Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 9 (2003) 413–422

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Linear recurring sequence subgroups in finite fields[☆]

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

[a] *Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa, Bloco C1, Piso 3, 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*

Received 13 August 2001; revised 10 February 2003

Communicated by Peter Jau-Shyong Shiue

Abstract

Given a finite field $\mathbb{F}$ and a linear recurrence relation over $\mathbb{F}$ it is possible to find, in a fairly "obvious" way, a finite extension $\mathbb{L}$ of $\mathbb{F}$ and a subgroup M of the multiplicative group of $\mathbb{L}$ such that the elements of M may be written, without repetition, so as to form a cyclically closed sequence which obeys the recurrence. Here we investigate this phenomenon for second-order recurrences; the situation in which $\mathbb{F}$ has prime order and the characteristic polynomial of the relation is irreducible over $\mathbb{F}$ is described.

Keywords: Linear recurrence relation; Finite field; Subgroup; Group permutation polynomial

1. Introduction

In certain finite fields $\mathbb{F}$, it is possible to find a subgroup M of the multiplicative group of $\mathbb{F}$ such that the elements of M may be written, without repetition, so as to form a cyclically closed Fibonacci sequence; that is, $M = (\mu_0, \mu_1, \dots, \mu_{m-1})$ and $\mu_{i+2} = \mu_{i+1} + \mu_i$ for all relevant i, with indices $(\bmod\, m)$. For example, the

[☆] The authors acknowledge the partial support of the "Centro de Estruturas Lineares e Combinatórias" and of the Praxis Program (Praxis/2/2.1/mat/73/94).

[*] Corresponding author.

E-mail addresses: brison@ptmat.fc.ul.pt (O.J. Brison), jen@fct.unl.pt (J.E. Nogueira).

1071-5797/03/$ - see front matter © 2003 Elsevier Science (USA). All rights reserved.
doi:10.1016/S1071-5797(03)00014-5

multiplicative group of $\mathbb{F}_{11}$ and its subgroup of squares may be written

$$(1, 8, 9, 6, 4, 10, 3, 2, 5, 7) \quad \text{and} \quad (1, 4, 5, 9, 3),$$

respectively. We will see, (1.5), that there is an "obvious" way for this to occur, and the natural question, addressed in this paper, is whether the obvious way is the only way. It happens that the obvious way is the only way in many, but not all, cases and it is this behaviour which interested us. This seems to have been investigated first by Somer, [5,6]; see also [1].

We study this phenomenon for sequences which obey general second-order linear recurrence relations of the form

$$\mu_{i+2} = \sigma\mu_{i+1} + \rho\mu_i, \tag{1}$$

over a finite field $\mathbb{F}$, where $\sigma, \rho \in \mathbb{F}$, $\rho \neq 0$. Associated with (1) is the so-called *characteristic polynomial* of the relation

$$f(t) = t^2 - \sigma t - \rho \in \mathbb{F}[t],$$

a sequence which obeys (1) will be called an *f-sequence*.

Preliminaries 1.1. Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of order q and let $\mathbb{F}^*$ denote the multiplicative group of $\mathbb{F}$. If G is a finite group and $g \in G$ then $|G|$ and $|g|$ denote their respective orders. Our characteristic polynomials $f(t)$ are all monic, quadratic and satisfy $f(0) \neq 0$, so we write

$$\mathbb{F}_0[t] := \{f(t) \in \mathbb{F}[t]\colon f \text{ is monic, quadratic and } f(0) \neq 0\}.$$

Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{F}_0[t]$.

(a) The *unit f-sequence in* $\mathbb{F}$ (the *impulse-response* f-sequence in [4]) is the f-sequence $(u_i)_{i \in \mathbb{N}_0}$ such that $u_0 = 0$, $u_1 = 1$. If $n, b \in \mathbb{N}_0$ then $u_{n+b} = u_{n+1}u_b + \rho u_n u_{b-1}$: this is easy to prove by induction; alternatively, see [3, Lemma 1(a)].

(b) The *least period* of an f-sequence $(s_i)_{i \in \mathbb{N}_0}$ in $\mathbb{F}$ is the smallest natural number m such that $s_i = s_{i+m}$ for all $i \in \mathbb{N}_0$.

(c) The *order* of f, written ord(f), is the least natural number e for which $f(t)$ divides $t^e - 1$. If f has distinct roots ξ, ζ in an extension field $\mathbb{L}$ of $\mathbb{F}$ then $\text{ord}(f) = \text{lcm}(|\xi|, |\zeta|)$ (see [4, 3.11]).

Definition 1.2. Let $\mathbb{F}$ be a finite field and let $f(t) = t^2 - \sigma t - \rho \in \mathbb{F}_0[t]$.

By an *f-subgroup* we understand a subgroup $M \leqslant \mathbb{K}^*$, where $\mathbb{K}$ is some finite extension of $\mathbb{F}$, such that M may be written as

$$M = \{\mu_0 = 1, \mu_1, \ldots, \mu_{m-1}\} = \{\mu_i\},$$

where $\mu_{i+2} = \sigma\mu_{i+1} + \rho\mu_i$ for all i (indices $(\bmod\, m)$) and $\mu_i \neq \mu_j$ if $0 \leqslant i \neq j < m$. We emphasise that notation is always standardised so that $\mu_0 = 1$. In this situation we say that the f-sequence $(\mu_i)_{i\in\mathbb{N}_0}$ *represents* M.

Observation 1.3. Suppose that $f \in \mathbb{F}_0[t]$, that $\mathbb{K}$ is a finite extension of $\mathbb{F}$ and that M is an f-subgroup of $\mathbb{K}^*$. By [4, 8.27], $|M|$ divides $\mathrm{ord}(f)$.

Suppose f has roots $\xi \neq \zeta$ in the splitting field $\mathbb{L}$ of f over $\mathbb{K}$, so $\mathbb{L} = \mathbb{K}(\xi, \zeta)$. Now $\mathrm{ord}(f) = \mathrm{lcm}(|\xi|, |\zeta|)$ divides $|\mathbb{F}(\xi,\zeta)^*|$ and so $M \leqslant \mathbb{F}(\xi,\zeta)^*$ as $\mathbb{L}^*$ has a unique subgroup of each possible order.

Suppose f has the repeated root $\xi \in \mathbb{F}$. By [4, 3.8] $\mathrm{ord}(f) = |\xi|p$, where p is the characteristic of $\mathbb{F}$. Thus $|M|$ divides $|\xi|$ because $M \leqslant \mathbb{K}^*$, whence $M \leqslant \mathbb{F}^*$.

In particular, an f-subgroup is always contained in the splitting field of f over $\mathbb{F}$; this will in future be assumed without comment.

Furthermore, if f is irreducible over $\mathbb{F}$ then $|M| = \mathrm{ord}(f) = |\xi|$, the first equality by [4, 8.28], and then $M = \langle \xi \rangle$.

Lemma 1.4. *Let $\mathbb{F}$ be a finite field and let $f(t) = t^2 - \sigma t - \rho \in \mathbb{F}_0[t]$. If $M = \{1, \mu_1, \ldots\}$ is an f-subgroup with $|M| \leqslant 4$ then $f(\mu_1) = 0$.*

Proof

(a) If $M = 1$ then $1 = \sigma + \rho$ and $f(1) = 0$.

(b) If $|M| = 2$ then $M = \{1, -1\}$, whence $1 = -\sigma + \rho$ and $f(-1) = 0$.

(c) If $|M| = 3$ then $M = \{1, \mu_1, \mu_1^2\}$ and $f(\mu_1) = 0$.

(d) Suppose $|M| = 4$. If $|\mu_1| = 4$ and $\mu_2 = \mu_1^2$ then $f(\mu_1) = 0$. If $|\mu_1| = 4$ and $\mu_2 = \mu_1^3$ then $\mu_3 = \mu_1^2$ whence $\mu_1^3 = \sigma\mu_1 + \rho$ and $1 = \sigma\mu_1^2 + \rho\mu_1^3$. The last equation gives $\mu_1^3 = \sigma\mu_1 + \rho\mu_1^2$, so $\rho\mu_1^2 = \rho$ and $\mu_1^2 = 1$, a contradiction. If $|\mu_1| = 2$, similar reasoning gives a contradiction. □

Observation 1.5. Let $f \in \mathbb{F}_0[t]$ and let ξ, ζ be the roots of f in a splitting field. Write $|\xi| = m$. Then $(1, \xi, \xi^2, \ldots, \xi^{m-1}, \ldots)$ is clearly an f-sequence, and $M = \langle \xi \rangle$ is an f-subgroup. If $|\zeta| = |\xi|$ then $(1, \zeta, \zeta^2, \ldots)$ is another way of writing M as an f-subgroup.

