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*

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 $k \geq 2$ are described. Here we exhibit two infinite families of standard groups for $k \geq 2$.

Key words: linear recurrence relation, finite field, standard subgroup, restricted period
1991 MSC: 11B39, 12E20

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.

1.1 Definition. Let

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

⋆ 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.
Email addresses: ojbrison@fc.ul.pt (Owen J. Brison), jen@fct.unl.pt (J. Eurico Nogueira).

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 $M \leq \mathbb{L}^*$, 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

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

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 $\delta(f) \geq k$.

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

1.2 Lemma. *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 $< \lambda > \leq \mathbb{A}^*$ 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 $M =< \lambda >$ and $f(\lambda) = 0$.
(c) Suppose $M \leq \mathbb{A}_q^*$ is finite. Suppose $M =< \lambda >$ 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 $\{1, \lambda, \cdots\}$ exhibits $M =< \lambda >$ 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 $< \omega > \leq \mathbb{A}_q^*$ may be regarded as (the underlying set of) an f-sequence of minimal period $|\omega|$:

$$< \omega >= (\cdots, 1, \omega, \omega^2, \cdots, \omega^{|\omega|-1}, \cdots).$$

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

1.3 Definition. Let $f(t) \in \mathbb{F}_q[t]$ be monic of degree k with $f(0) \neq 0$, and let M be an f-subgroup. Then M is said to be *non-standard* (as an f-subgroup) if M admits a representation as a non-cyclic f-sequence, while M is said to be *standard* (as an f-subgroup) if all f-sequences that represent M are cyclic.

The authors studied this concept when $f(t)$ has degree 2, in [2], [3] and [4], while Hollmann [7] (using a result from [4]) classified standard and non-standard subgroups when $f(t)$ is irreducible of degree 2.
In [5] the authors exhibited certain configurations that give rise to non-standard groups when $f(t)$ has degree $k \geq 2$.
In this paper the authors investigate two general configurations that give rise to standard groups when $k \geq 2$. The first configuration is when $f(t)$ has just one (repeated) root, and is studied in Section 2 (eee Theorem 2.3). The second is when the order of the group in question is of a very special kind, and is studied in Section 3 (see Theorem 3.4). In each case the results are proved under very restrictive upper bounds on k in terms of the prime p; however, for a given k we obtain standard groups over $\mathbb{F}_p$ for all primes $p > k$. It is worth pointing out that the standard groups obtained in these two theorems (or closely related groups: see Example 3.7 below) are the only ones we know to be standard for $k > 2$ apart from a few examples when $k \in \{3, 4\}$.
The first configuration is when $f(t)$ has just one (repeated) root and is studied in Section 2; the second configuration is when the order of the group in question is of a very special kind, and is studied in Section 3.
Note that Corollary 3.2 of [7] draws a strong connection between an f-subgroup being standard, or not, and the automorphisms of certain cyclic codes.

2 Polynomials with just one root

In this section we study f-sequences over a finite field of characteristic p where $f(t)$ is a polynomial of degree $k \leq p$ which admits just one root (of multiplicity

k). Our main result here, Theorem 2.3, guarantees that in this situation an f-subgroup is standard; the special case when $k = 2$ was proved as Proposition 1.7 of [2]. The restriction that $k \leq p$ is severe but we have been unable either to remove it or to show it is necessary.
We start by computing the restricted period in Proposition 2.1. This is not needed in the proof of Theorem 2.3, but it is simple and, given the part played by this concept in [2], [3], [4] and [5], we think it is of interest.

2.1 Proposition. *Let p be a prime and k, n be natural numbers with $2 \leq k \leq p$. Write $q = p^n$. Let $r \in \mathbb{F}_q^*$ and $f(t) = (t - r)^k \in \mathbb{F}_q[t]$. Then the restricted period of f is p.*

Proof. Let $\mathcal{U} = (u_i)$ denote the unit f-sequence. Then $u_j = 0$ for $0 \leq j \leq k-2$ while $u_{k-1} = 1$. By 8.23 of [8], which is applicable because $k \leq p$, there exists $P(t) \in \mathbb{F}_q[t]$, of degree at most $k - 1$, such that $u_i = P(i)r^i$ for all $i \in \mathbb{Z}$; as usual, i is considered as an element of $\mathbb{F}_p$ when $P(i)$ is to be evaluated. Because $r \neq 0$, then $P(j) = 0$ for $0 \leq j \leq k - 2$. But j and $j + p$ represent the same element in $\mathbb{F}_q$ and so $u_{j+p} = P(j + p)r^{j+p} = 0$ for $0 \leq j \leq k - 2$. It follows that the restricted period, $\delta(f)$, of f must divide p. But $\delta(f) \geq k$ when $f(t)$ has degree $k \geq 2$. Thus $\delta(f) = p$. □

2.2 Lemma. *Let p be a prime and k, n be natural numbers with $k \leq p$. Write $q = p^n$. Let $r \in \mathbb{F}_q^*$ and write $f(t) = (t - r)^k \in \mathbb{F}_q[t]$. Suppose that M is an f-subgroup. Then $r \in M$.*

Proof. By definition, there exists a finite extension $\mathbb{L}$ of $\mathbb{F}_q$ with $\mathbb{L} \subseteq \mathbb{A}_q*$ such that $M \leq \mathbb{L}^*$.
Let $(s_i)_{i\in\mathbb{Z}}$ be an f-sequence which represents M and write $|M| = m$. Again by 8.23 of [8], there exists $P(t) \in \mathbb{L}[t]$, of degree $h \leq k - 1$, such that $s_i = P(i)r^i$ for all $i \in \mathbb{Z}$. Write a_h for the leading coefficient of $P(t)$ (so that $a_h \neq 0$).
Fix $i \in \mathbb{Z}$ with $0 \leq i \leq p - 1$. Because M has order m then $s_i = s_{i+m}$ and so $P(i)r^i = P(i + m)r^{i+m}$; thus $P(i) = P(i + m)r^m$ because $r \neq 0$. Write $D(t) = P(t) - r^m P(t + m)$. Then $D(t)$ is a polynomial of degree at most $h < p$ (the hypothesis $k \leq p$ is again used here) which admits every element of $\mathbb{F}_p$ as a root, so that $D(t) = 0$. The coefficient of t^h in $D(t)$ is $a_h - r^m a_h$. Thus $a_h - r^m a_h = 0$, and because $a_h \neq 0$ it follows that $r^m = 1$. Thus $r \in M$. □

We now prove the main result of this section.

Theorem 2.3. *Write $q = p^n$ where p is a prime and $n \in \mathbb{N}$. Let $k \in \mathbb{N}$ with $2 \leq k \leq p$. Suppose that $f(t) = (t - r)^k \in \mathbb{F}_q[t]$ where $r \in \mathbb{F}_q^*$, and let M be an f-subgroup. Then M is standard as an f-subgroup, $|M| = |r|$ and $M \leq \mathbb{F}_q^*$.*

Proof. Write $m = |M|$. Note that $M \leq \mathbb{L}^*$ for suitable $\mathbb{L}$ as above and so $m \in \mathbb{N}$ is coprime with p; we may thus, when convenient, view m as an element

of $\mathbb{F}_p^*$. By hypothesis,

$$M = \{s_0, s_1, \ldots, s_{m-1}\}$$

where $(s_i)_{i\in\mathbb{Z}}$ is an f-sequence. Without loss, suppose that $s_0 = 1$.
Again by 8.23 of [8], there exists $P(t) \in \mathbb{L}[t]$, of degree at most $k-1$, such that $s_i = P(i)r^i$ for all $i \in \mathbb{Z}$. We have $1 = s_0 = P(0)r^0 = P(0)$ and so 0 is a root of the polynomial $D(t) = P(t) - 1$.
Because M is an f-subgroup of order m then $1 = s_0 = s_{jm}$ for all $j \in \mathbb{Z}$, so that $1 = P(jm)r^{jm}$ for all $j \in \mathbb{Z}$. But $r \in M$ by the previous lemma, and so $r^{jm} = 1$. Thus, jm is a root of $D(t)$ for all $j \in \mathbb{Z}$. Thus, $\{jm : 1 \le j \le k-1\}$ is a set of roots of $D(t)$. Because $m \in \mathbb{F}_p^*$ and $k-1 < p$, this set contains $k-1$ distinct, non-zero, elements. But also $D(0) = 0$ and so $D(t)$, of degree at most $k-1$, has k roots. Thus $D(t) = 0$ and so $P(t) = 1$. It follows that $s_i = r^i$ for all $i \in \mathbb{Z}$ and so M is standard; this also guarantees that $|M| = |r|$ and then that $M \le \mathbb{F}_q^*$ because $r \in \mathbb{F}_q^*$. □

3 Irreducible polynomials of order $m = a\left(\frac{q^k-1}{q-1}\right)$

We will need the following result whose proof may be found in 3.3 of [1]; a sketch proof appears in 1.8 of [2]. Firstly, some terminology: if $f(t) \in \mathbb{F}[t]$ is a polynomial and if $m \in \mathbb{N}$, by "the reduction of $f(t)(\mathrm{mod}\, t^m - 1)$" we will understand the unique polynomial $\overline{f(t)} \in \mathbb{F}[t]$ of degree at most $m-1$ such that $\overline{f(t)} \equiv f(t)(\mathrm{mod}\, t^m - 1)$.

Theorem 3.1. *Let $\mathbb{K}$ be a field. Suppose that $G \le \mathbb{K}^*$, with $|G| = m \in \mathbb{N}$, and that $p(t) \in \mathbb{K}[t]$ permutes the elements of G. If $b \in \mathbb{N}$ then the constant term of the reduction of $p(t)^b (\mathrm{mod}\, t^m - 1)$ is 0 if $b \not\equiv 0 \,(\mathrm{mod}\ m)$ and is 1 if $b \equiv 0 \,(\mathrm{mod} m)$.*

A polynomial $p(t) \in \mathbb{K}[t]$ that permutes the elements of $G \le \mathbb{K}^*$ will be called a *group permutation polynomial* of G. For the rest of this paper, indices (for example in the expression n_{j+h}) are understood to be taken $(\mathrm{mod}\, k)$ unless specifically stated otherwise.

Lemma 3.2. *Let p be a prime and q be a power of p. Let a, k be positive integers with $a \mid q-1$ and $n_0, \cdots, n_{k-1}$ be non-negative integers. Write $m = a\left(\frac{q^k-1}{q-1}\right)$. Suppose that*

$$\sum_{j=0}^{k-1} n_j q^j \equiv 0 \,(\mathrm{mod}\, m).$$

If $h \in \mathbb{Z}$ then

$$\sum_{j=0}^{k-1} n_{j+h}\, q^j \equiv 0 \,(\mathrm{mod}\, m);$$

that is, the first congruence remains valid after cyclic permutations of the n_j relative to the q^j.

Proof. Because $m = a\left(\frac{q^k-1}{q-1}\right)$ with $a \mid q-1$ then $q^k - 1 \equiv 0 \,(\mathrm{mod}\, m)$; so if $\sum_{j=0}^{k-1} n_j q^j \equiv 0 \,(\mathrm{mod}\, m)$, then we have

$$0 \equiv q \sum_{j=0}^{k-1} n_j q^j = \sum_{j=0}^{k-1} n_{j-1} q^j + (1-q^j) n_{k-1} \equiv \sum_{j=0}^{k-1} n_{j-1} q^j \,(\mathrm{mod}\, m),$$

This proves the result for $h = -1$. The general case follows by induction: we need only consider those values of h whose residue (mod k) lies between 0 and $k-1$. □

Lemma 3.3. (Lucas' theorem for the multinomial formula). *For integers $d \geq 0, t \geq 1$ and $m_0, \cdots, m_t \geq 0$, write*

$$m_0 = c_0 + c_1 p + \cdots + c_d p^d, \quad 0 \leq c_i \leq p-1, \quad i < d$$
$$m_j = c_{0,j} + c_{1,j} p + \cdots + c_{d,j} p^d, \quad 0 \leq c_{i,j} \leq p-1, \quad i < d, 1 \leq j \leq t$$

where $c_d, c_{d,j} \geq 0$. Then

$$\binom{m_0}{m_1, \cdots, m_t} \equiv \binom{c_0}{c_{0,1}, \cdots, c_{0,t}} \times \ldots \times \binom{c_d}{c_{d,1}, \cdots, c_{d,t}} (\mathrm{mod} p).$$

Proof. See congruence C2, of [6]. □

The proof of Theorem 3.4, that certain f-sequence subgroups, M, of degree $k \geq 2$ are standard, is based on the method used (for $k = 2$) in the papers [2], [3] and [4], and is divided into a number of steps, which we now outline for the convenience of the reader.

In Step 1 we exhibit a group permutation polynomial, $g(t)$, of M; $g(t)$ turns out to be a linearized polynomial as defined in 3.49 of [8]. The coefficients of g will depend on elements $\alpha_1, \cdots, \alpha_k$ in the splitting field of f which arise when an f-sequence underlying M is written, via the Binet formula, in terms of the roots of f. The exponents of t that arise in $g(t)$ are powers of q. The aim is to show that all but one of the elements α_i must be zero, so that M may be written as an f-sequence in essentially only one way.

Theorem 3.1 guarantees that, for certain powers b, the constant term of $g(t)^b (\mathrm{mod}(t^{|M|} - 1))$ must be zero; this then gives equations which involve the α_i. Our technique is to carefully choose relevant powers b so as to give equations in the α_i that can be solved to conclude that all but one of them must be zero. The present situation, where $k \geq 2$, is more complicated than when $k = 2$ because the powers $g(t)^b$ are calculated by the multinomial formula. The exponents of t that arise are linear combinations of the form $\sum_i n_i q^i$.

In Step 2 we define $\mathcal{S}$ to be the set of indices $i \in \mathcal{K} = \{0, \cdots, k-1\}$ such that $\alpha_i \neq 0$ and we write $|\mathcal{S}| = s$; in these terms, our aim is to prove that $s = 1$.
In Step 3 we take $b = ak$ and prove that at least one of the α_i must be zero; this means that $\mathcal{S} \neq \mathcal{K}$.
In Step 4 we take $b = N$ where N depends not only on the value of s but also on a certain supposition as to which of the α_i are zero and which are not. Ignoring the terms with zero coefficient (i.e., $\alpha_i = 0$) in the permutation polynomial $g(t)$, we raise $g(t)$, now with s terms, to the power N. We need to calculate the constant term of $g(t)^N (\mathrm{mod}(t^{|M|} - 1))$ (see Step 5). The exponents of t in $g(t)^N$ are of the form $e = n_{i_0} q^{i_0} + \cdots + n_{i_{s-1}} q^{i_{s-1}}$ where the n_{i_j} sum to N. Demanding that such an exponent be a multiple of $|M|$ imposes strong conditions on the n_{i_j}. It turns out that cyclic permutations of the n_{i_j} in the expression for e send e to another exponent of t in $g(t)^N$, which is also a multiple of $|M|$ (see Step 6). We choose a permutation that enables us to find an exponent which is most suitable for the purpose of calculating the n_{i_j}. Eventually, the n_{i_j} are uniquely determined in Steps 7 and 8 under the supposition that $s > 1$. After reversing the above permutation in Step 9, we are left with a unique monomial as the constant term of $g(t)^N (\mathrm{mod}(t^{|M|} - 1))$. This constant term is a product of a non-zero scalar with powers of the α_{i_j}; these α_{i_j} are supposed to be non-zero because the i_j belong to $\mathcal{S}$. But, by Theorem 3.1, this coefficient must be zero. This, still under the supposition that $s > 1$, is a contradiction. We finally conclude that $s = 1$ and that M is standard.

The hypothesis $ak < p$ in Theorem 3.4 is very restrictive. To illustrate the scope of this result, fix $k \geq 2$, let p be a prime with $p > k$, let $n \in \mathbb{N}$ and write $q = p^n$. Suppose $a \in \mathbb{N}$ is such that $a \mid q-1$ and $ak < p$; certainly $a = 1$ satisfies these conditions. Then $\mathbb{F}_{q^k}^*$ contains an element α of order $a\left(\frac{q^k-1}{q-1}\right)$. It is not hard to check that $\mathbb{F}_{q^k} = \mathbb{F}_q(\alpha)$ and that the minimum polynomial, $f(t)$, of α over $\mathbb{F}_q$ has degree k; the theorem guarantees that $< \alpha >$ is standard as an f-subgroup.

Theorem 3.4. *Let p be an odd prime and q be a power of p. Let $f(t) \in \mathbb{F}_q[t]$ be irreducible of degree $k \geq 2$, $\mathbb{F}$ be its splitting field over $\mathbb{F}_q$ and $M \leq \mathbb{F}^*$ be an f-subgroup of order m. Suppose that $m = a(\frac{q^k-1}{q-1})$ where $a \in \mathbb{N}$ is such that $a \mid (q-1)$ and $ak < p$. Then M is standard as an f-subgroup.*

Proof. Because an f-group of order $q^k - 1$ is non-standard, for p an odd prime (see Theorem 4.3 of [5]), we start by confirming that the hypotheses imply that $a < q - 1$. Because p is an odd prime then $q > 2$ and so $\frac{q}{2} < q - 1$. Thus

$$a < \frac{p}{k} \leq \frac{q}{2} < q - 1,$$

as claimed. The proof is divided into a number of distinct steps.

