Finite Fields and Their Applications 26 (2014) 123–143

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Normal bases and primitive elements over finite fields

Giorgos Kapetanakis *

Department of Mathematics, University of Crete, Voutes Campus, 70013, Heraklion, Greece

ARTICLE INFO

Article history:
Received 2 October 2013
Received in revised form 22 November 2013
Accepted 3 December 2013
Available online 21 December 2013
Communicated by D. Panario

MSC:
11T30
11T06
11T24
12E20

Keywords:
Primitive element
Free element
Normal basis
Character sum
Finite field

ABSTRACT

Let q be a prime power, $m \geqslant 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ if $q = 2$ and m is odd. We prove an extension of the primitive normal basis theorem and its strong version. Namely, we show that, except for an explicit small list of genuine exceptions, for every q, m and A, there exists some primitive $x \in \mathbb{F}_{q^m}$ such that both x and $(ax+b)/(cx+d)$ produce a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

1. Introduction

Let q be a power of some prime number p. We denote by $\mathbb{F}_q$ the finite field of q elements and by $\mathbb{F}_{q^m}$ its extension of degree m. A generator of the multiplicative group $\mathbb{F}_{q^m}^*$ is called *primitive* and an element $x \in \mathbb{F}_{q^m}$ is called *free*, if the set $\{x, x^q, x^{q^2}, \ldots, x^{q^{m-1}}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$. Such a basis is called *normal*.

* Fax: +30 2810 393881.
E-mail address: gkapet@math.uoc.gr.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.12.002

It is well-known that both primitive and free elements exist. The existence of elements that are simultaneously primitive and free is also known:

Theorem 1.1 *(Primitive normal basis theorem). Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ that is simultaneously primitive and free.*

Lenstra and Schoof [14] were the first to provide a complete proof of the above, completing partial proofs of Carlitz [1,2] and Davenport [10]. Later, Cohen and Huczynska [8] provided a computer-free proof, with the help of sieving techniques, previously introduced by Cohen [5]. Also, several generalizations of Theorem 1.1 have been investigated [7,11,19]. Recently, an even stronger result was shown.

Theorem 1.2 *(Strong primitive normal basis theorem). Let q be a prime power and m a positive integer. There exists some $x \in \mathbb{F}_{q^m}$ such that x and x^{-1} are both simultaneously primitive and free, unless the pair (q, m) is one of $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$ or $(5, 4)$.*

Tian and Qi [18] were the first to prove this result for $m \geqslant 32$, but Cohen and Huczynska [9] were those who extended it to its stated form, once again with the help of their sieving techniques. The reader is referred to [6,12] and the references therein, for more complete surveys of this, very active, line of research.

More recently, an extension of both theorems was considered [13]:

Theorem 1.3. *Let $q \geqslant 23$ be a prime power, $m \geqslant 17$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, such that if A has exactly two non-zero entries and q is odd, then the quotient of these entries is a square in $\mathbb{F}_{q^m}$. There exists some $x \in \mathbb{F}_{q^m}$ such that both x and $(ax + b)/(cx + d)$ are simultaneously primitive and free.*

Clearly, Theorems 1.1 and 1.2 are special cases of the above, for matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & a \\ a & 0 \end{smallmatrix}\right)$, where $a \neq 0$, respectively. It is clear though, that despite Theorem 1.3 being a natural extension of Theorems 1.1 and 1.2, the large number of possible exceptions leaves room for improvement. It is worth noting though, that, since the mentioned sieving techniques have been employed in this work, one would not expect much improvement. On the other hand, thanks to a notice of Stephen Cohen, if the condition of $(ax + b)/(cx + d)$ to be primitive was missing from Theorem 1.3, the resulting problem would still be an extension of Theorems 1.1 and 1.2 (to make this clear, notice that the two conditions of x and x^{-1} to be primitive in Theorem 1.2 overlap, i.e. the latter actually has three genuine conditions) and also would be of comparable complexity with Theorem 1.2, thus a pursue to a complete solution would be more realistic.

In this paper, we omit the condition of $(ax+b)/(cx+d)$ to be primitive in Theorem 1.3 and completely solve the resulting problem. In particular, we prove the following:

Theorem 1.4. *Let q be a prime power, $m \geqslant 2$ an integer and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, where $A \neq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ if $q = 2$ and m is odd. There exists some primitive $x \in \mathbb{F}_{q^m}$, such that*