This is the "obvious" way for an f-subgroup to occur. By Lemma 1.4, any f-subgroup of order at most 4 can only be written in this way. There exist cases when it is possible to rewrite an f-subgroup $\langle \xi \rangle$ as an f-sequence $(1, \beta, \gamma, \ldots)$ where β is *not* a root of f: examples of this phenomenon will be given in Section 2. By Observation 1.3, if f is irreducible then any f-subgroup has the form $\langle \xi \rangle$ (considered as a group), but we have no proof that this must occur in general.

These considerations motivate the following.

Definition 1.6. Let $\mathbb{F}$ be a finite field and $f \in \mathbb{F}_0[t]$. Suppose that M is an f-subgroup. Then M is said to be *nonstandard* if there exists a choice of $\beta \in \mathbb{L}^*$ where

$f(\beta)\neq 0$ such that for $\mu_1 = \beta$ we have $M = \{1, \mu_1, \dots\}$; otherwise, M is said to be *standard.*

Thus by Lemma 1.4, any f-subgroup of order at most 4 is standard. There is another general situation where it is very easy to prove that an f-subgroup must be standard.

Proposition 1.7. *Let $\mathbb{F}$ be a finite field and let $f(t)\in\mathbb{F}_0[t]$. Suppose that $f(t)$ has a double root $\xi\in\mathbb{F}^*$ and that M is an f-subgroup. Then M is standard.*

Proof. Write $|M| = m$; then $m \mid \operatorname{ord}(f)$ by [4, 8.27]. By [4, 8.23], we have

$$M = \{(\alpha + n\beta)\xi^n\colon\ n\in\mathbb{N}_0\} = \{(\alpha + n\beta)\xi^n\colon\ 0\leqslant n\leqslant m-1\}.$$

Write $\mu_n = (\alpha + n\beta)\xi^n$ (with $\mu_0 = 1$); then $\alpha = 1$ and $\mu_n = (1 + n\beta)\xi^n$. Because $\mu_m = \mu_0$ then $(1 + m\beta)\xi^m = 1$, and then because $\mu_1 = \mu_{m+1}$ and $\xi\neq 0$, easy calculations give $\beta = \beta\xi^m$. If $\beta\neq 0$ then $\xi^m = 1$, whence $1 + m\beta = 1$ and $m\beta = 0$. But $m \mid |\mathbb{F}^*|$ so $m\neq 0$ and then $\beta = 0$. The assertion follows. □

The proof of our main result, Theorem 3.1, depends on the following Hermite-type condition for a polynomial to permute the elements of a finite multiplicative subgroup of a field. For the reader's convenience, we outline a proof; more details are given in [2, Theorem 3.3].

Theorem 1.8 (Brison [2]). *Let $\mathbb{F}$ be a field and suppose that $G\leqslant\mathbb{F}^*$ where $|G| = m\in\mathbb{N}$. Suppose that $g(t)\in\mathbb{F}[t]$ induces a permutation of the elements of G. If $b\in\mathbb{N}$, let $\bar{g}^{(b)}(t)$ denote the reduction of $(g(t))^b \pmod{(t^m - 1)}$ and let $\phi_0^{(b)}$ denote the constant term of $\bar{g}^{(b)}(t)$. Then $\phi_0^{(b)} = 0$ whenever $b\not\equiv 0 \pmod{m}$.*

Proof. For $b\in\mathbb{N}$, write $S_b = \sum_{k\in G} k^b$. The elements of G are precisely the roots of $t^m - 1$; it follows by Newton's Formula [4, 1.75] that $S_b = 0$ if $1\leqslant b<m$ and thus that $S_b = 0$ whenever $b\not\equiv 0 \pmod{m}$ because $k^m = 1$ for $k\in G$.

