Finite Fields and Their Applications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2

Jiyou Li [a,1], David B. Chandler [b], Qing Xiang [b,*,2]

[a] Mathematics Department, Shanghai JiaoTong University, Shanghai 200240, PR China
[b] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

ARTICLE INFO

Article history:
Received 12 February 2010
Accepted 18 July 2010
Available online xxxx
Communicated by Rudolf Lidl

MSC:
11T

Keywords:
Finite field
Multinomial coefficient
Permutation polynomial

ABSTRACT

In Dickson (1896–1897) [2], the author listed all permutation polynomials up to degree 5 over an arbitrary finite field, and all permutation polynomials of degree 6 over finite fields of odd characteristic. The classification of degree 6 permutation polynomials over finite fields of characteristic 2 was left incomplete. In this paper we complete the classification of permutation polynomials of degree 6 over finite fields of characteristic 2. In addition, all permutation polynomials of degree 7 over finite fields of characteristic 2 are classified.

1. Introduction

Let $\mathbb{F}_q$ be a field of q elements, where $q = p^t$, p is a prime. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (**PP**) of $\mathbb{F}_q$ if the induced function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$. Permutation polynomials have been studied extensively in the literature, see [4–8] for surveys of known results on **PP**s.

In [2], Dickson determined all permutation polynomials of degree 6 over finite fields of odd characteristic. The classification of **PP**s of degree 6 over finite fields of characteristic 2 is much more complicated. Concerning **PP**s of general degree $n \geqslant 1$, Carlitz conjectured in 1966 that if q is odd, then for each even positive integer n, there is a constant C_n such that when $q > C_n$, there do not exist **PP**s of degree n over $\mathbb{F}_q$. Carlitz's conjecture was resolved in the affirmative by Fried, Guralnick

[*] Corresponding author.
E-mail addresses: lijiyou@sjtu.edu.cn (J. Li), davidbchandler@gmail.com (D.B. Chandler), xiang@math.udel.edu (Q. Xiang).

[1] Research supported in part by Science and Technology Commission of Shanghai Municipality (Grant No. 09XD1402500).

[2] Research supported in part by NSF Grant DMS 0701049, and by the Overseas Cooperation Fund (Grant 10928101) of China.

1071-5797/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2010.07.001

and Saxl in [3]. Wan [9] generalized the Carlitz conjecture to the following stronger conjecture: If $q > n^4$ and $\gcd(n, q-1) > 1$, then there are no **PP**s of degree n over $\mathbb{F}_q$. The Carlitz–Wan conjecture was proved by Lenstra; an elementary version of Lenstra's proof was given by Cohen and Fried in 1995 [1]. For more details we refer the reader to [3,7,9].

We are concerned with **PP**s of degree 6 or 7 over $\mathbb{F}_{2^t}$. First let us consider the degree 6 case. When t is even, we have $\gcd(6, 2^t - 1) = 3 > 1$. It then follows from the Carlitz–Wan conjecture (Lenstra's theorem) that there are no **PP**s of degree 6 if $2^t > 6^4$. Therefore we have an almost complete classification of degree 6 **PP**s over $\mathbb{F}_{2^t}$ when t is even. Indeed the case where t is even and $t \geqslant 6$ was completely settled by Mertens in 1993, as reported by Mullen [7]. When t is odd, the Carlitz–Wan conjecture (Lenstra's theorem) does not apply since in this case we always have $\gcd(6, 2^t - 1) = 1$.

In this paper, we determine all permutation polynomials of degree 6 over $\mathbb{F}_{2^t}$. This result completes the table of permutation polynomials of degree $\leqslant 6$ given by Dickson in [2]. We include the proof of the classification of **PP**s over $\mathbb{F}_{2^t}$ when t is even. The proof when t is odd is more complicated, but similar to the t even case. In addition, we classify all permutation polynomials of degree 7 over $\mathbb{F}_{2^t}$.

Notation. For $x \in \mathbb{R}$, let $(x)_0 = 1$ and $(x)_k = x(x-1)\cdots(x-k+1)$ for $k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. For $k \in \mathbb{N} = \{0, 1, 2, \ldots\}$ the binomial coefficient $\binom{x}{k}$ is defined by $\binom{x}{k} = \frac{(x)_k}{k!}$. When $x, k \in \mathbb{N} = \{0, 1, 2, \ldots\}$ and $k > x$, we define $\binom{x}{k} = 0$.

2. Preliminaries

In general it is very hard to determine whether a given polynomial is a **PP**. The following well-known criterion is a useful characterization of permutation polynomials over a finite field $\mathbb{F}_q$.

Theorem 2.1 *(Hermite and Dickson). Let $\mathbb{F}_q$ be a finite field of order q, where q is a power of a prime p. Then $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold*:

(1) *$f(x)$ has exactly one root in $\mathbb{F}_q$*;
(2) *for each integer n with $1 \leqslant n \leqslant q-2$ and $n \not\equiv 0 \pmod p$, the reduction of $[f(x)]^n \pmod{x^q - x}$ has degree $\leqslant q-2$.*

Suppose $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_{p^t}[x]$ is a polynomial of degree n. Then we set

$$\psi f(x) = \sum_{i=0}^{n} a_i^p x^i.$$

Lemma 2.2. *If $f(x)$ is a* **PP** *of $\mathbb{F}_q$, then so are $f_1(x) = af(bx+c)+d$ and $\psi f(x)$, for all $a, b \neq 0, c, d \in \mathbb{F}_q$.*

By Lemma 2.2, when considering **PP**s of degree n over $\mathbb{F}_q$ ($q = p^t$), it suffices to consider monic polynomials $f(x)$ of degree n satisfying the conditions that $f(0) = 0$ and the coefficient of x^{n-1} is equal to 0 if $p \nmid n$. Such a **PP** will be called a *normalized* **PP**. For convenience, a monic polynomial in $\mathbb{F}_q[x]$ satisfying the above two conditions will also be called a *normalized polynomial.*

We define an equivalence relation on the set of polynomials over $\mathbb{F}_{2^t}$.