Step 1: The permutation polynomial. Here we exhibit a group permutation

polynomial, $g(t)$, of M. This will enable us to apply Theorem 3.1 at various stages in the proof.
Because $f(t)$ is irreducible of degree k over $\mathbb{F}_q$, it admits k distinct roots in $\mathbb{F}$, which may be written in the form

$$\omega, \omega^q, \omega^{q^2}, \cdots, \omega^{q^{k-1}} \in \mathbb{F}^*.$$

Further, Theorems 8.28 and 3.3 of [8] guarantee that $m = \mathrm{ord}(f) = |\omega|$ and so $M =< \omega >$. Suppose that $(\mu_i)_{i=0}^{m-1}$ is a representation of M as an f-sequence. By 8.21 of [8] there exist $\alpha_0, \cdots, \alpha_{k-1} \in \mathbb{F}$ such that

$$\mu_i = \sum_{j=0}^{k-1} \alpha_j \, (\omega^i)^{q^j}$$

for all $i \in \mathbb{Z}$. Write $\mathcal{K} := \{0, \cdots, k-1\}$ and

$$g(t) := \sum_{j \in \mathcal{K}} \alpha_j \, t^{q^j} \in \mathbb{F}[t].$$

The reasoning in the proof of Proposition 2.2 of [3] may be extended to the case where $f(t)$ has general degree k to show that $g(t)$ is a group permutation polynomial of M. Without loss of generality, we may suppose notation chosen so that

$$1 = \mu_0 = \sum_{j=0}^{k-1} \alpha_j = g(1);$$

in particular not all of the α_j can be zero.

Step 2: The set $\mathcal{S}$.

Let $\mathcal{S} \subseteq \mathcal{K}$ be such that $i \in \mathcal{S}$ if and only if $\alpha_i \neq 0$, where the α_j are as defined in Step 1. We will write $|\mathcal{S}| = s$ and $\mathcal{S} = \{i_0, \cdots, i_{s-1}\}$ where $0 \leq i_0 < i_1 < \cdots < i_{s-1} \leq k-1$; then $s \geq 1$ because the α_j are not all zero. Our aim is to show $s = 1$, which will imply that M is standard.

Step 3: Proof that $s < k$.

We have

$$g(t)^{ak} = \sum \frac{(ak)!}{n_0! \ldots n_{k-1}!} \, \alpha_0^{n_0} \cdots \alpha_{k-1}^{n_{k-1}} \, t^{n_0 + n_1 q + \cdots + n_{k-1} q^{k-1}},$$

where the sum is taken over all k-tuples $(n_0, \cdots, n_{k-1})$ of non-negative integers n_j such that $n_0 + \cdots + n_{k-1} = ak$. Note that the multinomial coefficients here are evaluated as natural numbers and then reduced $(\mathrm{mod}\, p)$. Because $m = a(1 + q + \cdots + q^{k-1})$, the constant term of $g(t)^{ak} (\mathrm{mod}\ t^m - 1)$ is the sum

of those terms for which the power of t is a multiple of m; that is, for which there exist non-negative integers $Q = Q(n_0, \cdots, n_{k-1})$ such that

$$n_0 + n_1 q + \cdots + n_{k-1} q^{k-1} = Qa(1 + q + \cdots + q^{k-1}). \tag{1}$$

Because the n_i are non-negative with $n_{k-1} + \cdots + n_0 = ak > 0$ then $Q > 0$. By hypothesis $ak < p$ and so $0 \leq n_0, \cdots, n_{k-1} < p \leq q$ and also $0 < a < p \leq q$. By (1) we have $Qa \equiv n_0 (\bmod q)$. Because $n_i < q$ for $i = 0, \cdots, k-1$, then

$$n_0 + n_1 q + \cdots + n_{k-1} q^{k-1} < q(1 + q + \cdots + q^{k-1}).$$

Thus $Qa < q$ and so $Qa = n_0 < q$. But now both sides of (1) represent the base-q expansion of the same number and then $n_i = Qa$ for $i = 0, \cdots, k-1$, by the uniqueness of that expansion. Thus we have

$$n_0 + \cdots + n_{k-1} = k(Qa).$$

By hypothesis, $n_0 + \cdots + n_{k-1} = ak$ and so $Q = 1$. But now $n_0 = \cdots = n_{k-1} = a$ and so the constant term of $g(t)^{ak}$ is given by

$$\frac{(ak)!}{a! \ldots a!} \alpha_0^a \cdots \alpha_{k-1}^a.$$

Because $p > ak$, the term $\dfrac{(ak)!}{a! \ldots a!}$ is non-zero as an element of $\mathbb{F}_q$. But, because $k \geq 2$,

$$m = a\frac{q^k - 1}{q - 1} = a \sum_{j=0}^{k-1} q^j > a \sum_{j=0}^{k-1} 1^j = ak$$

and so $ak < m$. Thus by Theorem 3.1 this constant term must be zero and so

$$\alpha_0^a \cdots \alpha_{k-1}^a = 0.$$

Thus $\alpha_j = 0$ for at least one j with $0 \leq j \leq k-1$ and so $\mathcal{S} \neq \mathcal{K}$ and $s < k$.

Step 4: The definition of N.

Because $\alpha_j = 0$ if $j \in \mathcal{K} \backslash \mathcal{S}$ then

$$g(t) = \sum_{j \in \mathcal{S}} \alpha_j \, t^{q^j}, \tag{2}$$

where $g(t)$ is as in Step 1 and $\mathcal{S} = \{i_0, \cdots, i_{s-1}\}$ is as in Step 2. If $n \in \mathbb{N}$ then, by Theorem 3.1, the constant term of $g(t)^n \, (\bmod t^m - 1)$ must be zero (as an

element of $\mathbb{F}$) whenever $n \not\equiv 0 \,(\mathrm{mod}\, m)$. The multinomial formula, applied to (2), gives

$$g(t)^n = \sum \frac{n!}{n_{i_0}! \ldots n_{i_{s-1}}!} \alpha_{i_0}^{n_{i_0}} \cdots \alpha_{i_{s-1}}^{n_{i_{s-1}}} t^{n_{i_0} q^{i_0} + \cdots + n_{i_{s-1}} q^{i_{s-1}}} \tag{3}$$

where the sum is taken over all s-tuples $(n_{i_0}, \cdots, n_{i_{s-1}})$ of non-negative integers n_i such that $\sum_{i_j \in \mathcal{S}} n_{i_j} = n$. Again, the multinomial coefficients are evaluated as natural numbers and then reduced $(\mathrm{mod}\, p)$.
The monomials in the right-hand side of (3) which contribute to the constant term of $g(t)^n (\mathrm{mod}\, t^m - 1)$ are exactly those such that

$$m \mid n_{i_0} q^{i_0} + \cdots + n_{i_{s-1}} q^{i_{s-1}}.$$

Recall that we wish to prove $s = 1$. If $s > 1$, define $\theta : \{0, \cdots, s-1\} \mapsto \mathcal{K}$ by

$$\theta(j) = \begin{cases} i_{j+1} - i_j - 1, 0 \leq j \leq s-2 \\ k - 1 - i_{s-1} + i_0, j = s-1. \end{cases}$$