Now $S_b = \sum_{k\in G} (g(k))^b$ because g permutes the elements of G. Write $\bar{g}^{(b)}(t) = \sum_{i=0}^{m-1}\phi_i^{(b)}t^i$, where $\phi_i^{(b)}\in\mathbb{F}$. Then $(g(k))^b = \bar{g}^{(b)}(k) = \sum_{i=0}^{m-1}\phi_i^{(b)}k^i$ for $k\in G$ and so

$$S_b = \sum_{k\in G}\sum_{i=0}^{m-1}\phi_i^{(b)}k^i = \phi_0^{(b)}m + \phi_1^{(b)}S_1 + \cdots + \phi_{m-1}^{(b)}S_{m-1},$$

whence $S_b = \phi_0^{(b)}m$, for $b\in\mathbb{N}$, because $S_1 = \cdots = S_{m-1} = 0$. Because $G\leqslant\mathbb{F}^*$ then m, considered as an element of $\mathbb{F}$, is nonzero. Thus $\phi_0^{(b)} = 0$ whenever $b\not\equiv 0 \pmod{m}$. □

2. Some nonstandard subgroups

In this section some general configurations which give rise to nonstandard f-subgroups are presented. Firstly, an example.

Example 2.1. Let $f(t) = t^2 - t - 1 \in \mathbb{F}_3[t]$; f is irreducible over $\mathbb{F}_3$ and splits in $\mathbb{F}_9$. Easy calculations show that for *any* of the six elements $\lambda \in \mathbb{F}_9^* \backslash \mathbb{F}_3^*$, the f-sequence $(1, \lambda, \ldots)$ represents $\mathbb{F}_9^*$; thus $\mathbb{F}_9^*$ is a nonstandard f-subgroup. This example illustrates the case $q = 3$ and $\mathrm{ord}(f) = 8$ of Proposition 2.4.

Lemma 2.2. *Let $\mathbb{L}$ be a finite field of odd characteristic. Let $\xi \in \mathbb{L}^*$. Then*

(a) *Not both $|\xi|$ and $|-\xi|$ can be odd.*
(b) *Suppose that $|\xi| = 2k$ where $k \in \mathbb{N}$. If k is even then $|\xi| = |-\xi|$. If k is odd then $|-\xi| = k$ and $|\xi| = 2|-\xi|$.*

Proof.

(a) If $h := |\xi| \times |-\xi|$ were odd then $1 = (\xi)^h/(-\xi)^h = (-1)^h = -1$, which is false.
(b) We have $|\xi^k| = 2$, $\xi^k = -1$ and $-\xi = \xi^{k+1}$. If k is even then $\gcd(2k, k+1) = 1$ and $|-\xi| = |\xi|$. If k is odd then $\gcd(2k, k+1) = 2$ and so $k + 1 = 2v$, where $v \in \mathbb{N}$ with $\gcd(|\xi|, v) = 1$. But now $-\xi = \xi^{k+1} = (\xi^v)^2$, where $|\xi^v| = |\xi|$, and the final assertion follows. □

Proposition 2.3. *Let $\mathbb{F}$ be a finite field of odd characteristic and $\mathbb{L}$ be the splitting field of $f(t) = t^2 - \rho \in \mathbb{F}_0[t]$. Let $\xi \in \mathbb{L}^*$ be a root of f with $|\xi|$ even. Let M be an f-subgroup with $|M| > 4$.*

(a) *If $|M|$ is odd then $M = \langle -\xi \rangle$ and M is standard.*
(b) *If $|M|$ is even then $M = \langle \xi \rangle$ and M is nonstandard. Moreover, when $|\rho|$ is even then $|M|$ is even.*

Proof. That f has a root of even order follows from Lemma 2.2.