Definition 2.3. In this paper, two polynomials $f(x), g(x) \in \mathbb{F}_{2^t}[x]$ are said to be *equivalent* if either $g(x) = af(bx+c)+d$ or $g(x) = \psi f(x)$, with $a, b \neq 0$, $c, d \in \mathbb{F}_{2^t}$.

For normalized polynomials over $\mathbb{F}_{2^t}$ of degrees 6 or 7, if we are only concerned with their permutation behavior, then Lemma 2.2 also allows us to assume that the coefficient of x^5 is either 0 or 1, by suitable choices of a and b in the lemma (with $c = d = 0$). Let μ be any element of $\mathbb{F}_{2^t}$ such that

$\mathrm{Tr}(\mu) = 1$, where $\mathrm{Tr} : \mathbb{F}_{2^t} \to \mathbb{F}_2$ is the absolute trace. Suppose $f(x) = x^6 + x^5 + bx^4 + cx^3 + dx^2 + ex \in \mathbb{F}_{2^t}[x]$ is a polynomial of degree 6. Then the coefficient of x^4 in $f(x+a)$ is either 0 or μ, where a is a root of $x^2 + x + b$ (if $\mathrm{Tr}(b) = 0$) or of $x^2 + x + b + \mu$ (if $\mathrm{Tr}(b) = 1$), respectively, in $\mathbb{F}_{2^t}$.

We will need the following classical result due to Lucas.

Theorem 2.4 *(Lucas). Let p be a prime, and n, r be positive integers having the following p-adic expansions*:

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k \quad (0 \leqslant a_i \leqslant p-1,\ \forall 0 \leqslant i \leqslant k),$$
$$r = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k \quad (0 \leqslant b_i \leqslant p-1,\ \forall 0 \leqslant i \leqslant k).$$

Then

$$\binom{n}{r} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \pmod p.$$

We will also need to use multinomial coefficients, which we define below. For all n, r, $k_1, \ldots, k_r$ in $\mathbb{N} = \{0, 1, 2, \ldots\}$ with $k_1 + \cdots + k_r = n$ and $r \geqslant 2$, we define the multinomial coefficient $\binom{n}{k_1, k_2, \ldots, k_r}$ by

$$\binom{n}{k_1, k_2, \ldots, k_r} = \frac{n!}{k_1! k_2! \cdots k_r!}.$$

The following theorem is known as the multinomial theorem.

Theorem 2.5. *We have the following expansion*:

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{\substack{k_1 + k_2 + \cdots + k_r = n \\ k_1 \geqslant 0,\ k_2 \geqslant 0,\ \ldots,\ k_r \geqslant 0}} \binom{n}{k_1, k_2, \ldots, k_r} x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r}.$$

The following is the multinomial analogue of the Lucas theorem.

Proposition 2.6. *Let p be a prime, and let $k_1, k_2, \ldots, k_r, n$ be nonnegative integers having the following p-adic expansions*:

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_s p^s \quad (0 \leqslant a_j \leqslant p-1,\ \forall 0 \leqslant j \leqslant s),$$
$$k_i = b_{i0} + b_{i1} p + b_{i2} p^2 + \cdots + b_{is} p^s \quad (0 \leqslant b_{ij} \leqslant p-1,\ \forall 1 \leqslant i \leqslant r,\ 0 \leqslant j \leqslant s).$$

Then

$$\binom{n}{k_1, k_2, \ldots, k_r} \equiv \binom{a_0}{b_{10}, b_{20}, \ldots, b_{r0}} \cdots \binom{a_s}{b_{1s}, b_{2s}, \ldots, b_{rs}} \pmod p.$$

In particular,

$$\binom{n}{k_1, k_2, \ldots, k_r} \not\equiv 0 \pmod p \quad \Leftrightarrow \quad \sum_{i=1}^{r} b_{ij} = a_j, \quad \forall 0 \leqslant j \leqslant s.$$

3. Permutation polynomials of degree 6 over finite fields of characteristic 2

Our aim in this section is to classify all permutation polynomials of degree 6 of $\mathbb{F}_{2^t}$. First we note that in [2], Dickson already obtained some restrictions on the coefficients of these polynomials.

Theorem 3.1 *(Dickson). Let*

$$f(x) = x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex \in \mathbb{F}_{2^t}[x]$$

be a **PP** *of $\mathbb{F}_{2^t}$ such that $f(x) \neq x^6$ and when $t = 5$, $f(x) \neq x^6$, or $x^6 + ax^5 + a^4x^2$. Then*

(1) *when t is even, we have $c = a^3 \neq 0$;*
(2) *when t is odd, we have $a \neq 0$, $c \neq 0$ and $c \neq a^3$.*

Based on this result we obtain the main result of this section.

Theorem 3.2. *Let α and β be roots of $x^3+x+1 \in \mathbb{F}_2[x]$ and $x^4+x+1 \in \mathbb{F}_2[x]$, respectively, in some extension fields of $\mathbb{F}_2$. The following are permutation polynomials of degree* 6 *over $\mathbb{F}_{2^t}$:*

$$\begin{array}{ll}
x^6, & \text{whenever } t \text{ is odd,}\\
x^6+x^5+x^3+x^2+x, & t=3,\\
x^6+x^5+x^3+\alpha x^2+\alpha x, & t=3,\\
x^6+x^5+\alpha x^3, & t=3,\\
x^6+x^5+x^4+x^3+x^2, & t=3,\\
x^6+x^5+x^4+x^3+x, & t=3,\\
x^6+x^5+x^4+\alpha^3x^3+\alpha^4x^2+\alpha^6x, & t=3,\\
x^6+x^5+x^4, & t=3,\\
x^6+x^3+x^2, & t=3,\\
x^6+x^5+x^3+\beta^3x^2+\beta^5x, & t=4,\\
x^6+x^5+\beta^3x^4+x^3+\beta x^2+\beta^6x, & t=4,\\
x^6+x^5+\beta^3x^4+x^3+\beta^8x^2+\beta^{13}x, & t=4,\\
x^6+x^5+x^2, & t=5.
\end{array}$$

All other **PP***s of degree* 6 *over $\mathbb{F}_{2^t}$ are equivalent to one of the above.*

We will prove Theorem 3.2 in two steps. First we deal with the t even case, which was previously handled by Mertens, as reported by Mullen in [7]. We begin with a lemma.