The function θ is non-negative and measures the number of indices $i \in \mathcal{K}$ strictly between i_j and i_{j+1}, where for these purposes i_s is identified with i_0. Note that $\theta(j) = 0$ if and only if $i_{j+1} = i_j + 1$. For completeness, when $s = 1$ we define $\theta(0) = k - 1$. Write

$$N = a \sum_{j=0}^{s-1} (1 + q + \cdots + q^{\theta(j)}) = a \sum_{j=0}^{s-1} \sum_{b=0}^{\theta(j)} q^b \in \mathbb{N}.$$

Note that $N > 0$, that N depends on the set $\mathcal{S}$ and that $N \equiv as \,(\mathrm{mod}\, p)$. Now $s < k$ so $as < ak < p$, the final inequality by hypothesis. Thus $0 < as < p$ and so $N \not\equiv 0 \,(\mathrm{mod}\, p)$.
For each i_j $(0 \leq j \leq s-1)$ write

$$\mathcal{B}_j = \{i_j, i_j + 1, \cdots, i_j + \theta(j)\} \subseteq \mathcal{K},$$

where we are reducing the elements of $\mathcal{B}_j$ $(\mathrm{mod}\, k)$. Thus $\mathcal{B}_j$ starts with the index i_j, for which $\alpha_{i_j} \neq 0$, and contains those indices l such that $i_j \leq l < i_{j+1}$ for which $\alpha_l = 0$. The next index l for which $\alpha_l \neq 0$ is $l = i_{j+1}$, and this index is the starting point of $\mathcal{B}_{j+1}$. Thus the sequence $(0, 1, \cdots, k-1)$ is the disjoint union of the blocks $\mathcal{B}_0, \cdots, \mathcal{B}_{s-1}$. Note that when $s = 1$ we have just the block $\mathcal{B}_0 = \{0, \cdots, k-1\}$.

Step 5: A specific constant term.

We study the constant term of $g(t)^N (\mathrm{mod}\, t^m - 1)$ where N is as above. By

(3) we have

$$g(t)^N = \sum \frac{N!}{n_{i_0}! \dots n_{i_{s-1}}!} \alpha_{i_0}^{n_{i_0}} \cdots \alpha_{i_{s-1}}^{n_{i_{s-1}}} t^{n_{i_0} q^{i_0} + \cdots + n_{i_{s-1}} q^{i_{s-1}}} \tag{4}$$

where, as usual, the multinomial coefficients are reduced $(\mathrm{mod}\, p)$ and where the sum is taken over all s-tuples $(n_{i_0}, \cdots, n_{i_{s-1}})$ of non-negative integers n_{i_j} with $i_j \in \mathcal{S}$ such that

$$\sum_{j=0}^{s-1} n_{i_j} = N. \tag{5}$$

The constant term of $g(t)^N (\mathrm{\ mod\ } t^m - 1)$ arises from the sum of all those monomials in (4) (and thus subject to (5)) such that

$$\sum_{i \in \mathcal{S}} n_i q^i = \sum_{j=0}^{s-1} n_{i_j} q^{i_j} \equiv 0 \,(\mathrm{mod}\, m). \tag{6}$$

Step 6: Cyclic permutation of the n_{i_j}.

We assume for the rest of the proof that the non-negative integers n_i for $i \in \mathcal{S}$ satisfy conditions (5) and (6). Define $n_i = 0$ if $i \in \mathcal{K} \backslash \mathcal{S}$, and recall our convention that indices in expressions such as n_{i+h} are taken $(\mathrm{mod}\, k)$. Note that n_i could be zero for some $i \in \mathcal{S}$; this means that the maximum value, θ_0, of θ is less than or equal to the greatest distance between two consecutive non-zero n_i. Condition (6) now becomes

$$\sum_{i \in \mathcal{S}} n_i q^i = \sum_{i \in \mathcal{K}} n_i q^i \equiv 0 \,(\mathrm{mod}\, m) \tag{7}$$

If $h \in \mathbb{Z}$ (with $0 \leq h \leq k-1$), Lemma 3.2 gives

$$\sum_{i \in \mathcal{K}} n_{i+h}\, q^i \equiv 0 \,(\mathrm{mod}\, m). \tag{8}$$

This corresponds to a cyclic permutation, π_h, of the n_i relative to the q^i.
We may now choose, and fix, h in (8) so that the coefficient, n_h, of q^0 in this sum is non-zero, while the maximum possible number of consecutive coefficients of the form $n_{k-v+h}, \cdots, n_{k-1+h}$ of $q^{k-v}, \cdots, q^{k-1}$, respectively, are all zero: this defines the integer v which then coincides with the maximum number of cyclically-consecutive n_j which can possibly be 0. Because the coefficient of q^0 is non-zero then $v \leq k-1$, while from the second sentence of this step we have $\theta_0 \leq v$.

