# Some basic results on finite linear recurring sequence subgroups 

Henk D. L. Hollmann<br>University of Tartu<br>Institute of Computer Science<br>Tartu 50409, Estonia.<br>Email: henk.d.l.hollmann@ut.ee

Medet Zhanbulatuly<br>10 Anson Road, International Plaza, \#38-16, 079903 Singapore<br>Email: medet.ntu@gmail.com

December 1, 2020


#### Abstract

An $f$-subgroup is a linear recurring sequence subgroup, a multiplicative subgroup of a field whose elements can be generated (without repetition) by a linear recurrence relation, with characteristic polynomial $f$. It is called non-standard if it can be generated in a non-cyclic way (that is, not in the order $\alpha^{i}, \alpha^{i+1}, \alpha^{i+2} \ldots$ for a zero $\alpha$ of $f$ ), and standard otherwise. We will show that a finite $f$-subgroup is necessarily generated by a subset of the zeros of $f$. We use this result to improve on a recent theorem of Brison and Nogueira. A old question by Brison and Nogueira asks if there exist automatically non-standard $f$-subgroups, $f$-subgroups that cannot be generated by a zero of $f$. We answer that question affirmatively by constructing infinitely many examples.


Keywords - linear recurrence relation, linear recurring sequence, $f$-subgroup, linear recurring sequence subgroup, non-standard sequence subgroup

## 1 Introduction

A finite multiplicative subgroup of $\mathbb{F}^{*}$, the nonzero elements in a commutative field $\mathbb{F}$, is necessarily cyclic (see, e.g. [22, Chapter 1, Lemma 1]), that is, of the form $\langle\alpha\rangle=$ $\left\{1, \alpha, \alpha^{2}, \ldots\right\}$ for some field element $\alpha$ of finite order. In a sequence of papers [1, 3, 4, [5, 6, 7, 8], Brison and Nogueira have investigated presentations of such a subgroup in a finite field by means of a (periodic) linear recurring sequence. Here, we say that a linear recurring sequence $s$ presents (or generates) a finite subgroup $M$ if $s$ has period $|M|$ and $M=\left\{s_{0}, s_{1}, \ldots, s_{|M|-1}\right\}$; moreover, if the linear recurrence relation satisfied by the sequence $s$ has characteristic polynomial $f$, then we refer to $M$ as an $f$-subgroup and to the generating sequence $s$ as an $f$-sequence.

For example, consider the (Fibonacci-type) linear recurrence relation

$$
\begin{equation*}
s_{n}=s_{n-1}+s_{n-2} \tag{1}
\end{equation*}
$$

with characteristic polynomial $f(x)=x^{2}-x-1$. If $\alpha$ is a zero of $f$ in some finite field $\mathbb{F}_{q}$ of size $q$ and characteristic $p>0$ (so with $q$ a power of the prime $p$ ), then the sequence $s$ with $s_{n}=\alpha^{n}$ for $n \in \mathbb{Z}$ obviously satisfies the recurrence relation (1), so if $\alpha$ has order $m$, then $M=\left\{1, \alpha, \ldots, \alpha^{m-1}\right\}$ is a presentation of $M$ by $s$, and hence $M$ is an $f$-subgroup. Usually, this is essentially the only way to present $M$, and then we refer to $M$ as a standard $f$-subgroup. However, it sometimes happens that there is another, essentially different way to present $M$. When $p \equiv \pm 2 \bmod 5$, the polynomial $f$ is irreducible and $q=p^{2}$; by combining results from [1] and [3], it can be shown that the subgroup $M \leq \mathbb{F}_{q}^{*}$ generated by a zero of $f$ is a standard $f$-subgroup except when $p=3, q=9$ : in that case, if $\omega \in \mathbb{F}_{9} \backslash \mathbb{F}_{3}$, the sequence

$$
s=\ldots, 1, \omega, 1+\omega, 1-\omega,-1,-\omega,-1-\omega,-1+\omega, 1, \omega, \ldots
$$

satisfies the recursion (1) and has period 8 , so this $f$-sequence $s$ presents $M=\mathbb{F}_{9}^{*}$. This gives 6 presentations for $M$ but $f$ has at most two zeros, and so 4 of these presentations are non-standard. We now refer to $M=\mathbf{F}_{9}^{*}$ as a non-standard $f$-subgroup. (In the remaining cases where $p=5$ or $p \equiv \pm 1 \bmod 5$, both zeros $a, b$ of $x^{2}-x-1$ are in $\mathbb{F}_{p}$, so $q=p$; later in this paper we show that $M=\langle a, b\rangle$ is in fact the only possible non-standard $f$-subgroup, but we do not know if this possibility ever occurs.)