Write $|M| = m$. Because M is an f-subgroup then

$$M = (\mu_0, \mu_1, \ldots) = (1, a, \rho, a\rho, \ldots, 1, a, \ldots), \tag{2}$$

for some $a \in \mathbb{L}^*$, and $\mu_k = 1$ if and only if $m \mid k$. We have $\mu_{2h} = \rho^h$ and $\mu_{2h+1} = a\rho^h$ for $h \geqslant 0$. Because $1 = \rho^{|\rho|} = \mu_{2|\rho|}$ then $m \mid 2|\rho|$ and so $|\rho| > 2$ because $m > 4$.

Suppose firstly that m is odd; then $m = 2n + 1$ with $n \in \mathbb{N}$. We have $1 = \mu_m = \mu_{2m}$ and so $1 = a\rho^n = \rho^m = \rho^{2n+1}$. Thus, $|\rho| \mid m$, and so $m = |\rho|$ because m is odd and $m \mid 2|\rho|$; in particular, $|\rho|$ is odd. This, incidentally, proves the final statement of (b).

We also have $a = \rho^{n+1}$ and $a^2 = \rho$, whence $|a| = |\rho|$. Thus a is an odd-order root of $f(t)$, so $a = -\xi$ and $M = (1, a, a^2, \ldots) = \langle -\xi \rangle$ is standard.

Suppose next that m is even with $m > 4$. If M were standard, the only possible representing f-sequences for M would be

$$(1, \xi, \rho, \xi\rho, \ldots) \quad \text{and} \quad (1, -\xi, \rho, -\xi\rho, \ldots),$$

with the second only if $|-\xi|$ is even (as otherwise $\langle -\xi \rangle \neq M$). Choose $d \in \langle \rho \rangle$ so that $d \neq \pm 1$: this is possible because $|\rho| > 2$. Then

$$\begin{aligned}\{1, d\xi, \rho, d\xi\rho, \ldots\} &= \{1, \rho, \ldots\} \dot\cup \xi d\{1, \rho, \ldots\} \\ &= \{1, \rho, \ldots\} \dot\cup \xi\{1, \rho, \ldots\} \\ &= M,\end{aligned}$$

and $(1, d\xi, \rho, d\xi\rho, \ldots)$ is an f-sequence which represents M while $f(d\xi) \neq 0$. Thus M is nonstandard. □

Proposition 2.4. *Let $\mathbb{F}$ be a finite field of order q and $f \in \mathbb{F}_0[t]$ be irreducible with order $q^2 - 1$. Then every f-subgroup M with $|M| > 4$ is nonstandard.*

Proof. Let $\mathbb{K}$ be the splitting field of f over $\mathbb{F}$ and let M be an f-subgroup with $|M| > 4$. We have $|M| = \mathrm{ord}(f) = q^2 - 1 = |\mathbb{K}^*|$, the first equality by [4, 8.28]; in particular, $q \geqslant 3$. Thus $M = \mathbb{K}^*$. Let ξ be a root of f in $\mathbb{K}$.

Recall that $(u_n)_{n \in \mathbb{N}_0}$ denotes the unit f-sequence in $\mathbb{F}_q$. By [4, 8.27], $(u_n)_{n \in \mathbb{N}_0}$ has least period $q^2 - 1$ and $u_{q^2-1} = 0$. Let $\alpha(f)$ be the least element of $\{n \in \mathbb{N}: u_n = 0\}$; it is well-known that if $n \in \mathbb{N}_0$ then $u_n = 0$ if and only if $\alpha(f) \mid n$.

Fix $b \in \mathbb{N}$ such that $0 < b \leqslant q^2 - 2$ and $b \not\equiv 0 \pmod{\alpha(f)}$; then $u_b \neq 0$ while if $n \in \mathbb{N}_0$ then $(u_n, u_{n+b}) \neq (0, 0)$. Thus $u_n + \xi u_{n+b} \neq 0$ for all $n \in \mathbb{N}_0$ because $\{1, \xi\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}_q$.