Henceforth we will write $n'_i = n_{i+h}$ where h is as just fixed. Then $\{n'_0, \cdots, n'_{k-1}\} = \{n_0, \cdots, n_{k-1}\}$. In this notation, $n'_0 \neq 0$. Write

$$\mathcal{S}_h = \{(i+h)(\mathrm{mod} k) : i \in \mathcal{S}\} = \{(i_j + h)(\mathrm{mod} k) : 0 \leq j \leq s-1\};$$

then $i \in \mathcal{S}_h$ if and only if $(i-h)(\mathrm{mod}\, k) \in \mathcal{S}$, which holds if and only if $\alpha_{i-h} \neq 0$. The condition $n_i = 0$ if $i \in \mathcal{K}\backslash\mathcal{S}$ becomes $n'_i = 0$ if $i \in \mathcal{K}\backslash\mathcal{S}_h$.
In this notation, condition (5) gives

$$N = \sum_{j=0}^{s-1} n_{i_j} = \sum_{i\in\mathcal{S}} n_i = \sum_{i\in\mathcal{K}} n_i = \sum_{i\in\mathcal{K}} n'_i = \sum_{i\in\mathcal{S}_h} n'_i = \sum_{j=0}^{s-1} n'_{i_j+h} \tag{9}$$

while condition (7) becomes

$$\sum_{i\in\mathcal{K}} n'_i q^i \equiv 0\,(\mathrm{mod}\, m). \tag{10}$$

This last congruence may be written

$$\sum_{i\in\mathcal{K}} n'_i q^i = mQ \tag{11}$$

where $Q \in \mathbb{N}$ depends on the n'_i; note that $Q \neq 0$ because $\sum_{i=0}^{k-1} n'_i = N \neq 0$.

Step 7: Calculation of the constant term when $q \leq aQ$.

Suppose that $q \leq aQ$. Recall from Step 6 that we chose notation so that $n'_0 \neq 0$ and that for some v with $\theta_0 \leq v \leq k-1$, we have $n'_{k-v} = \cdots = n'_{k-1} = 0$. Further, v is maximal such that this occurs.
Because $q > 1$, then if $c_0, \cdots, c_{k-v-1}$ (note that $k-v-1 \geq 0$) are non-negative integers subject only to $N = \sum_{i=0}^{k-v-1} c_i$, the expression

$$c_0 + c_1 q + \cdots + c_{k-v-1} q^{k-v-1}$$

assumes its maximum value when $c_{k-v-1} = N$ and $c_0 = c_1 = \cdots = c_{k-v-2} = 0$; this maximum is Nq^{k-v-1}. In particular,

$$n'_0 + n'_1 q + \cdots + n'_{k-v-1} q^{k-v-1} \leq Nq^{k-v-1}. \tag{12}$$

According to the definition of N in Step 4, an upper bound for N is given by the product of s with the maximum possible value (as j varies) of the expression $a(1 + q + \cdots + q^{\theta(j)})$. The maximum value of this latter expression occurs when $\theta(j)$ assumes its maximal value θ_0. But $\theta_0 \leq v$ and $s \leq k$, and so

$$N \leq sa(1 + q + \cdots + q^{\theta_0}) \leq ak(1 + q + \cdots + q^v).$$

Thus

$$Nq^{k-v-1} \leq ak(q^{k-v-1} + q^{k-v} + \cdots + q^{k-1}).$$

But $ak < p$ by hypothesis, and so

$$ak < p \leq q \leq aQ$$

while

$$q^{k-v-1} + q^{k-v} + \cdots + q^{k-1} \leq 1 + q + \cdots + q^{k-1}$$

because $k - v - 1 \geq 0$, as we have just seen; thus

$$Nq^{k-v-1} < aQ(1 + q + \cdots + q^{k-1}).$$

This gives the second inequality in the following expression; the first equality is (11), the first inequality is given by (12) and the final equality is one of the hypotheses:

$$mQ = n'_0 + n'_1 q + \cdots + n'_{k-1} q^{k-1} \leq Nq^{k-v-1} < aQ(1 + q + \cdots + q^{k-1}) = mQ.$$

This is a contradiction. Therefore (9) and (11) admit no solution in the case $q \leq aQ$. Thus, it remains to consider the case $aQ < q$.

Step 8: Calculation of the constant term when $aQ < q$.

Suppose that $aQ < q$. By (11) and hypothesis we have

$$\sum_{i \in \mathcal{K}} n'_i q^i = mQ = aQ(1 + q + \cdots + q^{k-1}).$$

By our choice in Step 6, $n'_{k-v} = \cdots = n'_{k-1} = 0$ and so

$$n'_0 + n'_1 q + \cdots + n'_{k-v-1} q^{k-v-1} = aQ(1 + q + \cdots + q^{k-1}). \tag{13}$$

Since $aQ < q$, we have $n'_0 \equiv aQ \pmod{q}$; now write $n'_0 = aQ + m_0 q$. Similarly we can derive that

$$m_0 + n'_1 = aQ + m_1 q.$$

We continue the process, finding a new quotient $m_i \in \mathbb{N}_0$ at each stage, until we reach

$$m_{k-v-2} + n'_{k-v-1} q^0 = aQ(1 + \cdots + q^v). \tag{14}$$

Finally, we divide $m_{k-v-2} + n'_{k-v-1}$ by q to give

$$m_{k-v-2} + n'_{k-v-1} = aQ + m_{k-v-1} q$$

where $m_{k-v-1} \in \mathbb{N}_0$. We also deduce the following:

$$m_{k-v-1} = aQ(1 + \cdots + q^{v-1}).$$

From the above we may collect the equalities

$$\begin{aligned} n'_0 &= aQ + m_0 q \\ m_0 + n'_1 &= aQ + m_1 q \\ &\cdots \\ m_{k-v-2} + n'_{k-v-1} &= aQ + m_{k-v-1} q. \end{aligned} \tag{15}$$

Recall from Step 4 that, for $j = 0, \cdots, s-1$,

$$\mathcal{B}_j = \{i_j, i_j + 1, \cdots, i_j + \theta(j)\}.$$

Then (see Step 6) $\alpha_{i_j} \neq 0$, $n'_{i_j} \neq 0$ and $n'_{i_j+1} = n'_{i_j+2} = \cdots = n'_{i_j+\theta(j)} = 0$, while also $n'_i \neq 0$ only if $i \in \mathcal{S}_h$. Now (9) gives

$$N = \sum_{i \in \mathcal{K}} n'_i = \sum_{i \in \mathcal{S}_h} n'_i.$$

We have, as a subset of (15), corresponding to the block $\mathcal{B}_j$ (and where, for convenience, we set $m_{-1} = 0$):

$$\begin{aligned} m_{i_j-1} + n'_{i_j} &= aQ + m_{i_j} q \\ m_{i_j} + n'_{i_j+1} &= aQ + m_{i_j+1} q \\ &\cdots \\ m_{i_j+\theta(j)-1} + n'_{i_j+\theta(j)} &= aQ + m_{i_j+\theta(j)} q. \end{aligned}$$

