Bull. Aust. Math. Soc. **101** (2020), 56–60
doi:10.1017/S0004972719000728

A NEW PROOF OF THE CARLITZ–LUTZ THEOREM

RACHID BOUMAHDI, OMAR KIHEL, JESSE LARONE✉ and MAKHLOUF YADJEL

(Received 6 April 2019; accepted 9 May 2019; first published online 10 July 2019)

Abstract

A polynomial f over a finite field $\mathbb{F}_q$ can be classified as a permutation polynomial by the Hermite–Dickson criterion, which consists of conditions on the powers f^e for each e from 1 to $q-2$, as well as the existence of a unique solution to $f(x) = 0$ in $\mathbb{F}_q$. Carlitz and Lutz gave a variant of the criterion. In this paper, we provide an alternate proof to the theorem of Carlitz and Lutz.

2010 *Mathematics subject classification*: primary 11T06; secondary 12E20.

Keywords and phrases: permutation polynomial, Hermite–Dickson theorem.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a permutation polynomial if the induced map from $\mathbb{F}_q$ to $\mathbb{F}_q$ is bijective. Permutation polynomials form an active area of research with many open problems and conjectures (see [4]).

Denote the image of $f(x)$ modulo $x^q - x$ by $\overline{f(x)}$. The best-known criterion for classifying permutation polynomials is given by the Hermite–Dickson theorem [3].

Theorem 1.1. *Let $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is a permutation polynomial if and only if:*

(i) $\deg \overline{f(x)^\ell} \le q-2$ *for* $1 \le \ell \le q-2$;
(ii) $f(x)$ *has a unique root in* $\mathbb{F}_q$.

Ayad *et al.* [1] improved this criterion for binomials. Carlitz and Lutz [2] gave a variant of the Hermite–Dickson theorem, providing sufficient conditions for a polynomial to be a permutation polynomial.

Theorem 1.2. *Let $f(x) \in \mathbb{F}_q[x]$. Suppose that:*

(i) $\deg \overline{f(x)^\ell} \le q-2$ *for* $1 \le \ell \le q-2$;
(ii) $\deg \overline{f(x)^{q-1}} = q-1$.

The second and third authors were supported by NSERC.

Then $f(x)$ is a permutation polynomial.

In this paper, we refine Theorem 1.2 by proving the following result.

THEOREM 1.3. *Let $f(x) \in \mathbb{F}_q[x]$. Then the following conditions are equivalent.*

(i) $\deg \overline{f(x)^\ell} \le q-2$ *for* $1 \le \ell \le q-2$, *and* $\deg \overline{f(x)^{q-1}} = q-1$.

(ii) $\deg \overline{f(x)^\ell} \le q-2$ *for each* ℓ *with* $1 \le \ell \le q-2$ *and relatively prime to* $\mathrm{char}(\mathbb{F}_q)$, *and* $\deg \overline{f(x)^{q-1}} = q-1$.

(iii) *$f(x)$ is a permutation polynomial.*

2. Preliminary results

Let $x_1, \ldots, x_n$ be n variables. For each $k \in \{1, \ldots, n\}$, let

$$s_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} \cdots x_{i_k}$$

be the elementary symmetric polynomial of degree k in n variables, and let

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k$$

be the power sum symmetric polynomial of degree k in n variables, with the conventional definition $\sigma_0(x_1, \ldots, x_n) = n$. The polynomials s_k and σ_k satisfy the relation

$$\sigma_k - s_1\sigma_{k-1} + \cdots + (-1)^k k s_k = 0 \quad \text{for } 1 \le k \le n, \tag{2.1}$$

the validity of which is demonstrated in [6].

A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if $f(\mathbb{F}_q) = \mathbb{F}_q$, which is equivalent to

$$\prod_{c \in \mathbb{F}_q} (x - f(c)) = \prod_{c \in \mathbb{F}_q} (x - c) = x^q - x. \tag{2.2}$$