Suppose $u_k + \xi u_{k+b} = u_m + \xi u_{m+b}$ where $0 \leqslant k \leqslant m \leqslant q^2 - 2$. Then $u_k = u_m$ and $u_{k+b} = u_{m+b}$. By 1.1(a),

$$u_{k+b} = u_{k+1}u_b + \rho u_k u_{b-1}$$

$$u_{m+b} = u_{m+1}u_b + \rho u_m u_{b-1},$$

and so $u_{k+1} = u_{m+1}$. From this, the fact that $u_k = u_m$ and the fact that the sequence is determined by any two consecutive terms, we conclude that $m - k$ is divisible by the least period, $q^2 - 1$. Thus $k = m$. It follows that $|\{u_k + \xi u_{k+b}: 0 \leqslant k \leqslant q^2 - 2\}| = q^2 - 1$, and since $u_k + \xi u_{k+b} \neq 0$ for all k, then

$$\{u_k + \xi u_{k+b}: 0 \leqslant k \leqslant q^2 - 2\} = \mathbb{K}^* = M.$$

Suppose now that $0 \leqslant c \neq d \leqslant q^2 - 2$ with $c, d \not\equiv 0 \pmod{\alpha(f)}$. If for some h, $0 \leqslant h \leqslant q^2 - 2$, we have

$$u_0 + \xi u_c = u_h + \xi u_{h+d}$$

and

$$u_1 + \xi u_{1+c} = u_{h+1} + \xi u_{h+1+d}$$

then

$$u_0 = u_h, \quad u_1 = u_{h+1},$$

$$u_c = u_{h+d}, \quad u_{1+c} = u_{h+1+d},$$

whence $h = 0$ and so $c = d$, contrary to supposition. Thus the sequences $(u_k + \xi u_{k+c})_{k \in \mathbb{N}_0}$ and $(u_k + \xi u_{k+d})_{k \in \mathbb{N}_0}$ are distinct in the strong sense that there is no translation of one that can make it coincide with the other from some point onwards.

The unit f-sequence $(u_n)_{n \in \mathbb{N}_0}$ has least period $q^2 - 1$; in the initial segment $(u_n)_{0 \leqslant n \leqslant q^2-2}$, each possible ordered pair $(v, w) \neq (0, 0)$, where $v, w \in \mathbb{F}_q$, must appear exactly once as consecutive elements (where we regard (u_{q^2-2}, u_0) as being consecutive) because there are $q^2 - 1$ such pairs, each of which determines the sequence. Thus, in the initial segment, each pair $(0, w)$ for $w \in \mathbb{F}_q^*$ appears exactly once, and so the element 0 appears exactly $q - 1$ times. But $u_n = 0$ if and only if $\alpha(f) \mid n$. Thus there are exactly $q - 1$ integers e with $0 \leqslant e \leqslant q^2 - 2$ such that $e \equiv 0 \pmod{\alpha(f)}$. By what we saw above, this means that there are $q^2 - q$ sequences $(u_k + \xi u_{k+c})_{k \in \mathbb{N}_0}$ where $c \not\equiv 0 \pmod{\alpha(f)}$, distinct in the above strong sense, which represent M. But $q \geqslant 3$ and so $q^2 - q > 2$, whence M is nonstandard. □

In the situation of the above result, there are $q^2 - q - 2$ nonroot choices of μ_1 (in our usual notation) which yield M.

3. The main theorem

The content of our main theorem is that, for irreducible polynomials over fields of prime order, the nonstandard cases of the previous section are the only ones.

Theorem 3.1. *Let $\mathbb{F}$ be a field of prime order, p, and let $f(t) \in \mathbb{F}_0[t]$ be irreducible. Suppose that M is an f-subgroup with $|M| > 4$. Then M is standard if and only if both $|M| \neq p^2 - 1$ and $|M|$ does not divide $2(p-1)$.*

Proof. Write $|M| = m$. Then $m = \operatorname{ord}(f)$ by [4, 8.28], while $m \nmid (p-1)$ because f is irreducible.

Write $\mathbb{L}$ for the splitting field of f. Since $M \leqslant \mathbb{L}^*$ then $m \mid (p^2-1)$ and so $m = (c/d)(p-1)$ where $c, d \in \mathbb{N}$, $c \mid (p+1)$, $d \mid (p-1)$ and $\gcd(c,d) = 1$, while $c > 1$ because $m \nmid p-1$. As $m > 4$ then $p > 2$.