Lemma 3.3. *Let*

$$f(x) = x^6 + x^5 + bx^4 + x^3 + dx^2 + ex$$

be a normalized polynomial in $\mathbb{F}_{2^t}[x]$, and let $[x^k](f(x))^n$ denote the coefficient of x^k in the expansion of $(f(x))^n \pmod{x^q - x}$, where $q = 2^t$. If t is even and $m \geqslant 42$, where $2^t = 6m + 4$, then in $\mathbb{F}_q$ we have

$$\left[x^{6m+3}\right]f(x)^{m+5} = \left(b^8 + 1 + e^4\right)\left(1 + b^2 + e\right) + \left(b^8 + b^4 + d^4\right)\left(e^2 + d^2 + e\right), \tag{3.1}$$

$$\left[x^{6m+3}\right]f(x)^{m+13} = \left(b^{32} + b^{16} + d^{16}\right)\left(1 + b^2 + e^2 + d^2\right). \tag{3.2}$$

Please cite this article in press as: J. Li et al., Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, Finite Fields Appl. (2010), doi:10.1016/j.ffa.2010.07.001

Proof. The highest power of x when we expand $f(x)^{m+13}$ is $6(m+13)$. Since we want to find the coefficient of x^{q-1} in the expansion of $f(x)^{m+13} \pmod{x^q - x}$, the terms we are interested in are of the form $x^{i(q-1)}$, $i \geqslant 1$. Thus if we need to consider the terms $x^{i(q-1)}$, $i \geqslant 2$, it must be that

$$6(m+13) \geqslant 2(6m+3),$$

which is equivalent to $m \leqslant 12$. Since we have assumed that $m \geqslant 42$, we do not need to consider the terms $x^{i(q-1)}$, $i \geqslant 2$, when try to find the coefficient of x^{q-1} in the expansion of $f(x)^{m+13} \pmod{x^q - x}$. The same comment holds true when we try to compute the coefficient of x^{q-1} in the expansion of $f(x)^{m+5} \pmod{x^q - x}$.

By the above comment and the multinomial theorem, the coefficient of x^{q-1} in the expansion of $f(x)^{m+5} \pmod{x^q - x}$ is equal to

$$\sum_{\substack{i_1+i_2+\cdots+i_6=m+5\\ 6i_1+5i_2+4i_3+3i_4+2i_5+i_6=6m+3}} \binom{m+5}{i_1, i_2, \ldots, i_6} b^{i_3} d^{i_5} e^{i_6},$$

where the multinomial coefficient is viewed modulo 2. We can easily find all solutions to the system of equations:

$$\begin{gathered} i_1+i_2+i_3+i_4+i_5+i_6 = m+5; \\ 6i_1+5i_2+4i_3+3i_4+2i_5+i_6 = 6m+3; \\ i_1, i_2, \ldots, i_6 \geqslant 0 \end{gathered}$$

for which the multinomial coefficient $\binom{m+5}{i_1, i_2, \ldots, i_6}$ is 1 modulo 2. We give some details below.

The above system of equations is equivalent to

$$\begin{gathered} i_1+i_2+i_3+i_4+i_5+i_6 = m+5; \\ i_2+2i_3+3i_4+4i_5+5i_6 = 27; \\ i_1, i_2, \ldots, i_6 \geqslant 0. \end{gathered}$$

Note that m has the following 2-adic expansion:

$$m = 2^1 + 2^3 + 2^5 + \cdots + 2^{t-3}, \tag{3.3}$$

and thus

$$m+5 = 1 + 2^1 + 2^2 + 2^3 + 2^5 + \cdots + 2^{t-3}. \tag{3.4}$$

Now, in view of Lucas' theorem and Proposition 2.6, the multinomial coefficient $\binom{m+5}{i_1, i_2, \ldots, i_6}$ vanishes modulo 2 whenever any two of $i_1, \ldots, i_6$ have a 1 in the same digit of the 2-adic expansion. For instance, the solution $(i_1, i_2, i_3, i_4, i_5, i_6) = (m-10, 8, 4, 1, 2, 0)$ gives $\binom{m+5}{m-10, 8, 4, 1, 2, 0} b^4 d^2 = b^4 d^2$ for any $m \geqslant 42$, since

$$\begin{aligned} m+5 &= 1+1\cdot 2^1+1\cdot 2^2+1\cdot 2^3+0\cdot 2^4+1\cdot 2^5+\cdots+1\cdot 2^{t-3}, \\ m-10 &= 0+0\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4+1\cdot 2^5+\cdots+1\cdot 2^{t-3}, \\ 8 &= 0+0\cdot 2^1+0\cdot 2^2+1\cdot 2^3+0\cdot 2^4+0\cdot 2^5+\cdots+0\cdot 2^{t-3}, \\ 4 &= 0+0\cdot 2^1+1\cdot 2^2+0\cdot 2^3+0\cdot 2^4+0\cdot 2^5+\cdots+0\cdot 2^{t-3}, \\ 2 &= 0+1\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4+0\cdot 2^5+\cdots+0\cdot 2^{t-3}, \\ 1 &= 1+0\cdot 2^1+0\cdot 2^2+0\cdot 2^3+0\cdot 2^4+0\cdot 2^5+\cdots+0\cdot 2^{t-3}, \end{aligned}$$

and thus there are no carries in the sum $(m-10)+8+4+1+2+0=m+5$ for any $m \geqslant 42$. The other computations are similar. We omit the details.

Similarly we can find the coefficient of x^{q-1} in the expansion of $f(x)^{m+13} \pmod{x^q-x}$. We leave the details to the reader.

