Finite Fields and Their Applications 25 (2014) 326–340

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Standard sequence subgroups in finite fields [☆]

Owen J. Brison [a,*], J. Eurico Nogueira [b]

[a] Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa, Bloco C6, Piso 2, Campo Grande, 1749-016 Lisboa, Portugal

[b] Departamento de Matemática, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Quinta da Torre, 2825-114 Monte da Caparica, Portugal

ARTICLE INFO

Article history:
Received 13 May 2013
Received in revised form 13 October 2013
Accepted 21 October 2013
Available online 15 November 2013
Communicated by Gary L. Mullen

MSC:
11B39
12E20

Keywords:
Linear recurrence relation
Finite field
Standard subgroup
Restricted period

ABSTRACT

In previous work, the authors describe certain configurations which give rise to standard and to non-standard subgroups for linear recurrences of order $k = 2$, while in subsequent work, a number of families of non-standard subgroups for recurrences of order $k \geqslant 2$ are described. Here we exhibit two infinite families of standard groups for $k \geqslant 2$.

1. Introduction

In what follows, p will always denote a prime, q a power of p, $\mathbb{F}_q$ the field of order q and $\mathbb{A}_q$ a fixed algebraic closure of $\mathbb{F}_q$. We will assume that all our finite extensions of $\mathbb{F}_q$ are subfields of $\mathbb{A}_q$. Further, k will be a positive integer and $\mathbb{N}$ will denote the set of all positive integers.

☆ This research was partially supported by the Fundação de Ciência e Tecnologia, and was undertaken within the "Centro de Estruturas Lineares e Combinatórias da Universidade de Lisboa".

* Corresponding author.
E-mail addresses: ojbrison@fc.ul.pt (O.J. Brison), jen@fct.unl.pt (J.E. Nogueira).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.10.009

Definition 1.1. Let

$$f(t) = t^k - f_{k-1}t^{k-1} - \cdots - f_1 t - f_0 \in \mathbb{F}_q[t]$$

where $f(0) \neq 0$.

(a) An *f-sequence* in $\mathbb{A}_q$ is a (doubly-infinite) sequence $S = (s_i)_{i\in\mathbb{Z}}$ of elements $s_i \in \mathbb{A}_q$ such that

$$s_i = f_{k-1}s_{i-1} + \cdots + f_1 s_{i-k+1} + f_0 s_{i-k}$$

for all $i \in \mathbb{Z}$.

(b) An *f-subgroup* is a finite subgroup $M \leqslant \mathbb{L}^*$, where $\mathbb{L} \subseteq \mathbb{A}_q$ is a finite extension of $\mathbb{F}_q$, such that M may be written as (the underlying set of a minimal periodic segment of) a periodic f-sequence

$$(\cdots, m_0 = 1, m_1, \ldots, m_{|M|-1}, \ldots)$$

of least period $|M|$, where $|M|$ denotes the order of M. In this situation we say that the f-sequence $(m_i)_{i\in\mathbb{Z}}$ *represents M as an f-subgroup*.

(c) The f-sequence $S = (s_i)_{i\in\mathbb{Z}}$ in $\mathbb{A}_q^*$ is called *cyclic* if there exists $\lambda \in \mathbb{A}_q^*$ such that $s_{i+1} = \lambda s_i$ for all $i \in \mathbb{Z}$; in this situation, λ will be called the *common ratio* of S.

(d) The *unit f-sequence*, $\mathcal{U} = (u_n)_{n\in\mathbb{Z}}$, is the f-sequence in $\mathbb{F}_q$ defined by $u_0 = \cdots = u_{k-2} = 0$, $u_{k-1} = 1$ if $k > 1$; when $k = 1$ the unit f-sequence will be the f-sequence defined by $u_0 = 1$.

(e) The *restricted period*, $\delta(f)$ of f, is defined to be 1 if $k = 1$ and is the least integer $n > 0$ with $u_n = \cdots = u_{n+k-2} = 0$ if $k > 1$ (see [3]).

In (a) it is known (because $f(0) \neq 0$) that an f-sequence must be periodic: see 8.11 of [8]. In (e), it is clear that if $k > 1$ then $\delta(f) \geqslant k$.

The following lemma relates f-subgroups with cyclic f-sequences.

Lemma 1.2. *Suppose that $f(t) \in \mathbb{F}_q[t]$ is monic of degree k with $f(0) \neq 0$.*

(a) *Suppose that S is a non-null cyclic f-sequence in $\mathbb{A}_q^*$ with common ratio $\lambda \neq 0$. If S contains* 1 *then S represents $\langle\lambda\rangle \leqslant \mathbb{A}^*$ as an f-subgroup and $f(\lambda) = 0$.*

(b) *Let M be an f-subgroup. Then M is a cyclic group. If S is a cyclic f-sequence which represents M then the common ratio λ of S satisfies $M = \langle\lambda\rangle$ and $f(\lambda) = 0$.*

(c) *Suppose $M \leqslant \mathbb{A}_q^*$ is finite. Suppose $M = \langle\lambda\rangle$ and let $m(t)$ be the minimum polynomial of λ over $\mathbb{F}_q$. Then M is an m-group and also an f-group for any multiple $f(t)$ of $m(t)$ in $\mathbb{F}_q[t]$.*

Proof. For (a) and (b), see Lemma 1.3 of [5]. Note that in (a), S is periodic because $f(0) \neq 0$ and so λ has finite multiplicative order, while in (b) a finite subgroup of the multiplicative group of a field is always cyclic: see Exercise 2.9 in [8].

(c) It is clear that $\{1, \lambda, \ldots\}$ exhibits $M = \langle\lambda\rangle$ as an m-sequence; then by Theorem 8.42 of [8], M is an f-subgroup for any multiple $f(t)$ of $m(t)$ in $\mathbb{F}_q[t]$. $\square$

The motivation for studying f-subgroups seems to go back to Somer [9,10]. In particular, if $\omega \in \mathbb{A}_q^*$ is a root of $f(t) \in \mathbb{F}_q[t]$ then $\langle\omega\rangle \leqslant \mathbb{A}_q^*$ may be regarded as (the underlying set of) an f-sequence of minimal period $|\omega|$:

$$\langle\omega\rangle = \left(\cdots, 1, \omega, \omega^2, \ldots, \omega^{|\omega|-1}, \ldots\right).$$

It can sometimes happen, for certain choices of $\mathbb{F}_q$, $f(t)$ and ω with $f(\omega) = 0$, that the subgroup $\langle\omega\rangle$ may be represented in an alternative, “less obvious”, manner as an f-sequence; this leads to the following definition: