Finite Fields and Their Applications 41 (2016) 132–158

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On monomial complete permutation polynomials ☆

Daniele Bartoli [a], Massimo Giulietti [a,*], Giovanni Zini [b]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1, 06123 Perugia, Italy*
[b] *Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67/A, 50134 Firenze, Italy*

A R T I C L E I N F O

Article history:
Received 11 February 2016
Received in revised form 26 April 2016
Accepted 13 June 2016
Communicated by Xiang-dong Hou

MSC:
11T06

Keywords:
Permutation polynomials
Complete permutation polynomials
Bent–negabent boolean functions

A B S T R A C T

We investigate monomials ax^d over the finite field with q elements $\mathbb{F}_q$, in the case where the degree d is equal to $\frac{q-1}{q'-1}+1$ with $q=(q')^n$ for some n. For $n=6$ we explicitly list all a's for which ax^d is a complete permutation polynomial (CPP) over $\mathbb{F}_q$. Some previous characterization results by Wu et al. for $n=4$ are also made more explicit by providing a complete list of a's such that ax^d is a CPP. For odd n, we show that if q is large enough with respect to n then ax^d cannot be a CPP over $\mathbb{F}_q$, unless q is even, $n \equiv 3 \pmod 4$, and the trace $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(a^{-1})$ is equal to 0.

☆ The research of D. Bartoli, M. Giulietti, and G. Zini was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza" – Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA – INdAM).

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), massimo.giulietti@unipg.it (M. Giulietti), gzini@math.unifi.it (G. Zini).

http://dx.doi.org/10.1016/j.ffa.2016.06.005
1071-5797/

1. Introduction

Let $\mathbb{F}_\ell$, $\ell = p^h$, p prime, denote the finite field of order ℓ. A *permutation polynomial* (or PP) $f(x) \in \mathbb{F}_\ell[x]$ is a bijection of $\mathbb{F}_\ell$ onto itself. A polynomial $f(x) \in \mathbb{F}_\ell[x]$ is a *complete permutation polynomial* (or CPP), if both $f(x)$ and $f(x)+x$ are permutation polynomials of $\mathbb{F}_\ell$. Both permutation polynomials and complete permutation polynomials have been extensively studied also because of their applications to cryptography and combinatorics; see for instance [6,9,11,12,16,18] and the references therein. In particular, CPPs over fields of characteristic 2 give rise to bent–negabent boolean functions, which are a useful tool in cryptography; see [14].

Some families of CPPs are obtained in [6,9,11,13,17,18]. Nevertheless, CPPs seem to be very rare objects, even if we restrict to the monomial case. It is easily seen that a monomial ax^d is a CPP if and only if $(d, \ell-1) = 1$ and $x^d + \frac{x}{a}$ is a PP. This motivates the investigation of permutation binomials of type $x^d + bx$ for $d = (\ell-1)/m + 1$ with m a divisor of $\ell - 1$.

In [3–5,18,19] PPs of type $f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx$ over $\mathbb{F}_{q^n}$ are thoroughly investigated for $n = 2$, $n = 3$, and $n = 4$. For $n = 6$, sufficient conditions for f_b to be a PP of $\mathbb{F}_{q^6}$ are provided in [18,19] in the special cases of characteristic $p \in \{2, 3, 5\}$. The case $p = n + 1$ is dealt with in [10].

In this paper, we provide a complete classification of permutation polynomials f_b in the case $n = 6$, for arbitrary q. Theorems 1.1 and 1.2 list explicitly for $q \geq 421$ all elements $b \in \mathbb{F}_{q^6} \setminus \mathbb{F}_q$ such that f_b is a PP. For smaller values of q, Theorems 1.1 and 1.2 provide families of PPs of type f_b. We also determine the number of PPs of type f_b for $q \geq 421$; see Corollary 4.3. It should be noted that for $p = 7$, the sufficient condition in [10] for f_b to be a PP is that $b^{q-1} = -1$; our results show that this is not a necessary condition.

Our methods also work for $n = 4$. This allows us to list PPs of type f_b for $n = 4$; see Remark 4.4. In this way, a more explicit description of the necessary and sufficient conditions of [19, Theorem 4.1] is given.

In the paper the case n odd is dealt with as well. Note that for n odd f_b being a PP implies that $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP only for $p = 2$. We show that if p does not divide $(n+1)/2$ or $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q'}}(b) \neq 0$, then for q large enough with respect to n the polynomial f_b is never a PP; see Theorem 5.2. This shows that for n odd the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is never a CPP unless $n \equiv 3 \pmod 4$. For $n = 3$ Theorem 5.2 provides a shorter proof of the results of [5, Section 3].

A key tool in our investigation is the following criterion from [13], which relates the existence of a suitable $\mathbb{F}_q$-rational point of some algebraic curve to f_b being a PP of $\mathbb{F}_{q^n}$ or not.

Niederreiter–Robinson Criterion. *The polynomial*

$$f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx \tag{1}$$