The proof of the lemma is now complete. □

Theorem 3.4. *There are no permutation polynomials of degree* 6 *over* $\mathbb{F}_{2^t}$ *when* $t>4$ *is even.*

Proof. The cases where $t=4$, or 6 are easily checked, for example, by a computer. Thus we assume that $t \geqslant 8$. Write $2^t=6m+4$. Then $m \geqslant 42$.

Assume to the contrary that $f(x)=x^6+ax^5+bx^4+cx^3+dx^2+ex \in \mathbb{F}_{2^t}[x]$ is a permutation polynomial of $\mathbb{F}_{2^t}$. In view of Lemma 2.2 and Theorem 3.1, we may assume that $f(x)=x^6+x^5+bx^4+x^3+dx^2+ex$ (i.e., $a=1$ and $c=a^3=1$). By the Hermite–Dickson criterion, the coefficient $[x^{6m+3}]f(x)^{m+13}$ must be zero. Thus the expression on the right-hand side of (3.2) is equal to zero. We consider two cases.

Case 1. $d^2+e^2+b^2+1=0$. In this case, we have $e=1+b+d$. Then

$$f(x)=x^6+x^5+bx^4+x^3+dx^2+(1+b+d)x.$$

The above $f(x)$ has at least two roots, 0 and 1, in $\mathbb{F}_{2^t}$. So $f(x)$ cannot be a permutation polynomial of $\mathbb{F}_{2^t}$, a contradiction.

Case 2. $d^8+b^{16}+b^8=0$. In this case, we have $d=b^2+b$. Substituting d by $b+b^2$ in (3.1) and by the Hermite–Dickson criterion, we get

$$\bigl(b^8+1+e^4\bigr)\bigl(1+b^2+e\bigr)=0.$$

It follows that $e=1+b^2$, and we have

$$f(x)=x^6+x^5+bx^4+x^3+\bigl(b^2+b\bigr)x^2+\bigl(b^2+1\bigr)x.$$

Once again, $f(x)$ has at least the two roots, 0 and 1, in $\mathbb{F}_{2^t}$, a contradiction.

The proof of the theorem is complete. □

To classify permutation polynomials of degree 6 over $\mathbb{F}_{2^t}$, where t is odd, we need more lemmas. The following lemma is well known, see [4, p. 56].

Lemma 3.5. *The quadratic equation* $x^2+x+b=0$, $b \in \mathbb{F}_{2^t}$, *has a solution in* $\mathbb{F}_{2^t}$ *if and only if* $\mathrm{Tr}(b)=0$.

Lemma 3.6. *Let $c \in \mathbb{F}_q \backslash \{0, 1\}$, where q is an odd power of 2. Then the quintic polynomial*

$$g(x) = x^5 + cx^2 + x + c^2 + c$$

has exactly one root in $\mathbb{F}_q$.

Proof. Suppose to the contrary that g has two roots, $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Set $A := \alpha_1 + \alpha_2$, and $u := \alpha_1\alpha_2$. Then we have the factorization

$$g(x) = \left(x^2 + Ax + u\right)\left(x^3 + Ax^2 + Bx + D\right),$$

where $A, B, D, u \in \mathbb{F}_q$. Setting the coefficients on the left and right equal, we have

$$\begin{aligned} B &= A^2 + u; \\ D &= AB + uA + c \\ &= A^3 + c; \\ AD + uB &= 1 \quad \text{or} \\ &\qquad Ac = A^4 + uA^2 + u^2 + 1; \\ uD &= c^2 + c \quad \text{or} \\ uA^5 + uA(Ac) &= (Ac)^2 + A(Ac). \end{aligned}$$

In the last equation, substituting Ac by $A^4 + uA^2 + u^2 + 1$, we have

$$u^4 + Au^3 + \left(A^4 + A^3 + A\right)u^2 + \left(A^3 + A\right)u + A^8 + A^5 + A + 1 = 0.$$

Making the substitution $u = w + A + 1$, we get

$$w^4 + Aw^3 + \left(A^4 + A^3 + A^2\right)w^2 + A^8 + A^6 = 0. \tag{3.5}$$

Now we note that if $w = 0$, then either $A = 1$ or $A = 0$. If $A = 0$, then $u = \alpha_1 = \alpha_2 = 1$, and substituting into $g(x)$ gives $c = 0$, which we do not allow. If $A = 1$, then $u = w = 0$, and $\{\alpha_1, \alpha_2\} = \{0, 1\}$, which again we do not allow. Thus we can divide both sides of (3.5) by w^4 to get

$$1 + \left(A/w + A^2/w^2\right) + \left(A^4/w^2 + A^8/w^4\right) + \left(A^3/w^2 + A^6/w^4\right) = 0.$$

Since $\mathrm{Tr}(1) = 1$ and the trace of each term in parentheses is zero, taking trace of both sides of the last equation, we get $1 = 0$, which is absurd. Therefore, $g(x)$ has at most one root in $\mathbb{F}_q$.

Now suppose g has no roots in $\mathbb{F}_q$. Then it is either irreducible over $\mathbb{F}_q$, or it factors into irreducible second and third degree polynomials over $\mathbb{F}_q$. In either case, there are at least three roots lying in an extension field whose order is an odd power of 2, a contradiction. The proof is now complete. □

Lemma 3.7. *Let*

$$f(x) = x^6 + x^5 + bx^4 + cx^3 + dx^2 + ex$$

be a normalized polynomial in $\mathbb{F}_{2^t}[x]$, and let $[x^k](f(x))^n$ denote the coefficient of x^k in the expansion of $(f(x))^n \pmod{x^q - x}$, where $q = 2^t$. If t is odd and $m \geqslant 85$, where $2^t = 6m + 2$, then in $\mathbb{F}_{2^t}$ we have

