Finite Fields and Their Applications 50 (2018) 272–278

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Normal bases and irreducible polynomials

Hua Huang, Shanmeng Han, Wei Cao [*]

Department of Mathematics, Ningbo University, Ningbo, Zhejiang 315211, PR China

ARTICLE INFO

Article history:
Received 13 September 2016
Accepted 7 December 2017
Available online xxxx
Communicated by Gary L. Mullen

MSC:
11T06
05A15

Keywords:
Finite field
Normal basis
N-polynomial
q-polynomial

ABSTRACT

A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$. An irreducible polynomial in $\mathbb{F}_q[x]$ is called an N-polynomial if its roots are linearly independent over $\mathbb{F}_q$. Let p be the characteristic of $\mathbb{F}_q$. Pelis et al. showed that every monic irreducible polynomial with degree n and nonzero trace is an N-polynomial provided that n is either a power of p or a prime different from p and q is a primitive root modulo n. Chang et al. proved that the converse is also true. By comparing the number of N-polynomials with that of irreducible polynomials with nonzero traces, we present an alternative treatment to this problem and show that all the results mentioned above can be easily deduced from our main theorem.

1. Introduction

Let p be a prime number, $n \geq 2$ be an integer. Let $\mathbb{F}_q$ denote the finite field of q elements with characteristic p, and $\mathbb{F}_{q^n}$ be its extension of degree n. A *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$, i.e., a basis consisting of all the algebraic conjugates of a fixed element. We say that α generates a normal basis, or α is a

[*] Corresponding author.
E-mail address: caowei@nbu.edu.cn (W. Cao).

https://doi.org/10.1016/j.ffa.2017.12.004
1071-5797/© 2017 Elsevier Inc. All rights reserved.

normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In either case we are referring to the fact that the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$. In 1850, Eisenstein [3] first conjectured the existence of normal bases for finite fields, and its proof was given by Schönemann [13] later in 1850 for the case $\mathbb{F}_p$ and then by Hensel [6] in 1888 for arbitrary finite fields. Normal bases over finite fields have proved very useful for fast arithmetic computations with potential applications to coding theory and to cryptography, see, e.g., [4,7,8].

An irreducible polynomial in $\mathbb{F}_q[x]$ is called an *N-polynomial* if its roots are linearly independent over $\mathbb{F}_q$. The minimal polynomial of any element in a normal basis $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ is $m(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i}) \in \mathbb{F}_q[x]$, which is irreducible over $\mathbb{F}_q$. The elements in a normal basis are exactly the roots of an N-polynomial. Hence an N-polynomial is just another way of describing a normal basis. In general, it is not easy to check whether an irreducible polynomial is an N-polynomial. However in certain cases, the thing may be very simple according to Theorems 1.1 and 1.2 below.

Theorem 1.1. (Pelis [11]) *Let $n = p^e$ with $e \geqslant 1$. Then an irreducible polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ is an N-polynomial if and only if $a_1 \neq 0$.*

Theorem 1.2. (Pei, Wang and Omura [10]) *Let n be a prime different from p and q be a primitive root modulo n. Then an irreducible polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ is an N-polynomial if and only if $a_1 \neq 0$.*

In 2001, Chang, Truong and Reed [2] furthermore proved that the conditions in Theorems 1.1 and 1.2 are also necessary.

Theorem 1.3. *If every irreducible polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ with $a_1 \neq 0$ is an N-polynomial, then n is either a power of p or a prime different from p and q is a primitive root modulo n.*

By comparing the number of N-polynomials with that of irreducible polynomials over $\mathbb{F}_q$, we will present an alternative treatment to this problem. Throughout the rest of the paper, write $n = mp^e$ with $p \nmid m$. It will be seen that Theorems 1.1, 1.2 and 1.3 are all the direct consequences of the following theorem.

Theorem 1.4. (Main Theorem) *The following inequality holds*

$$q^{n-m} \prod_{d|m} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)} \leqslant \frac{q-1}{q} \sum_{d|m} \mu(d) q^{n/d}, \tag{1}$$

where $\tau(d)$ is the order of q modulo d, $\phi(d)$ is the Euler totient function, and $\mu(d)$ is the Möbius function. Furthermore, (1) becomes an equality if and only if $n = p^e$, or n is a prime different from p and q is a primitive root modulo n.