Let ξ, $\xi^p \in \mathbb{L}$ be the roots of f. Then $|\xi| = |\xi^p| = m$ and $M = \langle \xi \rangle$. By [4, 8.21] there exist $\alpha, \beta \in \mathbb{L}$ (not both zero) such that

$$M = \{\alpha\xi^i + \beta(\xi^p)^i,\ 0 \leqslant i \leqslant m-1\}.$$

To prove that M is standard, it will suffice to prove that one of α, β must be zero; thus assume for a contradiction that $\alpha\beta \neq 0$ and write $\gamma = -\beta/\alpha$. Now

$$M = \{\alpha\xi^i + \beta(\xi^i)^p,\ 0 \leqslant i \leqslant m-1\} = \{\alpha\mu + \beta\mu^p,\ \mu \in M\},$$

whence $g(t) := \alpha t + \beta t^p$ permutes the elements of M.

By Theorem 1.8, $(g(t))^b \pmod{(t^m-1)}$ has constant term zero if $b \not\equiv 0 \pmod{m}$ and then the constant term of $(h(t))^b \pmod{(t^m-1)}$ is zero for these b, where $h(t) = g(t)/\alpha = t - \gamma t^p$.

Suppose now that $m \nmid 2(p-1)$ and that $c < p+1$. Then

$$(h(t))^b \pmod{(t^m-1)} \text{ has constant term zero if } b \in \{p-1, 2(p-1)\}. \tag{3}$$

We have

$$(h(t))^{p-1} = (t - \gamma t^p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (-\gamma)^i t^{(i+1)(p-1)}.$$

But

$$\binom{p-1}{i} = \frac{(p-1)(p-2)\cdots(p-i)}{1 \times 2 \times \cdots \times i} \equiv (-1)^i \pmod{p}.$$

Thus

$$(h(t))^{p-1} = \left(\sum_{i=0}^{p} \gamma^i t^{(i+1)(p-1)}\right) - \gamma^p t^{(p^2-1)}.$$

Because $c \mid (p+1)$ the summation may be rewritten as a double sum, over a rectangular array of size $c \times (p+1)/c$:

$$(h(t))^{p-1} = \sum_{j=0}^{c-1} \left(\sum_{i=0}^{\frac{p+1}{c}-1} \gamma^{ci+j} t^{ci(p-1)} \right) t^{(j+1)(p-1)} - \gamma^p t^{(p^2-1)}.$$

Now $m = (c/d)(p-1)$ where $\gcd(c,d) = 1$, so if $k \in \mathbb{N}$ then $m \mid k(p-1)$ if and only if $c(p-1) \mid kd(p-1)$. Thus

$$m \mid k(p-1) \quad \text{if and only if} \quad c \mid k. \tag{4}$$

Thus, $t^{ci(p-1)} \equiv t^0 \pmod{(t^m - 1)}$ for all i, while $t^{p^2-1} \equiv t^0 \pmod{(t^m-1)}$ because $m \mid (p^2-1)$. Thus,

$$(h(t))^{p-1} \equiv \sum_{j=0}^{c-1} \left(\sum_{i=0}^{\frac{p+1}{c}-1} \gamma^{ci} \right) \gamma^j t^{(j+1)(p-1)} - \gamma^p \pmod{(t^m-1)}.$$

For j in the range of summation, $t^{(j+1)(p-1)} \equiv t^0$ precisely when $j = c-1$. Thus the constant term of $(h(t))^{p-1} \pmod{(t^m-1)}$ is

$$\left(\sum_{i=0}^{\frac{p+1}{c}-1} \gamma^{ci} \right) \gamma^{c-1} - \gamma^p,$$

and by (3) this must be zero. Since $\gamma \neq 0$, this yields

$$\sum_{i=0}^{\frac{p+1}{c}-1} \gamma^{ci} = \gamma^{p-c+1},$$

and so

$$(h(t))^{p-1} \equiv \gamma^{p-c+1} \sum_{j=0}^{c-2} \gamma^j t^{(j+1)(p-1)} \pmod{(t^m-1)}.$$

Note that the term with $j = c-1$ cancels with γ^p. Thus

$$(h(t))^{2(p-1)} \equiv \gamma^{2(p-c+1)} \left(\sum_{j=0}^{c-2} \sum_{i=0}^{c-2} \gamma^{i+j} t^{(i+j+2)(p-1)} \right) \pmod{(t^m-1)}.$$