Thus we have

$$\begin{aligned} m_{i_j-1} + n'_{i_j} &= aQ + m_{i_j} q \\ m_{i_j} + 0 &= aQ + m_{i_j+1} q \\ &\cdots \\ m_{i_j+\theta(j)-1} + 0 &= aQ + m_{i_j+\theta(j)} q. \end{aligned}$$

We start by substituting m_{i_j} from the second equation into the first to obtain

$$m_{i_j-1} + n'_{i_j} = aQ + (aQ + m_{i_j+1} q)q.$$

We then substitute the value of m_{i_j+1} from the third equation, and so on. We finally obtain, corresponding to the block $\mathcal{B}_i$, the equality

$$m_{i_j-1} + n'_{i_j} = m_{i_j+\theta(j)} q^{\theta(j)+1} + aQ \sum_{u=0}^{\theta(j)} q^u.$$

We have such an equality for each block $\mathcal{B}_0, \cdots, \mathcal{B}_{s-1}$:

$$\begin{aligned} m_{i_0-1} + n'_{i_0} &= m_{i_0+\theta(0)} q^{\theta(0)+1} + aQ \sum_{u=0}^{\theta(0)} q^u \\ &\cdots \\ m_{i_{s-1}-1} + n'_{i_{s-1}} &= m_{i_{s-1}+\theta(s-1)} q^{\theta(s-1)+1} + aQ \sum_{u=0}^{\theta(s-1)} q^u \end{aligned} \tag{16}$$

We sum equations (16) from $j = 0$ to $j = s-1$ (not forgetting that $i_0 = 0$ and $m_{-1} = 0$):

$$\sum_{j=0}^{s-1} m_{i_j-1} + \sum_{j=0}^{s-1} n'_{i_j} = \sum_{j=0}^{s-1} m_{i_j+\theta(j)} q^{\theta(j)+1} + aQ \sum_{j=0}^{s-1} \sum_{u=0}^{\theta(j)} q^u \tag{17}$$

Note that,

$$\sum_{j=0}^{s-1} n'_{i_j} = \sum_{j=0}^{s-1} n_{i_j+h} = \sum_{i=0}^{k-1} n_i = N.$$

But we have seen that $N = a \sum_{j=0}^{s-1} \sum_{u=0}^{\theta(j)} q^u$. Thus (17) simplifies to

$$\sum_{j=0}^{s-1} m_{i_j-1} + N = \sum_{j=0}^{s-1} m_{i_j+\theta(j)} q^{\theta(j)+1} + QN$$

that is,

$$\sum_{j=0}^{s-1} m_{i_j-1} = \sum_{j=0}^{s-1} m_{i_j+\theta(j)} q^{\theta(j)+1} + (Q-1)N \tag{18}$$

Now, the second sum in (18) may be written as:

$$\sum_{j=0}^{s-1} m_{i_j+\theta(j)} q^{\theta(j)+1} = \sum_{j=0}^{s-1} m_{i_j+\theta(j)} (q^{\theta(j)+1} - 1) + \sum_{j=0}^{s-1} m_{i_j+\theta(j)}.$$

Recall that we wish to prove that $s = 1$. Suppose $s > 1$. Then from the definition of $\theta(j)$ (for $s > 1$) we have $i_j + \theta(j) = i_{j+1} - 1$ when $0 \leq j \leq s-2$, and then (18) may be written as

$$\sum_{j=0}^{s-1} m_{i_j-1} = \sum_{j=0}^{s-1} m_{i_j+\theta(j)} (q^{\theta(j)+1} - 1) + (m_{i_{s-1}+\theta(s-1)} + \sum_{j=0}^{s-2} m_{i_{j+1}-1}) + (Q-1)N.$$

The first summand of the left-hand sum is $m_{i_0-1} = m_{-1} = 0$ and so the sum, in practice, runs from $j = 1$ until $j = s-1$. This sum then cancels with

$\sum_{j=0}^{s-2} m_{i_{j+1}-1}$ and so we have

$$m_{i_{s-1}+\theta(s-1)} + (Q-1)N + \sum_{j=0}^{s-1} m_{i_j+\theta(j)}(q^{\theta(j)+1} - 1) = 0.$$

Recall that for all $j = 0, \cdots, s-1$, we have $m_i \in \mathbb{N}_0$ and $q^{\theta(j)+1} - 1 > 0$, while also $N > 0$ (see Step 4). Thus the left-hand side here is a sum of non-negative terms, and so

$$Q - 1 = m_{i_0+\theta(0)} = \cdots = m_{i_{s-1}+\theta(s-1)} = 0$$

that is, $Q = 1$, and then (16) implies that

$$n'_{i_j} = \sum_{u=0}^{\theta(j)} aq^u$$

for $j = 0, \cdots, s-1$.

Step 9: Conclusion.

We continue to suppose that $s > 1$. By Steps 7 and 8, the only solution to (9) and (11) occurs when $Q = 1$ and is given by

$$n_{i_j+h} = n'_{i_j} = \sum_{u=0}^{\theta(j)} aq^u$$

for $j = 0, \cdots, s-1$. We now apply the permutation π_{-h} (the inverse of π_h) to n_{i_j+h} to conclude that

$$n_{i_j} = \sum_{u=0}^{\theta(j)} aq^u.$$

We saw above that the constant term of $g(t)^N (\mathrm{mod}\, t^m - 1)$ is given by

$$\frac{N!}{n_{i_0}! n_{i_1}! \cdots n_{i_{s-1}}!} \alpha_{i_0}^{n_{i_0}} \cdots \alpha_{i_{s-1}}^{n_{i_{s-1}}}$$

where the n_{i_j} are as just described and where $\alpha_{i_0}, \cdots, \alpha_{i_{s-1}}$ are all non-zero. Now,