$$\begin{aligned}
E_1 &= \bigl[x^{6m+1}\bigr] f(x)^{m+2}\\
&= b^4(1+c) + \bigl(c^2+b^2c+e\bigr) + \bigl(e^2+cd^2+c^2e\bigr);\\
E_2 &= \bigl[x^{6m+1}\bigr] f(x)^{m+6}\\
&= \bigl(b^{16}+b^8+d^8\bigr)(1+c) + \bigl(1+c^8\bigr)\bigl(e^2+cd^2+c^2e\bigr);\\
E_3 &= \bigl[x^{6m+1}\bigr] f(x)^{m+40}\\
&= \bigl[\bigl(c^{64}+b^{16}c^{64}+b^{64}c^{32}+b^{112}+b^{64}d^{16}+e^{32}+b^{16}d^{32}+c^{32}d^{16}+d^{16}e^{32}\bigr)\bigl(1+c^4\bigr)\\
&\quad + \bigl(c^{64}+b^{96}+b^{64}c^{16}+b^{64}e^{16}+d^{32}+c^{48}+b^{32}e^{16}+c^{16}e^{32}+d^{32}e^{16}\bigr)\bigl(c^8+b^8c^4+e^4\bigr)\\
&\quad + \bigl(c^{64}+b^{96}+b^{80}+b^{64}d^{16}+d^{32}+b^{16}c^{32}+b^{32}d^{16}+b^{16}e^{32}+d^{48}\bigr)\bigl(e^8+c^4d^8+c^8e^4\bigr)\\
&\quad + \bigl(b^{64}+b^{64}c^{16}+c^{32}+b^{32}c^{16}+e^{16}+e^{32}+d^{32}c^{16}+c^{32}e^{16}\bigr)e^{12}\bigr]c.
\end{aligned}$$

Similarly to the proof of Lemma 3.3, the coefficients $[x^{q-1}]f(x)^{m+i}$, for various values of i, can be obtained by hand. One can also use a computer to obtain these coefficients easily. The following are two Maple procedures that we used for this purpose. To use it, one sets the degree, “deg,” as well as “m” and “r”, where $q = \deg * \mathrm{m} + \mathrm{r}$, but the value of “m” is reduced modulo a high enough fixed power of 2. Then typing `hermite (i)` computes $[x^{q-1}]f(x)^{m+i}$. For polynomials of degree higher than 11, the procedures need to be modified slightly.

```
m:=85;r:=2;deg:=6;
nextstage:=proc(ex,monoin,stage,tsum)
  local incr,tempsum,ind,monoout,exout,digit;
  global poly,deg,A,tot;
  exout:=iquo(ex,2,’digit’);incr:=2^stage;
  if tsum+2*incr <= tot then
    nextstage(exout,monoin,stage+1,tsum);
    end if;
  tempsum:=tsum;
  if digit = 1 then
    for ind to deg-1 do
      tempsum:=tempsum+incr;
      if tempsum > tot then  break; end if;
      monoout:=monoin*A[ind]^incr;
      if tempsum=tot then poly:=poly+monoout;break;end if;
      nextstage(exout,monoout,stage+1,tempsum);
      end do;
    end if;
  end proc;

hermite:=proc(u)
  global m,r,deg, A,a,b,c,d,e,f,g,h,i,j,poly,tot;
  local exout;
  description "find [q-1]f^{m+u}";
     a:=’a’;b:=’b’;c:=’c’;d:=’d’;e:=’e’;
     f:=’f’;g:=’g’;h:=’h’;i:=’i’;j:=’j’;
     A:=array(1..10,[a,b,c,d,e,f,g,h,i,j]);poly:=0;
  tot:=deg*u-r+1;exout:=m+u; nextstage(exout,1,0,0); RETURN(poly);
end proc; hermite(2); hermite(6); hermite(40);
```

We are now ready to give the proof of Theorem 3.2 in the case where t is odd. We state the result separately as a theorem.

Theorem 3.8. *Let $f(x)$ be a permutation polynomial of degree* 6 *over $\mathbb{F}_{2^t}$, where t is odd. Then*

(1) *when $t=3$, $f(x)$ is equivalent to one of the degree* 6 *polynomials listed in the statement of Theorem* 3.2;
(2) *when $t=5$, $f(x)$ is equivalent to either x^6 or $x^6+x^5+x^2$*;
(3) *when $t>5$, $f(x)$ is equivalent to x^6.*

Proof. For odd t, we have $\gcd(6, 2^t-1)=1$, thus x^6 is a permutation polynomial of $\mathbb{F}_{2^t}$. Again, the cases where $t<9$ are easily checked by a computer. From now on, we assume that $t \geqslant 9$. We will prove that $f(x)=x^6+ax^5+bx^4+cx^3+dx^2+ex \in \mathbb{F}_{2^t}[x]$ $(f(x) \neq x^6)$ cannot be a permutation polynomial of $\mathbb{F}_{2^t}$ when $t \geqslant 9$.

By way of contradiction, assume that $f(x)=x^6+ax^5+bx^4+cx^3+dx^2+ex \in \mathbb{F}_{2^t}[x]$ $(f(x) \neq x^6)$ is a **PP**. In view of part (2) of Theorem 3.1 and Lemma 2.2, we may assume without loss of generality that

$$f(x)=x^6+x^5+bx^4+cx^3+dx^2+ex,$$

where $c \neq 0$ or 1. By Lemma 3.7 and the Hermite–Dickson criterion, we must have $E_1=0$, $E_2=0$, and $E_3=0$.

Using the equation $E_1=0$ to eliminate the variable d from E_2, we have

$$\begin{aligned} E_5 &:= c^4E_2 \\ &= (c+1)e^8+(c+1)^9e^4+c^4(c+1)^8e \\ &\quad + (c+1)\big(b^{16}+c^8+c^4b^4+c^{12}b^4\big)+c^5(c+1)^8\big(b^2+c\big) \\ &= 0. \end{aligned}$$

For compact expression we introduce

$$\gamma := c(c+1)\big(c^2+b^2\big)+\big(c+b^2\big)^2.$$

Then we have the factorization

$$E_5=(c+1)\cdot E_4\cdot E_6,$$

where

$$\begin{aligned} E_4 &= e^2+(c+1)e+c^4+c^3+\big(b^2+1\big)c^2+b^2c+b^4 \\ &= e^2+(c+1)e+\gamma \end{aligned}$$

and

$$\begin{aligned} E_6 = {} & e^6+(c+1)e^5+\big(\gamma+c^2+1\big)e^4+(c+1)^3e^3+\big(\gamma^2+\big(c^2+1\big)\gamma+c^8+c^4\big)e^2 \\ & + \big((c+1)\gamma^2+c^4(c+1)^5\big)e+\big(\gamma^3+\big(c^8+c^4\big)\gamma+c^4(c+1)^6\big). \end{aligned}$$

Since $c \neq 1$, we must have $E_4=0$ or $E_6=0$.

