Finite Fields and Their Applications 51 (2018) 238–269

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Existence of primitive 1-normal elements in finite fields

Lucas Reis [1], David Thomson *

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

A R T I C L E   I N F O

Article history:
Received 28 October 2017
Received in revised form 3 February 2018
Accepted 4 February 2018
Available online xxxx
Communicated by D. Panario

MSC:
11T30
11T06
11T24
12E20

Keywords:
Finite fields
Primitive elements
Normal bases
k-Normal elements

A B S T R A C T

An element $\alpha \in \mathbb{F}_{q^n}$ is *normal* if $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ forms a basis of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$; in this case, $\mathcal{B}$ is a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The notion of k-normal elements was introduced in Huczynska et al. (2013) [10]. Using the same notation as before, α is k-normal if $\mathcal{B}$ spans a co-dimension k subspace of $\mathbb{F}_{q^n}$. It can be shown that 1-normal elements always exist in $\mathbb{F}_{q^n}$, and Huczynska et al. (2013) [10] show that elements that are simultaneously primitive and 1-normal exist for $q \geq 3$ and for large enough n when $\gcd(n, q) = 1$ (we note that primitive 1-normals cannot exist when $n = 2$). In this paper, we complete this theorem and show that primitive, 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ exist for all prime powers q and all integers $n \geq 3$, thus solving Problem 6.3 from Huczynska et al. (2013) [10].

* Corresponding author.
E-mail addresses: lucasreismat@gmail.com (L. Reis), dthomson@math.carleton.ca (D. Thomson).
[1] Permanent address: Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG 30123-970, Brazil.

https://doi.org/10.1016/j.ffa.2018.02.002

1. Introduction

Let q be a power of a prime, there is a unique (up to isomorphism) finite field of q elements, denoted $\mathbb{F}_q$. For all positive integers n, the finite extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ can be viewed as a vector space over $\mathbb{F}_q$. Finite extension fields display cyclicity in multiple forms; for example, their Galois groups are cyclic of order n, generated by the Frobenius automorphism $\alpha_q(\alpha) = \alpha^q$ for any $\alpha \in \mathbb{F}_{q^n}$. The multiplicative group of $\mathbb{F}_{q^n}$, denoted $\mathbb{F}_{q^n}^*$ is a cyclic group of order $q^n - 1$.

An element $\alpha \in \mathbb{F}_{q^n}$ is *primitive* if it is a generator of $\mathbb{F}_{q^n}^*$. An element $\alpha \in \mathbb{F}_{q^n}$ is *normal* in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if its Galois orbit is a spanning set for $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Specifically, α is a normal element if $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, whence we call $\mathcal{B}$ a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The existence of normal elements of finite extension fields $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ was established for all q and n by Hensel [9] in 1888 and re-established by Ore [14] in 1934 by studying properties of linearized polynomials. In this work, we draw on ideas extending from Ore.

A natural question is to establish the existence of elements of $\mathbb{F}_{q^n}$ which are simultaneously primitive and normal over $\mathbb{F}_q$. This was proven for q sufficiently large by Carlitz [3] in 1952 and completely when $q = p$ a prime by Davenport [8] in 1968. The *primitive normal basis theorem* was finally established for all q, n by Lenstra and Schoof in 1988 [11] using a combination of character sums, sieving results and a computer search. Using more complicated sieving techniques, Cohen and Huczynska [4] established the primitive normal basis theorem for all q and n without the use of a computer in 2003.

Recently, Huczynska et al. [10] defined *k-normal elements* as generalizations of normal elements. In [10], they showed multiple equivalent definitions, we pick the most natural for this work.

Definition 1.1. Let $\alpha \in \mathbb{F}_{q^n}$, then α is k-normal over $\mathbb{F}_q$ if its orbit under the cyclic (Frobenius) Galois action spans a co-dimension k subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; that is, if $V = \mathrm{Span}(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$, then $\dim_{\mathbb{F}_q}(V) = n - k$.

Under Definition 1.1, normal elements are 0-normal elements, and all elements of $\mathbb{F}_{q^n}$ are k-normal for some $0 \le k \le n$. Notice that it is important to specify over which field subfield an element of $\mathbb{F}_{q^n}$ is k-normal. If not otherwise specified, when we say $\alpha \in \mathbb{F}_{q^n}$ is k-normal, we always assume it is k-normal over $\mathbb{F}_q$.

It can be shown (see Section 2) that there always exist 1-normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In [10], using a similar methodology to Lenstra-Schoof, the authors partially establish a primitive 1-normal element theorem; that is, the existence of elements which simultaneously generate the multiplicative group of a finite fields and whose Galois orbit is a spanning set of a (Frobenius-invariant) hyperplane.

Theorem 1.2 *([10], Theorem 5.10). Let $q = p^e$ be a prime power and n a positive integer not divisible by p. Assume that $n \ge 6$ if $q \ge 11$ and that $n \ge 3$ if $3 \le q \le 9$. Then there exists a primitive 1-normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*