Finite Fields and Their Applications 54 (2018) 113–132

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Applications of the Hasse–Weil bound to permutation polynomials

Xiang-dong Hou

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, United States of America

ARTICLE INFO

Article history:
Received 26 October 2017
Received in revised form 1 August 2018
Accepted 2 August 2018
Available online xxxx
Communicated by Rudolf Lidl

MSC:
11T06
11T55
14H05

Keywords:
Absolute irreducibility
Finite field
Hasse–Weil bound
Permutation polynomial

ABSTRACT

Riemann's hypothesis on function fields over a finite field implies the Hasse–Weil bound for the number of zeros of an absolutely irreducible bi-variate polynomial over a finite field. The Hasse–Weil bound has extensive applications in the arithmetic of finite fields. In this paper, we use the Hasse–Weil bound to prove two results on permutation polynomials over $\mathbb{F}_q$ where q is sufficiently large. To facilitate these applications, the absolute irreducibility of certain polynomials in $\mathbb{F}_q[X, Y]$ is established.

1. Introduction

Recent years have seen a surge of research activities in permutation polynomials over finite fields. We give a few references [4,7,9,18,19,25,30], noting that it is impossible to include a comprehensive literature review. While interesting results continue to appear

E-mail address: xhou@usf.edu.

https://doi.org/10.1016/j.ffa.2018.08.005
1071-5797/

in the literature, broad challenges are condensed into clearly defined questions, some of which appear in the following form: In a class of polynomials under consideration, known permutation polynomials have been enumerated, and the conjecture is that the enumeration is complete; see for example [2,5,7,12,15]. The Hasse–Weil bound is a powerful tool for proving such conjectures asymptotically, i.e., when the finite field is sufficiently large. Usually, when applying the Hasse–Weil bound, the technical difficulty is the proof of the absolute irreducibility of the involved polynomial; see for example [1], [23, §§V.2–V.4].

Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $g \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$. The main results of the present paper are the following two theorems.

Theorem 1.1. *Assume that* $r > 2$, $q \geq 2^8(r-1)^4$, $a \in \mathbb{F}_{q^2}^*$, *and* $a^{q+1} \neq 1$. *Then* $\mathtt{F}(X) = X(a + X^{r(q-1)})$ *is not a PP of* $\mathbb{F}_{q^2}$.

Theorem 1.2. *Let* q *be odd and let* a *and* e *be integers such that* $2 < a \leq e/4 + 1$. *Then* $\mathtt{F}_{a,q}(X) = X^{q-2} + X^{q^2-2} + \cdots + X^{q^{a-1}-2}$ *is not a PP of* $\mathbb{F}_{q^e}$.

Globally defined throughout the paper are two polynomials and a rational function; they appear in the typewriter font: $\mathtt{F}$ and $\mathtt{F}_{a,q}$ in the above theorems and $\mathtt{G}$ to be defined in (3.1).

Theorems 1.1 and 1.2 arise from different backgrounds, which we describe briefly below.

Let $\mathtt{F}(X) = X(a + X^{r(q-1)}) \in \mathbb{F}_{q^2}[X]$, where $2 \leq r \leq q$ and $a \in \mathbb{F}_{q^2}^*$. This polynomial has been studied by several authors; the primary goal is to determine the necessary and sufficient conditions on the parameters for $\mathtt{F}$ to be a PP of $\mathbb{F}_{q^2}$ [10,11,14,17,29]. The following is a summary of the existing results concerning the polynomial $\mathtt{F}$.

(i) [29] If $a^{q+1} = 1$, then $\mathtt{F}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(-a)^{(q+1)/\gcd(r,q+1)} \neq 1$ and $\gcd(r-1, q+1) = 1$.
(ii) [10] If $a^{q+1} \neq 1$ and $r = 2$, then $\mathtt{F}$ is a PP of $\mathbb{F}_{q^2}$ if and only if q is odd and $(-a)^{(q+1)/2} = 3$.
(iii) [14,17] For $a^{q+1} \neq 1$ and $r = 3, 5, 7$, there are only finitely many pairs (q, a) for which $\mathtt{F}$ is a PP of $\mathbb{F}_{q^2}$, and all such pairs are determined.
(iv) [11] If $a^{q+1} \neq 1$ and $r \geq 3$ is a prime, then there are only finitely many pairs (q, a) for which $\mathtt{F}$ is a PP of $\mathbb{F}_{q^2}$.

Theorem 1.1 of the present paper removes the requirement that r be a prime in Result (iv). We mention that the approach of the present paper is different from that of [11].

The background for Theorem 1.2 is different. Let $p = \operatorname{char} \mathbb{F}_q$. For $n \geq 0$, let $g_{n,q} \in \mathbb{F}_p[X]$ be the polynomial defined by the functional equation $\sum_{a \in \mathbb{F}_q} (X+a)^n = g_{n,q}(X^q - X)$. The polynomial $g_{n,q}$ was introduced in [9] and the permutation properties of $g_{n,q}$ in