Similarly, using $E_1 = 0$ to eliminate the variable d from E_3, we get an expression $E_8 := c^{23}E_3$ which can be factored

$$E_8 = (c+1)^4 \cdot {E_4}^4 \cdot {E_7}^4,$$

where

$$\begin{aligned} E_7 = {} & (c+1)e^{11} + \bigl(c^4 + c^3 + b^2c^2 + b^2c + \bigl(b^4+1\bigr)\bigr)e^{10} + \bigl(c^4 + b^8\bigr)e^8 \\ & + \bigl(c^7 + c^6 + b^4c^5 + b^4c^4 + b^4c^3 + b^4c^2 + c + 1\bigr)e^7 \\ & + \bigl(c^9 + \bigl(b^4+b^2\bigr)c^8 + \bigl(b^4+b^2\bigr)c^7 + \bigl(b^6+b^4\bigr)c^6 + \bigl(b^6+b^4\bigr)c^5 \\ & + \bigl(b^6+b^4\bigr)c^4 + \bigl(b^6+1\bigr)c^3 + \bigl(b^{12}+b^8+b^4+b^2\bigr)c^2 + b^2c + \bigl(b^4+1\bigr)\bigr)e^6 \\ & + \bigl(\bigl(b^8+1\bigr)c^5 + \bigl(b^8+1\bigr)c^4 + \bigl(b^{12}+b^4\bigr)c^3 + \bigl(b^{12}+b^4\bigr)c^2\bigr)e^5 \\ & + \bigl(c^{10} + b^4c^8 + \bigl(b^8+1\bigr)c^7 + \bigl(b^{12}+b^{10}+b^8+b^2\bigr)c^6 \\ & + \bigl(b^{12}+b^{10}+b^4+b^2\bigr)c^5 + \bigl(b^{14}+b^6+b^4+1\bigr)c^4 \\ & + \bigl(b^{14}+b^6\bigr)c^3 + \bigl(b^{16}+b^8+b^4\bigr)c^2 + b^8\bigr)e^4 + \bigl(c^9 + c^8 + b^{16}c + b^{16}\bigr)e^3 \\ & + \bigl(c^{14} + c^{12} + c^{11} + \bigl(b^4+b^2\bigr)c^{10} + b^2c^9 + \bigl(b^4+1\bigr)c^8 + b^{16}c^6 \\ & + b^{16}c^4 + b^{16}c^3 + \bigl(b^{20}+b^{18}\bigr)c^2 + b^{18}c + \bigl(b^{20}+b^{16}\bigr)\bigr)e^2 \\ & + \bigl(c^{15} + c^{14} + b^4c^{11} + b^4c^{10} + b^{16}c^7 + b^{16}c^6 + b^{20}c^3 + b^{20}c^2\bigr)e \\ & + c^{18} + c^{17} + b^2c^{16} + b^2c^{15} + c^{14} + b^4c^{13} + \bigl(b^6+1\bigr)c^{12} + b^6c^{11} \\ & + \bigl(b^{16}+b^8+b^4\bigr)c^{10} + b^{16}c^9 + \bigl(b^{18}+b^8\bigr)c^8 + b^{18}c^7 + b^{16}c^6 + b^{20}c^5 \\ & + \bigl(b^{22}+b^{16}\bigr)c^4 + b^{22}c^3 + \bigl(b^{24}+b^{20}\bigr)c^2 + b^{24}. \end{aligned}$$

We first consider the case $E_4 = 0$. Let $e = b^2 + c^2 + w$. Substituting e in E_4 by $b^2 + c^2 + w$ to get

$$w^2 + (c+1)w + b^2(c+1)^2 = 0.$$

Dividing both sides by $(c+1)^2$, we get $(w/(c+1))^2 + w/(c+1) + b^2 = 0$, which by Lemma 3.5 implies that $\mathrm{Tr}(b) = 0$. Thus by the comments immediately before the statement of Theorem 2.4, there exists a linear substitution to eliminate b. Hence we may assume that $f(x) = x^6 + x^5 + cx^3 + dx^2 + ex$ (i.e., $b = 0$). It follows that

$$E_4 = \bigl(e + c^2\bigr)\bigl(e + c^2 + c + 1\bigr).$$

Now $E_4 = 0$ leads to the following two cases.

Case 1. $e + c^2 = 0$. Then $E_1 = 0$ becomes $cd^2 = 0$, or $d = 0$, since $c \neq 0$. Then

$$f(x) = x^6 + x^5 + cx^3 + c^2x = x\bigl(x^5 + x^4 + cx^2 + c^2\bigr).$$

In the degree 5 factor of $f(x)$, substituting x by $y + 1$, we obtain $y^5 + cy^2 + y + c^2 + c$, which has exactly one root in $\mathbb{F}_{2^t}$ by Lemma 3.6. Therefore, $f(x)$ has two roots in $\mathbb{F}_{2^t}$, contradicting the assumption that f is a **PP**.

Case 2. $e + c^2 + c + 1 = 0$. Then $E_1 = 0$ becomes $d = c + 1$. Thus $f(x)$ must have the form

$$f(x) = x^6 + x^5 + cx^3 + (c+1)x^2 + \bigl(c^2 + c + 1\bigr)x.$$

Let us consider the following polynomial $g(x)$ that is equivalent to $f(x)$. Set

$$g(x) = x^6 + x^5 + cx^3 + (1+c)x^2 + \bigl(c^2 + c + 1\bigr)x + c^2 + c.$$

Then $g(x) = (x+1)(x^5 + cx^2 + x + c^2 + c)$. The second factor has exactly one root in $\mathbb{F}_{2^t}$ by Lemma 3.6. Thus $g(x)$ has two roots in $\mathbb{F}_{2^t}$. Hence $g(x)$ cannot be a **PP**. But $g(x)$ is equivalent to $f(x)$ and $f(x)$ is assumed to be a **PP**; we have reached a contradiction.

