

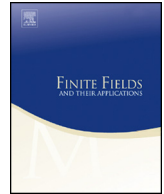


ELSEVIER

Contents lists available at ScienceDirect

# Finite Fields and Their Applications

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



## Irreducible factorization of translates of reversed Dickson polynomials over finite fields



Ron Evans<sup>a,\*</sup>, Mark Van Veen<sup>b</sup>

<sup>a</sup> Department of Mathematics, University of California at San Diego, La Jolla, CA 92093-0112, United States of America

<sup>b</sup> Varasco LLC, 2138 Edinburg Avenue, Cardiff by the Sea, CA 92007, United States of America

### ARTICLE INFO

#### Article history:

Received 6 February 2018

Received in revised form 15 May 2018

Accepted 1 August 2018

Available online xxxx

Communicated by Xiang-dong Hou

#### MSC:

11T06

12E10

13P05

#### Keywords:

Reversed Dickson polynomials over finite fields

Irreducible factorization of polynomials

Second order linear recurring sequence

Quadratic residuacity

### ABSTRACT

Let  $\mathbb{F}_q$  be a field of  $q$  elements, where  $q$  is a power of an odd prime. Fix  $n = (q + 1)/2$ . For each  $s \in \mathbb{F}_q$ , we describe all the irreducible factors over  $\mathbb{F}_q$  of the polynomial  $g_s(y) := y^n + (1 - y)^n - s$ , and we give a necessary and sufficient condition on  $s$  for  $g_s(y)$  to be irreducible.

© 2018 Elsevier Inc. All rights reserved.

\* Corresponding author.

E-mail addresses: [revans@ucsd.edu](mailto:revans@ucsd.edu) (R. Evans), [mark@varasco.com](mailto:mark@varasco.com) (M. Van Veen).

### 1. Introduction

Let  $\mathbb{F}_q$  be a field of  $q$  elements, where  $q$  is a power of an odd prime  $p$ . Fix

$$n = (q + 1)/2, \tag{1.1}$$

and write  $[n/2]$  for the floor of  $n/2$ . Define a polynomial  $f(y) \in \mathbb{F}_q[y]$  of degree  $[n/2]$  by

$$f(y) := (1 + \sqrt{y})^n + (1 - \sqrt{y})^n = D_n(2, 1 - y),$$

where  $D_n(2, 1 - y)$  is a reversed Dickson polynomial [5, eq. (1)]. Our choice of  $n$  in (1.1) was motivated by Katz’s work on local systems [6]. Indeed, by [3, Lemma 2.1],  $f(y)$  satisfies the equality

$$f(y)^2 = 2y^n + 2(1 - y)^n + 2, \tag{1.2}$$

which was instrumental in proving a theorem of Katz relating two twisted local systems [6, Theorem 16.6].

For each  $s \in \mathbb{F}_q$ , define the polynomial  $g_s(y) \in \mathbb{F}_q[y]$  of degree  $2[n/2]$  by

$$g_s(y) := y^n + (1 - y)^n - s = (f(y)^2 - 2s - 2)/2. \tag{1.3}$$

Observe that  $g_s(y)$  is a translate of the reversed Dickson polynomial  $g_0(y) = D_n(1, y - y^2)$  [5, eq. (3)]. For any zero  $x$  of  $g_s(y)$ , (1.3) can be written as

$$g_s(y) = (f(y)^2 - f(x)^2)/2. \tag{1.4}$$

By (1.4) and [3, Remark 2], the zeros of  $g_s(y)$  are all distinct when  $s \neq \pm 1$ .

The goal of this paper is to describe the irreducible factorization of  $g_s(y)$  over  $\mathbb{F}_q$ , for each  $s \in \mathbb{F}_q$ . We remark that irreducible factorizations of classical Dickson polynomials over  $\mathbb{F}_q$  have been given by Bhargava and Zieve [2, Theorem 3]; for related work, see the references in [8, Section 9.6.2].

Our study of the irreducible factors of  $g_s(y)$  was initially motivated by the following conjecture of the second author:

*For  $s \in \{\pm 1/2\}$  and  $q \equiv \pm 1 \pmod{12}$ , every irreducible factor of  $g_s(y)$  over  $\mathbb{F}_q$  has the form  $y^3 - (3/2)y^2 + (9/16)y - m$  for some  $m \in \mathbb{F}_q$ .*

For example, over  $\mathbb{F}_{13}$ , we have the complete factorizations

$$\begin{aligned} g_{-1/2}(y) &= y^7 + (1 - y)^7 + 7 = 7(y^3 + 5y^2 + 3y + 1)(y^3 + 5y^2 + 3y + 3), \\ g_{1/2}(y) &= y^7 + (1 - y)^7 - 7 = 7(y^3 + 5y^2 + 3y + 6)(y^3 + 5y^2 + 3y + 11). \end{aligned} \tag{1.5}$$

Download English Version:

<https://daneshyari.com/en/article/8895583>

Download Persian Version:

<https://daneshyari.com/article/8895583>

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