Finite Fields and Their Applications 49 (2018) 132–142

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# On the difference between permutation polynomials

Nurdagül Anbar [a,*], Almasa Odžak [b], Vandita Patel [c], Luciane Quoos [d], Anna Somoza [e,f], Alev Topuzoğlu [g]

[a] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040 Linz, Austria*
[b] *University of Sarajevo, Zmaja od Bosne 35, 71000 Sarajevo, Bosnia and Herzegovina*
[c] *University of Warwick, Coventry CV4 7AL, UK*
[d] *Universidade Federal do Rio de Janeiro, Cidade Universitária, Rio de Janeiro, RJ 21941-909, Brazil*
[e] *Universitat Politècnica de Catalunya, Calle Jordi Girona, 1-3, 08034 Barcelona, Spain*
[f] *Leiden University, Snellius building, Niels Bohrweg 1, 2300 RA Leiden, Netherlands*
[g] *Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey*

A R T I C L E   I N F O

*Article history:*
Received 22 June 2017
Received in revised form 20 September 2017
Accepted 21 September 2017
Available online xxxx
Communicated by Stephen D. Cohen

*MSC:*
11T06
14H05

*Keywords:*
Carlitz rank
Chowla–Zassenhaus conjecture
Curves over finite fields
Permutation polynomials

A B S T R A C T

The well-known Chowla and Zassenhaus conjecture, proved by Cohen in 1990, states that if $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial $f$ in $\mathbb{F}_p[x]$ of degree $d \geq 2$. For arbitrary finite fields $\mathbb{F}_q$, a similar non-existence result was obtained recently by Işık, Topuzoğlu and Winterhof in terms of the Carlitz rank of $f$.
Cohen, Mullen and Shiue generalized the Chowla–Zassenhaus–Cohen Theorem significantly in 1995, by considering differences of permutation polynomials. More precisely, they showed that if $f$ and $f + g$ are both permutation polynomials of degree $d \geq 2$ over $\mathbb{F}_p$, with $p > (d^2 - 3d + 4)^2$, then the degree $k$ of $g$ satisfies $k \geq 3d/5$, unless $g$ is constant. In this article, assuming $f$ and $f + g$ are permutation polynomials in $\mathbb{F}_q[x]$, we give lower bounds for the Carlitz rank of $f$ in terms of $q$ and $k$. Our results generalize the above mentioned result of Işık et al. We also show for a special class of per-

* Corresponding author.
*E-mail addresses:* nurdagulanbar2@gmail.com (N. Anbar), almasa.odzak@gmail.com (A. Odžak), vandita.patel@warwick.ac.uk (V. Patel), luciane@im.ufrj.br (L. Quoos), anna.somoza@upc.edu (A. Somoza), alev@sabanciuniv.edu (A. Topuzoğlu).

https://doi.org/10.1016/j.ffa.2017.09.009
1071-5797/© 2017 Elsevier Inc. All rights reserved.

mutation polynomials $f$ of Carlitz rank $n \geq 1$ that if $f + x^k$ is a permutation over $\mathbb{F}_q$, with $\gcd(k + 1, q - 1) = 1$, then $k \geq (q - n)/(n + 3)$.
© 2017 Elsevier Inc. All rights reserved.

## 1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where $r \geq 1$ and $p$ is a prime. Throughout we assume $q \geq 3$. We recall that $f \in \mathbb{F}_q[x]$ is a *permutation polynomial* over $\mathbb{F}_q$ if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$. If $f(x)$ and $f(x) + x$ are both permutation polynomials over $\mathbb{F}_q$, then $f$ is called a *complete mapping*. We refer the reader to [11] for a detailed study of complete mapping polynomials over finite fields. Their use in the construction of mutually orthogonal Latin squares is described, for instance, in [9]. For various other applications, see [10,12–14]. Recent work on generalizations of complete mappings can be found in [17].

Theorem 1 below was conjectured by Chowla and Zassenhaus [3] in 1968, and proved by Cohen [4] in 1990.

**Theorem 1.** *([4, Theorem 1]) If $d \geq 2$ and $p > (d^2 - 3d + 4)^2$, then there is no complete mapping polynomial of degree $d$ over $\mathbb{F}_p$.*

A significant generalization of this result was obtained by Cohen, Mullen and Shiue [5] in 1995, and gives a lower bound for the degree of the difference of two permutation polynomials in $\mathbb{F}_p[x]$ of the same degree $d$, when $p > (d^2 - 3d + 4)^2$.

**Theorem 2.** *([5, Theorem 2]) Suppose $f$ and $f + g$ are monic permutation polynomials over $\mathbb{F}_p$ of degree $d \geq 3$, where $p > (d^2 - 3d + 4)^2$. Then either $\deg(g) = 0$ or $\deg(g) \geq 3d/5$.*

An alternative invariant, the so-called Carlitz rank, attached to permutation polynomials, was recently used by Işık, Topuzoğlu and Winterhof [8] to obtain a non-existence result, similar to that in Theorem 1. The concept of Carlitz rank was first introduced in [1]. We describe it here briefly. The interested reader may see [16] for details.

By a well-known result of Carlitz [2] that any permutation polynomial over $\mathbb{F}_q$, $q \geq 3$, is a composition of linear polynomials $ax+b$, $a, b \in \mathbb{F}_q$, $a \neq 0$, and $x^{q-2}$, any permutation $f$ over $\mathbb{F}_q$ can be represented by a polynomial of the form

$$P_n(x) = \left(\dots\left((a_0x + a_1)^{q-2} + a_2\right)^{q-2} \dots + a_n\right)^{q-2} + a_{n+1}, \tag{1.1}$$

for some $n \geq 0$, where $a_i \neq 0$, for $i = 0, 2, \dots, n$. Note that $f(c) = P_n(c)$ holds for all $c \in \mathbb{F}_q$, however this representation is not unique, and $n$ is not necessarily minimal.

Download English Version:

https://daneshyari.com/en/article/5771540

Download Persian Version:

https://daneshyari.com/article/5771540

Daneshyari.com