Therefore we conclude that $E_4 \neq 0$. We must have $E_6 = E_7 = 0$. Viewing E_7 and E_6 as polynomials in e, by long division, the remainder of E_7 upon division by E_6 is

$$\begin{aligned} E_{10} := {} & c^{16}b^8 + c^{16}e^4 + c^{18}e + c^{19}e + c^{20}b^4 + c^{20}b^2 + c^{17}e + c^8b^4 \\ & + b^2c^9 + c^{10}b^2 + c^8b^8 + ec^{11} + c^9e + b^2c^{18} + c^{10}e + c^{19}b^2 + c^{16}e \\ & + b^2c^{12} + c^{12}b^4 + c^8e + c^{17}b^2 + c^8e^4 + c^{11}b^2 + c^{16}b^4 \\ & + c^{10} + c^8 + c^{12} + c^{11} + c^{18} + c^{16} + c^{13} + c^{21} + c^{19} + c^{20}. \end{aligned}$$

Again, E_{10} can be factored into

$$E_{10} = c^8(c+1)^8 \cdot E_9,$$

where

$$\begin{aligned} E_9 = {} & e^4 + \bigl(c^3 + c^2 + c + 1\bigr)e + c^5 + \bigl(b^4 + b^2 + 1\bigr)c^4 \\ & + \bigl(b^2 + 1\bigr)c^3 + \bigl(b^2 + 1\bigr)c^2 + b^2c + b^8 + b^4 + 1. \end{aligned}$$

Since $c \neq 0$ or 1, we must have $E_9 = 0$, using which E_6 can be reduced to $c^6 + c^4 + c^2 + 1 = (c+1)^6$. Since $c \neq 1$ we see that $E_6 \neq 0$, a contradiction. The proof is complete. □

4. Permutation polynomials of degree 7 over finite fields of characteristic 2

In this section we determine all permutation polynomials of degree 7 over finite fields of characteristic 2. The first lemma addresses the trivial case, in which $2^t \equiv 1 \pmod 7$.

Lemma 4.1. *Let $t > 0$ be such that $2^t \equiv 1 \pmod 7$. Then there are no permutation polynomials over $\mathbb{F}_{2^t}$ of degree 7.*

Proof. Let $f(x)$ be a monic polynomial over $\mathbb{F}_{2^t}$ of degree 7. Note that when $2^t = 7m + 1$ we have $[x^{7m}]f(x)^m = 1 \neq 0$. Hence by the Hermite–Dickson criterion, $f(x)$ cannot be a permutation polynomial. □

Lemma 4.2. *Let $t > 7$ be such that $2^t \equiv 2 \pmod 7$. Then every permutation polynomial for $\mathbb{F}_{2^t}$ of degree 7 is equivalent to either $x^7 + x^5 + x$ or x^7.*

Please cite this article in press as: J. Li et al., Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, Finite Fields Appl. (2010), doi:10.1016/j.ffa.2010.07.001

Proof. We proceed as in Section 3. We set $q = 7m + 2$, with

$$m = 2^1 + 2^4 + \cdots + 2^{t-3}.$$

Suppose that $f(x)$ is a monic degree 7 **PP** over $\mathbb{F}_q$. By Lemma 2.2, we may normalize $f(x)$ such that

$$f(x) = x^7 + bx^5 + cx^4 + dx^3 + ex^2 + fx \in \mathbb{F}_q[x].$$

Then we have the following conditions:

$$\left[x^{7m+1}\right] f(x)^{m+1} = c^2 + b^3 + f = 0; \tag{4.1}$$

$$\left[x^{7m+1}\right] f(x)^{m+3} = e^4 + d^5 = 0; \tag{4.2}$$

$$\begin{aligned}\left[x^{7m+1}\right] f(x)^{m+11} = {} & \left(c^{24} + b^{16}e^8\right)d + \left(d^{16} + c^{16}b^8 + b^{16}d^8\right)\left(c^4 + b^4 d\right) \\ & + b^{16}c^8\left(e^4 + d^5\right) + \left(c^{16} + b^{24} + f^8\right) f^4 d;\end{aligned} \tag{4.3}$$

$$\begin{aligned}\left[x^{7m+1}\right] f(x)^{m+13} = {} & \left(d^{16}c^8 + c^{16}e^8\right)b + \left(e^{16} + d^{16}b^8 + c^{16}d^8 + b^{16}f^8\right) \\ & \cdot \left(b^5 + e^2 + d^2 b + c^2 d + b^2 f\right) + \left(c^{24} + b^{16}e^8\right) \\ & \cdot \left(d^4 b + c^4\left(c^2 + b^3 + f\right) + b^4\left(e^2 + d^2 b + c^2 d + b^2 f\right) + f^3\right) \\ & + \left(d^{16} + c^{16}b^8 + b^{16}d^8\right)\left(f^4 b + e^4\left(c^2 + b^3 + f\right) + d^4\left(e^2 + d^2 b + c^2 d + b^2 f\right)\right. \\ & \left. + c^4\left(f^2 b + e^2 d + d^2 f\right) + b^2 f^3\right) + b^{16}c^8\left(f^4\left(e^2 + d^2 b + c^2 d + b^2 f\right)\right. \\ & \left. + e^4\left(f^2 b + e^2 d + d^2 f\right) + d^4 f^3\right) + \left(c^{16} + b^{24} + f^8\right) f^7;\end{aligned} \tag{4.4}$$

$$\left[x^{7m+1}\right] f(x)^{m+19} = d^{33} = 0. \tag{4.5}$$

Combining (4.2) and (4.5), we have $d = e = 0$. By the comments immediately before the statement of Theorem 2.4 in Section 2, we may assume that $b \in \{0, 1\}$. First we assume that $b = 1$. Then (4.3) reduces to $c^{20} = 0$ and (4.1) gives us $f = 1$. The **PP** is

$$x^7 + x^5 + x.$$

(Note that the above polynomial is indeed a **PP** by Theorem 7.16 [4, p. 356].) Next we assume that $b = 0$. Then (4.4) reduces to $c^{24} f^3 = 0$ (using (4.1) to eliminate the last term and one other term), which combined with (4.1) gives us $c = f = 0$. The **PP** is x^7. The proof is complete. □