$$N = \sum_{j=0}^{s-1} n_{i_j} = a \sum_{j=0}^{s-1} (1 + q + \cdots + q^{\theta(j)})$$

where

$$n_{i_j} = a(1 + q + \cdots + q^{\theta(j)}).$$

Let $r = \max\{\theta(j) : j = 0, \cdots s-1\}$. Then

$$N = \sum_{j=0}^{s-1} (c_{0,j} + c_{1,j} q + \cdots c_{r,j} q^r)$$

where $c_{r,j} = a$ if $i \leq \theta(j)$ and $c_{r,j} = 0$ if $i < \theta(j)$. Thus

$$N = \sum_{j=0}^{r} c_{0_j} + \sum_{j=0}^{r} c_{1_j} q + \cdots + \sum_{j=0}^{r} c_{r_j} q^r = C_0 + C_1 p^n + \cdots + C_r p^{rn},$$

where $C_i = \sum_{j=0}^{r} c_{i,j}$. It is clear that, for each i, $0 < a \leq C_i \leq as < ak < p$, thus $C_i! \not\equiv 0 \pmod{p}$.

Recall also that $N = n_{i_0} + n_{i_1} + \cdots + n_{i_{s-1}}$; the coefficient of p^{in} in n_{i_j} is a, and $a < p$. Further, C_i counts the number of times that a appears as a coefficient of q^i in the whole n_{i_j}. Now, using Lucas' Theorem (Lemma 3.3) we have

$$\frac{N!}{n_{i_0}! n_{i_1}! \cdots n_{i_v}!} \equiv \frac{C_0! C_1! \cdots C_r!}{(a!)^{C_0} (a!)^{C_1} \cdots (a!)^{C_r}} \not\equiv 0 \pmod{p}.$$

Theorem 3.1 implies that the constant term of $g(t)^N \pmod{t^m - 1}$ is 0, and so we must have

$$\alpha_{i_0}^{n_{i_0}} \cdots \alpha_{i_v}^{n_{i_v}} = 0,$$

a contradiction. It follows that $s = 1$; thus the set $\mathcal{S}$ has only one member and the group M is standard. This completes the proof. □

Example 3.5. In Theorem 3.4, take $q = 11$ and $k = 3$. Now, $\frac{11^3 - 1}{11 - 1} = 133$. The hypotheses of Theorem 3.4 are satisfied if $a \in \{1, 2\}$ and so the subgroups of orders 133 and $2 \times 133 = 266$ of $\mathbb{F}_{11^3}^*$ are standard as f-subgroups, where in each case $f(t)$ is the minimum polynomial over $\mathbb{F}_{11}$ of a generator of the group in question.

We may use results from [5] to extend Theorem 3.4 to cover cases where it is not immediately applicable. Suppose $M \leq \mathbb{A}_q^*$ is finite. It is shown in Section 2 of [5] that we may define the restricted period, $\delta(M)$, of M, as $\delta(h)$ where $h(t)$ is the minimum polynomial over $\mathbb{F}_q$ of a generator of the cyclic group M. With this in mind, we have the following:

Corollary 3.6. *Suppose that the hypotheses of Theorem 3.4 are satisfied by $f(t)$ and M. Let $M_1 \leq M$ be an f_1-subgroup such that $\delta(M_1) = \delta(M)$. Then M_1 is standard as an f_1-subgroup.*

Proof. If M_1 were non-standard as an f_1-subgroup, then by Theorem 3.1 of [5] M would be non-standard as an f-subgroup, contrary to Theorem 3.4 above. □

Example 3.7. Here we exhibit certain subgroups covered by Corollary 3.6 but not by Theorem 3.4. Take $q = 7$ and $k = 3$; then Theorem 3.4 guarantees

that the subgroups of $\mathbb{F}_{7^3}$ of order

$$a\left(\frac{7^3-1}{7-1}\right) = a \times 57,\ a \in \{1,2\}$$

are standard (for the respective minimum polynomials). We know from [5] that if $|M| = \frac{c}{d}(q-1)$ with $\gcd(c,d) = 1$, then $\delta(M) = c$. Thus the subgroups of orders 57 $(= \frac{19}{2} \times 6)$ and 114 $(= \frac{19}{1} \times 6)$ both have restricted period 19. But the subgroups of orders 19 $(= \frac{19}{6} \times 6)$ and 38 $(= \frac{19}{3} \times 6)$ in $\mathbb{F}_{7^3}^*$ also have restricted period 19. Because both 19 and 38 divide 114, so that the relevant subgroups are subgroups of the group of order 114, it follows from Corollary 3.6 that the subgroups of orders 19 and 38, although not covered by the hypotheses of Theorem 3.4, are also standard.

4 Acknowledgements

The authors would like to thank Maria Teresa Nogueira, sister of one of the authors and colleague of the other, for useful discussions concerning Step 8 of the proof of Theorem 3.4. They would also like to thank the Referees for their valuable suggestions.

References

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

[2] O.J. Brison and J.E. Nogueira, Linear recurring sequence subgroups in finite fields. Finite Fields and Their Applications 9 (2003) 413-422.

[3] O.J. Brison and J.E. Nogueira, Second order linear sequence subgroups in finite fields. Finite Fields and Their Applications 14 (2008) 277-290.

[4] O.J. Brison and J.E. Nogueira, Second order linear sequence subgroups in finite fields-II. Finite Fields and their Applications, 15 (2009), 40-53.

[5] O. J. Brison and J. E. Nogueira, Non-standard sequence subgroups in finite fields. Finite Fields and their Applications, 16 (2010), 187-203.

[6] Keith Conrad, Jacobi sums and Stickelberger's congruence, Enseignement Mathematique, 41 (1995), 141-153.

[7] H. Hollmann, Nonstandard linear recurring sequence subgroups in finite fields and automorphisms of cyclic codes, preprint (http:// arxiv.org/ abs/ 0807.0595v1.pdf).

[8] R. Lidl and H. Niederreiter, Finite fields. Second edition, Cambridge University Press, Cambridge (1997).

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

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