Let $c_1, \ldots, c_q$ be the distinct elements of $\mathbb{F}_q$. By expanding the left-hand side of equation (2.2) and identifying its coefficients with those of $x^q - x$, we deduce that $f(x)$ is a permutation polynomial if and only if

$$s_k(f(c_1), \ldots, f(c_q)) = 0$$

for each $k \in \{1, \ldots, q-2\}$ and

$$s_{q-1}(f(c_1), \ldots, f(c_q)) = -1.$$

Consider any map $\tau : \mathbb{F}_q \to \mathbb{F}_q$. There exists a unique polynomial $g(x) \in \mathbb{F}_q[x]$ of degree less than q such that $g(c) = \tau(c)$ for all $c \in \mathbb{F}_q$. The well-known formula

$$g(x) = \sum_{c \in \mathbb{F}_q} (1 - (x-c)^{q-1}) \tau(c)$$

provides an expression for $g(x)$ [5]. This expression implies that $\deg g \leq q-2$ if and only if

$$\sum_{c\in\mathbb{F}_q} \tau(c) = \sum_{c\in\mathbb{F}_q} g(c) = 0.$$

3. Proof of the theorem

Proof of Theorem 1.3. The implication (i) ⇒ (ii) is clear.

Next consider the implication (ii) ⇒ (iii). Let $p = \mathrm{char}(\mathbb{F}_q)$ and suppose that $\deg \overline{f(x)^\ell} \leq q-2$ for each $\ell \in \{1,\dots,q-2\}$ such that $\gcd(p,\ell)=1$ and in addition that $\deg \overline{f(x)^{q-1}} = q-1$. Set $a := \sigma_{q-1}(f(c_1),\dots,f(c_q))$. Then $a \neq 0$ and

$$\sigma_\ell(f(c_1),\dots,f(c_q)) = 0 \tag{3.1}$$

for each $\ell \in \{1,\dots,q-2\}$ not divisible by p. We show that

$$s_\ell(f(c_1),\dots,f(c_q)) = \sigma_\ell(f(c_1),\dots,f(c_q)) \tag{3.2}$$

for all $\ell \in \{1,\dots,q-1\}$ not divisible by p.

The statement is clear for $\ell = 1$, so let $e \in \{2,\dots,q-1\}$ be such that p does not divide e and assume that equation (3.2) holds for all $\ell \in \{1,\dots,e-1\}$ such that p does not divide ℓ. We write (2.1) in the form

$$\sigma_e(f(c_1),\dots,f(c_q)) + \sum(-1)^u s_u(f(c_1),\dots,f(c_q))\sigma_v(f(c_1),\dots,f(c_q)) \\ + (-1)^e e s_e(f(c_q),\dots,f(c_q)) = 0, \tag{3.3}$$

where the sum runs over all pairs (u,v) such that $u+v=e$ and $u,v \in \{1,\dots,e-1\}$. Letting (u,v) be any such pair, if p does not divide u, then $s_u(f(c_1),\dots,f(c_q)) = 0$ by hypothesis. If p does divide u, then p does not divide v and so $\sigma_v(f(c_1),\dots,f(c_q)) = 0$. Equation (3.3) is then reduced to

$$\sigma_e(f(c_1),\dots,f(c_q)) = (-1)^{e+1} e s_e(f(c_1),\dots,f(c_q)),$$

and (3.1) implies that

$$s_e(f(c_1),\dots,f(c_q)) = \sigma_e(f(c_q),\dots,f(c_q)) = 0$$

for each $e \in \{2,\dots,q-2\}$ not divisible by p, and

$$s_{q-1}(f(c_1),\dots,f(c_q)) = \sigma_{q-1}(f(c_1),\dots,f(c_q)) = a.$$

Let

$$h(x) = \prod_{c\in\mathbb{F}_q}(x - f(c)).$$

Expanding $h(x)$ yields an expression of the form

$$h(x) = x^q + ax + \sum_{p\mid i} a_i x^i,$$

https://doi.org/10.1017/S0004972719000728 Published online by Cambridge University Press

from which it is apparent that $h'(x) = a \neq 0$. Thus, $h(x)$ is separable, implying that $f(x)$ is a permutation polynomial.

To prove the implication (iii) ⇒ (i), we suppose that $f(x)$ is a permutation polynomial. Then

$$s_\ell(f(c_1), \ldots, f(c_q)) = 0$$

for $\ell \in \{1, \ldots, q-2\}$ and $s_{q-1}(f(c_1), \ldots, f(c_q)) = -1$. Equation (2.1) immediately implies that

$$\sigma_\ell(f(c_1), \ldots, f(c_q)) = 0$$

for $\ell \in \{1, \ldots, q-2\}$ and $\sigma_{q-1}(f(c_1), \ldots, f(c_q)) = -1$. It follows that

$$\sum_{c \in \mathbb{F}_q} f(c)^\ell = 0$$

for $\ell \in \{1, \ldots, q-2\}$ and

$$\sum_{c \in \mathbb{F}_q} f(c)^{q-1} = -1.$$

Therefore, $\deg \overline{f(x)^\ell} \leq q-2$ for $\ell \in \{1, \ldots, q-2\}$ and $\deg \overline{f(x)^{q-1}} = q-1$. □

We next state and prove an immediate consequence of Theorem 1.3.