Lemma 4.3. *Let $t > 5$ be such that $2^t \equiv 4 \pmod 7$. Then every permutation polynomial over $\mathbb{F}_{2^t}$ of degree 7 is equivalent either $x^7 + x^5 + x$ or x^7.*

Proof. We set $q = 7m + 4$ with

$$m = 2^2 + 2^5 + \cdots + 2^{t-3}.$$

Suppose that $f(x)$ is a monic degree 7 **PP** over $\mathbb{F}_q$. By Lemma 2.2, we may normalize $f(x)$ such that

$$f(x) = x^7 + bx^5 + cx^4 + dx^3 + ex^2 + fx \in \mathbb{F}_q[x].$$

This time we use the following relations:

$$[x^{7m+3}]f(x)^{m+1} = d = 0; \tag{4.6}$$

$$[x^{7m+3}]f(x)^{m+3} = d^4b + c^4(c^2 + b^3 + f) + b^4(e^2 + d^2b + c^2d + b^2f) + f^3 = 0; \tag{4.7}$$

$$[x^{7m+3}]f(x)^{m+9} = f^8c^4 + e^{12} + (f^8b^4 + e^8d^4 + d^8f^4)d = 0; \tag{4.8}$$

$$[x^{7m+3}]f(x)^{m+15} = (c^{32} + b^{48} + f^{16})(c^2 + b^3 + f) = 0; \tag{4.9}$$

$$\begin{aligned}[x^{7m+3}]f(x)^{m+19} = {} & (d^{32} + c^{32}b^{16} + b^{32}d^{16})b + b^{32}c^{16}(d^4b + c^4(c^2 + b^3 + f) \\ & + b^4(e^2 + d^2b + c^2d + b^2f) + f^3) + (c^{32} + b^{48} + f^{16}) \\ & \cdot (f^4(e^2 + d^2b + c^2d + b^2f) + e^4(f^2b + e^2d + d^2f) + d^4f^3) = 0.\end{aligned} \tag{4.10}$$

From (4.6) and (4.9) we get $d = 0$ and $f = c^2 + b^3$. By the comments immediately before the statement of Theorem 2.4 in Section 2, we may assume that $b \in \{0, 1\}$. First assume that $b = 1$. Substituting into (4.7) and (4.10) we get $e^2 + f + f^3 = 0$ and $c^{32} + e^2 + f + f^3 = 0$, or $c = 0$. We have $f = 1$, and (4.8) reduces to $e^{12} = 0$. The **PP** is $x^7 + x^5 + x$. Now assume $b = 0$. Then (4.7) reduces to $f^3 = 0$, and we have $b = c = d = f = 0$. Substituting into (4.8) gives e^{12} and the **PP** is x^7. The proof is now complete. □

Combining the lemmas and computer results for $\mathbb{F}_{16}$, $\mathbb{F}_{32}$, and $\mathbb{F}_{128}$, we have:

Theorem 4.4. *Let $2^t \geqslant 8$. If $t \equiv 0 \pmod 3$, then there are no permutation polynomials over $\mathbb{F}_{2^t}$ of degree 7. Otherwise, every permutation polynomial over $\mathbb{F}_{2^t}$ of degree 7 is equivalent to $x^7 + x^5 + x$, or to x^7, or $t = 4$, and the polynomial is equivalent to one of the following*

$$\begin{gathered} x^7 + a^3x^4 + a^6x, \\ x^7 + x^5 + x^4, \\ x^7 + x^5 + ax^4 + a^{14}x^3 + a^{12}x^2 + a^8x, \\ x^7 + x^5 + a^5x^4 + a^2x^3 + a^{12}x^2 + a^5x, \\ x^7 + x^5 + a^7x^4 + a^5x^2 + a^3x, \end{gathered}$$

where a is a root of $x^4 + x + 1 \in \mathbb{F}_2[x]$ in some extension field of $\mathbb{F}_2$.

Remark 4.5. The methods that we used for classifying **PP**s of $\mathbb{F}_{2^t}$ of degree 6 or 7 will not work when the degree of the **PP** is a power of the characteristic. In other cases, for fixed degree and fixed characteristic, the methods can be expected to work, although the number of terms to deal with is likely to increase rapidly with the characteristic.

References

[1] S.D. Cohen, M.D. Fried, Lenstra's proof of the Carlitz–Wan conjecture on exceptional polynomials: an elementary version, Finite Fields Appl. 1 (1995) 372–375.

[2] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, part I, Ann. of Math. 11 (1896–1897) 65–120.

[3] M.D. Fried, R. Guralnick, J. Saxl, Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993) 157–225.

[4] R. Lidl, H. Niederreiter, Finite Fields, second ed., Cambridge University Press, Cambridge, 1997.

[5] 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.

[6] 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.

[7] G.L. Mullen, Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results, Finite Fields Appl. 1 (1995) 242–258.

[8] G.L. Mullen, Permutation polynomials over finite fields, in: Finite Fields, Coding Theory and Advances in Communications and Computing, Las Vegas, NV, 1991, in: Lect. Notes Pure Appl. Math., vol. 141, Dekker, New York, 1993, pp. 131–151.

[9] D. Wan, A generalization of the Carlitz conjecture, in: Finite Fields, Coding Theory and Advances in Communications and Computing, in: Lect. Notes Pure Appl. Math., vol. 141, Dekker, 1993, pp. 431–432.

Please cite this article in press as: J. Li et al., Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, Finite Fields Appl. (2010), doi:10.1016/j.ffa.2010.07.001