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

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Carlitz–Wan conjecture for permutation polynomials and Weill bound for curves over finite fields ☆,☆☆

Jasbir S. Chahal [a], Sudhir R. Ghorpade [b,*]

[a] *Department of Mathematics, Brigham Young University, Provo, UT 84602, USA*
[b] *Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*

ARTICLE INFO

Article history:
Received 27 September 2013
Received in revised form 1 June 2018
Accepted 5 June 2018
Available online xxxx
Communicated by Rudolf Lidl

MSC:
11T06
11G20
12E20

Keywords:
Permutation polynomial
Exceptional polynomial
Separable polynomial
Weil bound

ABSTRACT

The Carlitz–Wan conjecture, which is now a theorem, asserts that for any positive integer n, there is a constant C_n such that if q is any prime power $> C_n$ with $\mathrm{GCD}(n, q-1) > 1$, then there is no permutation polynomial of degree n over the finite field with q elements. From the work of von zur Gathen, it is known that one can take $C_n = n^4$. On the other hand, a conjecture of Mullen, which asserts essentially that one can take $C_n = n(n-2)$ has been shown to be false. In this paper, we use a precise version of Weil bound for the number of points of affine algebraic curves over finite fields to obtain a refinement of the result of von zur Gathen where n^4 is replaced by a sharper bound. As a corollary, we show that Mullen's conjecture holds in the affirmative if $n(n-2)$ is replaced by $n^2(n-2)^2$.

☆ This is a republication, with minor changes, of the article published earlier in Vol. 28 (July 2014), pp. 282–291. The original article was wrongly retracted by the journal on July 8, 2015 for which the publisher apologizes to the authors.

☆☆ The second named author was partially supported during the course of this work by the Indo-Russian project INT/RFBR/P-114 from the Department of Science & Technology, Govt. of India and the IRCC Award grant 12IRAWD009 from IIT Bombay.

* Corresponding author.
E-mail addresses: jasbir@math.byu.edu (J.S. Chahal), srg@math.iitb.ac.in (S.R. Ghorpade).

https://doi.org/10.1016/j.ffa.2018.07.006
1071-5797/

Please cite this article in press as: J.S. Chahal, S.R. Ghorpade, Carlitz–Wan conjecture for permutation polynomials and Weill bound for curves over finite fields, Finite Fields Appl. (2018), https://doi.org/10.1016/j.ffa.2018.07.006

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q[x]$ (resp: $\mathbb{F}_q[x, y]$) the ring of polynomials in one variable x (resp: two variables x and y) with coefficients in $\mathbb{F}_q$. A permutation polynomial over $\mathbb{F}_q$ is an element of $\mathbb{F}_q[x]$ such that the corresponding function from $\mathbb{F}_q$ to $\mathbb{F}_q$ is bijective. For example, if n is a positive integer relatively prime to $q-1$, then x^n is a permutation polynomial over $\mathbb{F}_q$. A closely related notion is that of an exceptional polynomial, which by definition, is a univariate polynomial $f \in \mathbb{F}_q[x]$ such that the corresponding bivariate polynomial

$$f^*(x, y) = \frac{f(x) - f(y)}{x - y} \tag{1}$$

has no absolutely irreducible factor in $\mathbb{F}_q[x, y]$. The following result was proved in special cases by MacCluer [12] and Williams [22], and unconditionally, by Cohen [4, Theorem 5].

Theorem 1.1. *Every exceptional polynomial in $\mathbb{F}_q[x]$ is a permutation polynomial.*

The converse is not true, in general. For example, if p is the characteristic of $\mathbb{F}_q$ and $f(x) = x^p$, then f is a permutation polynomial, but not an exceptional polynomial. On the other hand, if we require f to be a separable polynomial, then as we shall see, f is necessarily an exceptional polynomial provided q is large enough. In fact, a result such as this and indeed much of the development concerning permutation polynomials, was motivated by a conjecture of Carlitz (1966), which states that for any even positive integer n, there is a constant C_n such that if q is any odd prime power with $q > C_n$, then there is no permutation polynomial in $\mathbb{F}_q[x]$ of degree n. This was subsequently generalized by Wan [19] in 1993 to what became known as Carlitz–Wan Conjecture, the statement of which has already been given in the abstract of this article. In the meantime, the use of fundamental inequalities concerning the number of points of algebraic curves over finite fields led to the following converse to Theorem 1.1.

Theorem 1.2. *If $f \in \mathbb{F}_q[x]$ is a separable polynomial of degree n such that f is a permutation polynomial, then f is an exceptional polynomial, provided $q \geq n^4$.*

Initially, this was proved by Hayes [9, Thm. 3.1] in 1969 with an additional hypothesis that $\mathrm{GCD}(q, n) = 1$ and with the explicit constant n^4 replaced by an abstract constant C_n. The latter stems from the use of Lang–Weil inequality. The version stated above was proposed by von zur Gathen [18] in 1991 who directly used Weil's inequality for curves, or rather, an erroneous version of it given in the book of Lidl and Niederreiter [11, p. 331]. Applications of results such as Theorem 1.2 to establish Carlitz's conjecture in a number of special cases are given by several authors beginning with Hayes [9] who considered the cases when $n = 8$ or 10. Eventually, by passing to Galois covers of the projective line over (the algebraic closure of) $\mathbb{F}_q$ and using results from group theory

Please cite this article in press as: J.S. Chahal, S.R. Ghorpade, Carlitz–Wan conjecture for permutation polynomials and Weill bound for curves over finite fields, Finite Fields Appl. (2018), https://doi.org/10.1016/j.ffa.2018.07.006