

permutes $\mathbb{F}_{p^n}$ if $p \equiv 5$ or 7 (mod 12).

Remark. It is clear that some of the previous results can be extended to the following slightly more general situation: if $q = p^s$ is a prime power and $\mathrm{Tr}(x)$ is the relative trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$.

4. Using other similar functions instead of the trace function

It is possible to extend some results of the previous section by replacing the trace function by a polynomial $\lambda(x) \in \mathbb{F}_p[x]$ which satisfies $\lambda(\alpha) \in \mathbb{F}_p$ and $\lambda(\alpha^p) = \lambda(\alpha)$ for all $\alpha \in \mathbb{F}_{p^n}$. We consider the second symmetric polynomial in n variables,

$$s_2(x_1, x_2, \ldots, x_n) = \sum_{1 \leqslant i < j \leqslant n} x_i x_j.$$

Now we define the polynomial

$$\lambda_2(x) = s_2\left(x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}\right) = \sum_{0 \leqslant i < j \leqslant n-1} x^{p^i + p^j},$$

which satisfies the above requirements. We also define another polynomial with similar features:

$$T_2(x) = \mathrm{Tr}\left(x^2\right) = x^2 + x^{2p} + x^{2p^2} + \cdots + x^{2p^{n-1}}.$$

Both polynomials satisfy the following property: if $\alpha \in \mathbb{F}_{p^n}$ and $a \in \mathbb{F}_p$, then $\lambda_2(a\alpha) = a^2\lambda_2(\alpha)$, and $T_2(a\alpha) = a^2 T_2(\alpha)$. Polynomials of this type have been studied in [4].

Proposition 12. *Let $\lambda(x)$ be either $\lambda_2(x)$ or $T_2(x)$. Let $h(x) \in \mathbb{F}_p[x]$. The polynomial $f(x) = xh(\lambda(x))$ permutes $\mathbb{F}_{p^n}$ if the following two conditions hold*:

- $h(0) \neq 0$.
- *The polynomial $g(x) = x(h(x))^2$ permutes $\mathbb{F}_p$.*

Proof. The two conditions imply that $h(i) \neq 0$ for all $i \in \mathbb{F}_p$. Let $\alpha \in \mathbb{F}_{p^n}$, and let $i = \lambda(\alpha) \in \mathbb{F}_p$. Then $f(\alpha) = \alpha h(i)$. It is clear that $f(x)$ is injective on the set

$$L_i = \left\{\alpha \in \mathbb{F}_{p^n} \colon \lambda(\alpha) = i\right\}.$$

Now let $\beta \in \mathbb{F}_{p^n}$, and let $j = \lambda(\beta) \in \mathbb{F}_p$. We assume that $f(\alpha) = f(\beta)$, that is

$$\alpha h(i) = \beta h(j).$$

We apply the function λ to both sides of the equality and we get

$$ih(i)^2 = jh(j)^2.$$

The second condition implies that $i = j$. Hence $\alpha = \beta$. □

Example. Let $a = \pm 2$ in $\mathbb{F}_5$. The polynomial $g(x) = x(x^2 - a)^2 \in \mathbb{F}_5[x]$ permutes $\mathbb{F}_5$. Hence, both polynomials

$$x\big(\lambda_2(x)^2 - a\big), \qquad x\big(\mathrm{Tr}\big(x^2\big)^2 - a\big)$$

permute $\mathbb{F}_{5^n}$.

One can give further results using other homogeneous symmetric polynomials applied to $x, x^p, x^{p^2}, \ldots, x^{p^{n-1}}$.

References

[1] A. Akbary, S. Alaric, Q. Wang, On some classes of permutation polynomials, Int. J. Number Theory 4 (2008) 121–133.
[2] A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, Proc. Amer. Math. Soc. 134 (2005) 15–22.
[3] A. Akbary, Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci. 2007 (2007), doi:10.1155/2007/23408, Article ID 23408.
[4] A. Blokhuis, R.S. Coulter, M. Henderson, C.M. O'Keefe, Permutations amongst the Dembowski–Ostrom polynomials, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications: Proceedings of the Fifth International Conference on Finite Fields and Applications, Springer-Verlag, 2001, pp. 37–42.
[5] L. Carlitz, A note on permutation functions over a finite field, Duke Math. J. 29 (1962) 325–332.
[6] H.D.L. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbf{F}_{2^m}$ related to Dickson polynomials, Finite Fields Appl. 11 (2005) 111–122.
[7] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (2007) 58–70.
[8] J.B. Lee, Y.H. Park, Some permuting trinomials over finite fields, Acta Math. Sci. Engl. Ed. 17 (1997) 250–254.
[9] A.M. Masuda, M.E. Zieve, Permutation binomials over finite fields, Trans. Amer. Math. Soc., in press, arXiv:0707.1108v3 [math.NT].
[10] G.L. Mullen, H. Niederreiter, Dickson polynomials over finite fields and complete mappings, Canad. Math. Bull. 30 (1987) 19–27.
[11] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Austral. Math. Soc. Ser. A 33 (1982) 197–212.
[12] Y.H. Park, J.B. Lee, Permutation polynomials with exponents in an arithmetic progression, Bull. Austral. Math. Soc. 57 (1998) 243–252.
[13] Y.H. Park, J.B. Lee, Permutation polynomials and group permutation polynomials, Bull. Austral. Math. Soc. 63 (2001) 67–74.
[14] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, Monatsh. Math. 112 (1991) 149–163.
[15] D. Wan, Permutation binomials over finite fields, Acta Math. Sinica (N.S.) 10 (1994) 30–35.
[16] L. Wang, On permutation polynomials, Finite Fields Appl. 8 (2002) 311–322.
[17] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, in: Lecture Notes in Comput. Sci., vol. 4893, Springer-Verlag, Berlin, 2007, pp. 119–128.
[18] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. 14 (2008) 482–493.
[19] M.E. Zieve, Some families of permutation polynomials over finite fields, Int. J. Number Theory 4 (2008) 851–857.
[20] M.E. Zieve, On some permutation polynomials over $GF(q)$ of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc., in press, electronically published on December 22, 2008.