As the above example suggests, non-standard $f$-subgroups tend to be rare (at least when we put some restrictions on $f$, see Section (6). In the case where $f(x) \in \mathbb{F}_{q}[x]$ is irreducible, it is known that an $f$-subgroup is necessarily generated by a zero of $f$. The cases where $f$ is irreducible of degree 2 have been fully classified, first when $q$ is prime in [3], then for general $q$ in [12], using a result from [6]. Interestingly, it turns out that for irreducible polynomials $f$, non-standardness occurs precisely when the irreducible cyclic code related to $f$ has extra automorphisms, for more details we again refer to [12]. Various types of non-standard irreducible cases have been identified, and we may well know them all.

In the general case, a clear understanding of the relation between the zeros of a polynomial $f$ and an $f$-subgroup was still missing. This relation is investigated in Section 3, The main result in this section states that an $f$-subgroup presented by a periodic sequence $s$ is equal to the group generated by the zeros of the minimal polynomial $f_{s}$ of $s$, hence is generated by some subset of the zeros of $f$. Note that this generalizes the result for irreducible polynomials mentioned earlier. We use our results to remove the degree condition " $k \leq p$ " in [8, Theorem 2.3].

Then in Section 4, we define a class of non-standard $f$-subgroups that we named automatically non-standard. These are subgroups $M$ of $\mathbb{F}^{*}$ presented by a periodic $f$ sequence $s$ where no zero of $f$ generates $M$. Note that if $s_{n+1} / s_{n}=\alpha$ for all $n$, then $f(\alpha)=0$ would follow from the recurrence relation; so the non-standardness of such an $f$-subgroup is inherent from the definition. This class is interesting since, as we show in this section, it turns out to be nonempty! We describe infinitely many examples, and we also prove an extension result. In [3, end of Observation 1.5], the authors state " $\ldots$ if $f$ is irreducible [with zero $\xi$ ] then any $f$-subgroup has the form $\langle\xi\rangle$ (considered as group), but we have no proof that this must occur in general." So our examples answer the implicit question here in the negative. In [2], automatically non-standard $f$-subgroups in the complex field where named non-standard of the second type. The authors informed us that they also knew examples in finite fields already in 2015.

To make the paper self-contained, in Section 2 we establish some notation and we quickly sketch a proof of most of the basic results concerning linear recurrence relations that are needed here. We basically follow the elegant approach in [9], but some of our proofs may be new and our method may be of independent interest.

Finally, in Section 6 we suggest some directions for further research and we discuss some open problems.

Part of this work is based on ideas obtained during a visit of the first author to Brison and Nogueira in 2013 and on later work by the second author [23, 24].

## 2 Preliminaries

In this section, we quickly sketch the required background on linear recurrence relations and linear recurring sequences. To describe the results, we will basically use the framework from [9]. While all the results in this section are known, parts of our approach may be new. For an element $\alpha \neq 0$ in a field $\mathbb{F}$, we write $\langle\alpha\rangle$ to denote the group $\left\{1, \alpha, \alpha^{2}, \ldots\right\}$ generated by $\alpha$. We will write $K \leq G$ to denote that $K$ is a subgroup of a group $G$. For other references for this material, see, for example, [14], [15], [16], [25].

Let $\mathbb{F}$ be an arbitrary field. A (two-way infinite) sequence $s=\left\{s_{n}\right\}_{n \in \mathbb{Z}}$ with $s_{n} \in \mathbb{F}$ for all $n \in \mathbb{Z}$ is called a ( $k$ th-order) linear recurring sequence over $\mathbb{F}$ if there exist $c_{0}, \ldots, c_{k-1}$ in $\mathbb{F}$, where $c_{0} \neq 0$ if $k>0$, such that

$$
\begin{equation*}
s_{n}=c_{k-1} s_{n-1}+c_{k-2} s_{n-2}+\cdots+c_{1} s_{n-k-1}+c_{0} s_{n-k} \tag{2}
\end{equation*}
$$

for all $n \in \mathbb{Z}$. A relation of the form (2) is called a ( $k$ th-order) linear recurrence relation. The polynomial