Corollary 3.1. *Let $f(x) \in \mathbb{F}_q[x]$. Then the following statements are equivalent.*

(i) *$f(x)$ is a permutation polynomial.*
(ii) *For any polynomial $u(x) \in \mathbb{F}_q[x]$, $\deg \overline{u(x)} = q-1$ if and only if $\deg \overline{u(f(x))} = q-1$.*

Proof. Suppose that $f(x)$ is a permutation polynomial and let $u(x) \in \mathbb{F}_q[x]$ be such that $\deg \overline{u(x)} = q-1$. By Theorem 1.3, we then have $\deg \overline{u(f(x))} = q-1$.

Conversely, let $u_i(x) = x^i$ for each $i \in \{1, \ldots, q-1\}$. Then $\overline{u_i(f(x))} = \overline{f(x)^i}$. By Theorem 1.3, $\deg \overline{u_i(f(x))} = q-1$ if and only if $i = q-1$. Therefore, $f(x)$ is a permutation polynomial. □

4. Concluding remarks

The theorems presented can be interpreted as properties of the composition on the left of $f(x)$ with each of the basis elements $\{x^i \mid i = 0, \ldots, q-1\}$ of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[x]/(x^q - x)$. Changing this basis to another will allow one to prove similar results.

Remark 4.1. Let $f(x)$ be a permutation polynomial over $\mathbb{F}_q$, and consider the map $\varphi : \{1, \ldots, q-1\} \to \{1, \ldots, q-1\}$ given by $\varphi(e) = \deg \overline{f(x)^e}$. Theorem 1.3 shows that $\varphi^{-1}(q-1) = \{q-1\}$.

In the particular case $f(x) = x^n$, where n is an integer relatively prime to $q-1$, $f(x)$ is a permutation polynomial [5], and it is straightforward to show that the corresponding map φ is injective. However, this is not always the case. For example, suppose that $q = p^r$ for an odd prime p and let $f(x) = ax^{q-2} + b$ with $a, b \in \mathbb{F}_q^*$. One can verify that $\varphi(1) = \varphi(2) = \varphi(3) = q-2$.

https://doi.org/10.1017/S0004972719000728 Published online by Cambridge University Press

REMARK 4.2. If $d > 1$ is a divisor of $q - 1$, then there is no permutation polynomial over $\mathbb{F}_q$ of degree d [5]. This introduces the following problem: for each $k \in \{1, \ldots, q-2\}$, let a_k be an element of $\{1, \ldots, q-2\}$ such that a_k does not divide $q-1$ whenever $\gcd(k, q-1) = 1$. Does there exist a permutation polynomial $f(x) \in \mathbb{F}_q[x]$ such that the corresponding map φ satisfies $\varphi(k) = a_k$ for each $k \in \{1, \ldots, q-2\}$ and $\varphi(q-1) = q-1$?

References

[1] M. Ayad, K. Belghaba and O. Kihel, 'On permutation binomials over finite fields', *Bull. Aust. Math. Soc.* **89**(1) (2014), 112–124.

[2] L. Carlitz and J. A. Lutz, 'A characterization of permutation polynomials over a finite field', *Amer. Math. Monthly* **85** (1978), 746–748.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* (Dover, New York, 1958).

[4] R. Lidl and G. L. Mullen, 'Does a polynomial permute the elements of the field?', *Amer. Math. Monthly* **95** (1988), 243–246.

[5] R. Lidl and H. Niedereiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, 2008).

[6] I. G. Macdonald, *Symmetric Functions and Hall Polynomials* (Clarendon Press, Oxford, 1998).

RACHID BOUMAHDI, La3c Laboratory,
Faculty of Mathematics, USTHB University, Algiers, Algeria
e-mail: r_boumehdi@esi.dz

OMAR KIHEL, Department of Mathematics,
Brock University, Ontario, Canada L2S 3A1
e-mail: okihel@brocku.ca

JESSE LARONE, Département de mathématiques et de statistique,
Université Laval, Québec, Canada G1V 0A6
e-mail: jesse.larone.1@ulaval.ca

MAKHLOUF YADJEL, La3c Laboratory,
Faculty of Mathematics, USTHB University, Algiers, Algeria
e-mail: yadmakhlouf@hotmail.fr