In the double sum, there are contributions to the constant term precisely when $c \mid (i+j+2)$, because of (4). The summations extend from 0 to $c-2$, so there are just $c-1$ such contributions, corresponding to the pairs

$$(j = 0, i = c-2), \ldots, (j = c-2, i = 0).$$

It follows that the constant term of $(h(t))^{2(p-1)} \pmod{(t^m-1)}$ is $\gamma^{2p-c}(c-1)$, and, again by (3), this must be zero. But $\gamma \neq 0$, and so $c-1 = 0$ as an element of $\mathbb{L}$; this is impossible as $1 < c < p+1$. This contradiction proves that M is standard in this case.

Next assume that $c = p+1$.

If $d = 1$ then $m = p^2 - 1$ and M is nonstandard by Proposition 2.4.

Suppose $d > 1$. Now $m = v(p+1)$ where $v = \frac{p-1}{d}$; in particular, $2v \not\equiv 0 \pmod{m}$. We have

$$(h(t))^{2v} = (t - \gamma t^p)^{2v} = \sum_{j=0}^{2v} \binom{2v}{j} (-\gamma)^j t^{2v+j(p-1)}.$$

If $j = v$ then $2v + j(p-1) = v(p+1) = m$. On the other hand, if $2v + j(p-1) \equiv 2v + k(p-1) \pmod{m}$ then $j \equiv k \ (\mathrm{mod}\ (m/\gcd(m, p-1)))$. Now

$$\gcd(m, (p-1)) \in \{v, 2v\}$$

because $\gcd(p-1, p+1) = 2$ and so

$$m/\gcd(m, p-1) \geqslant v(p+1)/2v = (p+1)/2 > v.$$

Thus for $j \in \{0, \ldots, 2v\}$ we have $2v + j(p-1) \equiv 0 \pmod{m}$ if and only if $j = v$, and so the constant term of $(h(t))^{2v} \ (\mathrm{mod}\ (t^m - 1))$ is $\binom{2v}{v}(-\gamma)^v$. But this constant term is zero, which is absurd because $\gamma \neq 0$ by choice and $\binom{2v}{v} \neq 0$ because $2v < p$. Thus M is standard in this case.

Finally, suppose $m \mid 2(p-1)$. Then $|\xi| \mid 2(p-1)$, $(\xi^{p-1})^2 = 1$ and $\xi^{p-1} = \pm 1$. If $\xi^{p-1} = 1$ then $\xi \in \mathbb{F}_p^*$, which is false. Thus $\xi^p = -\xi$ and $\sigma = \xi^p + \xi = 0$. Now $|\xi| = |-\xi|$ and so by Lemma 2.2, $|\rho|$ is even. By Proposition 2.3, M is nonstandard. □

The main theorem was proved for irreducible polynomials over fields of prime order. We are tempted by numerical evidence to conjecture that some similar result should be true over arbitrary finite fields.

Acknowledgments

We thank the anonymous referees for their very helpful suggestions.

References

[1] O.J. Brison, Complete Fibonacci sequences in finite fields, Fibonacci Quart. 30 (1992) 295–304.

[2] O.J. Brison, On group-permutation polynomials, Portugaliae Math. 50 (1993) 365–383.

[3] P. Bundschuh, Jau-Shyong Shiue, A generalization of a paper by D.D. Wall, Atti della Accademia Nazionale dei Lincei, Rendiconti—Classe di Scienze Fisiche, Mat. Nat. 56 (1974) 135–144.

[4] R. Lidl, H. Niederreiter, Finite Fields, 2nd Edition, Cambridge University Press, Cambridge, 1997.

[5] L.E. Somer, The Fibonacci group and a new proof that $\mathrm{F}_{p-(5/p)} \equiv 0 \pmod{p}$, Fibonacci Quart. 10 (1972) 345–348, 354.

[6] L.E. Somer, Fibonacci-like groups and periods of Fibonacci-like sequences, Fibonacci Quart. 15 (1977) 35–41.