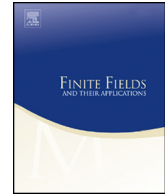




ELSEVIER

Contents lists available at ScienceDirect

Finite Fields and Their Applications

[www.elsevier.com/locate/ffa](http://www.elsevier.com/locate/ffa)


# A note on value sets of quartic polynomials



Robert C. Valentini

Department of Mathematics and Statistics, California State University,  
Long Beach, Long Beach, CA 90840, USA

## ARTICLE INFO

### Article history:

Received 8 August 2015

Accepted 27 January 2016

Communicated by Gary L. Mullen

### MSC:

11R58

11T55

### Keywords:

Quartic polynomial

Value set

Frobenius automorphism

## ABSTRACT

Let  $v$  be the number of distinct values of the polynomial  $f(x) = x^4 + ax^2 + bx$ , where  $a$  and  $b$  are elements of the finite field of size  $q$ , where  $q$  is odd. When  $b$  is 0, an exact formula for  $v$  can be given. When  $b$  is not 0,  $v = (5/8)q + O(\sqrt{q})$ , where the error term comes from the Riemann hypothesis. In this note we establish for the case that  $b$  is not 0, the inequality  $v \geq (q + 1)/2$ , without relying on the Riemann hypothesis.

© 2016 Elsevier Inc. All rights reserved.

## 1. Introduction

Let  $k$  be the finite field with  $q$  elements, where  $q$  is odd. Let  $g(x)$  be a quartic polynomial with coefficients in  $k$ . Let  $v$  be the number of distinct values of  $g(x)$ . By appropriate choice of  $\alpha$ ,  $\beta$ , and  $\gamma$ , the polynomial  $f(x) = \alpha g(x + \beta) + \gamma$  will have the form  $f(x) = x^4 + ax^2 + bx$  for some  $a$  and  $b$  of  $k$ . Since the number of distinct values of  $f(x)$  is the same as that of  $g(x)$ , in considering the possibilities for  $v$  it is sufficient to restrict attention to polynomials of the form  $f(x)$ .

E-mail address: [robert.valentini@csulb.edu](mailto:robert.valentini@csulb.edu).

<http://dx.doi.org/10.1016/j.ffa.2016.01.013>

1071-5797/© 2016 Elsevier Inc. All rights reserved.

In the case that  $b = 0$ , an exact formula for  $v$  can be obtained (see [5, p. 75] and [3] for  $q$  prime). For  $b \neq 0$ ,  $v = (5/8)q + O(\sqrt{q})$ , where the error term comes from the Riemann hypothesis for function fields over finite fields (see [5, p. 75] and [1]). In the next two sections we will consider the case that  $b \neq 0$  and establish the inequality  $v \geq (q + 1)/2$  without reference to the Riemann hypothesis.

## 2. No degree one ramification

If we set  $y = f(x)$ , the field extension  $k(x)/k(y)$  is separable of degree 4 and the minimal polynomial of  $x$  over  $k(y)$  is  $F(X) = f(X) - y$ . The discriminant of  $F(X)$  is a cubic polynomial in  $y$ . In this section we assume the discriminant is irreducible in  $k[y]$ . Hence no finite degree one primes of  $k[y]$  ramify in  $k(x)/k(y)$ .

For any  $c \in k$ ,  $y - c = f(x) - c$  is a quartic polynomial in  $k[x]$  and we may consider its factorization. Let

$$N_0 = \{c \in k \mid f(x) - c \text{ is irreducible}\}.$$

For  $i = 1, 2, 4$ , let

$$N_i = \{c \in k \mid f(x) - c \text{ has exactly } i \text{ distinct linear factors}\}.$$

Finally, let

$$N_3 = \{c \in k \mid f(x) - c \text{ factors into 2 distinct irreducible quadratics}\}.$$

By our assumption on the discriminant, these are the only possibilities for the factorization of  $f(x) - c$ . So if for  $i = 0, 1, 2, 3, 4$ , we let  $n_i = |N_i|$ , then we have

$$q = n_0 + n_1 + n_2 + n_3 + n_4 \tag{1}$$

and

$$q = n_1 + 2n_2 + 4n_4. \tag{2}$$

Furthermore,

$$v = n_1 + n_2 + n_4. \tag{3}$$

Now let  $K$  be the Galois closure of  $k(x)/k(y)$ . Then the Galois group  $G$  of  $K/k(y)$  is isomorphic to  $S_4$  [6]. The factorization of a degree one finite prime of  $k[y]$  in the extension  $k(x)/k(y)$  allows one to determine the nature of the Frobenius automorphism of any prime of  $K$  dividing it [4, pp. 97–99]. Indeed, since all elements of  $S_4$  with the same cycle structure are conjugate, we have Table 1.

Download English Version:

<https://daneshyari.com/en/article/4582696>

Download Persian Version:

<https://daneshyari.com/article/4582696>

[Daneshyari.com](https://daneshyari.com)