$$
f(x)=x^{k}-c_{k-1} x^{k-1}+\cdots-c_{1} x-c_{0}
$$

in $\mathbb{F}[x]$ is referred to as the characteristic polynomial of (21). We will say that the sequence $s$ satisfies the recursion $f$, or that $s$ is an $f$-sequence, if (2) holds for all $n \in \mathbb{Z}$, and we will write $\mathcal{L}_{\mathbb{F}}(f)$ to denote the collection of all $f$-sequences $s$ over $\mathbb{F}$. We say that a sequence satisfies a recursion $f$ where $f(x)=c x^{k}+\cdots$ has leading coefficient $c \neq 0$ if $s$ satisfies $c^{-1} f$. A sequence $s$ is called cyclic if there exists $\alpha \in \mathbb{F}$ such that $s_{n+1} / s_{n}=\alpha$ for all $n \in \mathbb{Z}$. Note that such a sequence is an $f$-sequence if and only if $f(\alpha)=0$.

Remark 2.1 Requiring instead that the coefficients $c_{0}, \ldots, c_{k-1}$ in (2) are contained in some extension field $\mathbb{E}$ of $\mathbb{F}$ would not have widened the notion of a linear recurring sequence over $\mathbb{F}$. That is, if a sequence $s$ with $s_{n} \in \mathbb{F}$ for all $n \in \mathbb{Z}$ satisfies some linear recurrence relation, then it also satisfies one where all coefficients are in $\mathbb{F}$. For periodic sequences, this follows from Theorem 2.8 below. In general, this follows from the existence of Berlekamp-Massey-type algorithms to compute the minimal polynomial, see, e.g., [17, 18, 20].

The collection $\mathcal{L}_{\mathbb{F}}$ of all sequences over $\mathbb{F}$ forms a vector space under point-wise addition and scalar multiplication, defined by $(s+t)_{n}=s_{n}+t_{n}$ and $(\lambda s)_{n}=\lambda s_{n}$ for $n \in \mathbb{Z}$ and $\lambda \in \mathbb{F}$. The (left) shift operator $\sigma$ operates on this vector space as $\sigma(s)=t$, where $t_{n}=s_{n+1}$ for $n \in \mathbb{Z}$. Let $\sigma^{k}$ denote $\sigma$ composed with itself $k$ times, and define $\left(a \sigma^{k}+\right.$ $\left.b \sigma^{l}\right)(s)=a \sigma^{k}(s)+b \sigma^{l}(s)$ for $a, b \in \mathbb{F}$. The next proposition collects some basic results for this set-up.

## Proposition 2.2

(i) The set of all operators $f(\sigma)$ for $f(x) \in \mathbb{F}[x]$, under addition and composition, is isomorphic to the polynomial ring $\mathbb{F}[\sigma]$, and the above defines a ring-action of $\mathbb{F}[\sigma]$ on the vector space $\mathcal{L}_{\mathbb{F}}$ (in technical terms, $\mathcal{L}_{\mathbb{F}}$ is a left $\mathbb{F}[\sigma]$-module).
(ii) A sequence $s \in \mathcal{L}_{\mathbb{F}}$ is an $f$-sequence if and only if $f(\sigma) s=0$.
(iii) If $s$ is an $f$-sequence and $t$ is a $g$-sequence, then $s+t$ is a $h$-sequence whenever both $f, g$ divide $h$.
(iv) If $f(x)$ has degree $k$, then the collection $\mathcal{L}_{\mathbb{F}}(f)$ of $s \in \mathcal{L}_{\mathbb{F}}$ for which $f(\sigma) s=0$ is a $k$-dimensional subspace of $\mathcal{L}_{\mathbb{F}}$.
(v) For every $s \in \mathcal{L}_{\mathbb{F}}$, the collection $\mathcal{I}_{\mathbb{F}}(s)$ of polynomials $f(x) \in \mathbb{F}[x]$ for which $f(\sigma) s=0$ is an ideal in $\mathbb{F}[x]$, and so there is a unique monic polynomial $f_{s}(x)$ such that $f(\sigma) s=0$ if and only if $f_{s}(x)$ divides $f(x)$.
(vi) If $(f, g)=1$, then $\mathcal{L}_{\mathbb{F}}(f) \cap \mathcal{L}_{\mathbb{F}}(g)=\mathcal{L}_{\mathbb{F}}(1)=\{0\}$.

Proof: (Sketch) (i) - (iii) are easy; for (i), remark that indeed $f(\sigma)(g(\sigma) s)=(f(\sigma) g(\sigma)) s$ for all $f(x), g(x) \in \mathbb{F}[x]$. Part (iv) follows from the observation that a sequence $s \in \mathcal{L}_{\mathbb{F}}$ satisfying a polynomial $f(\sigma)$ of degree $k$ is completely determined by $\left(s_{0}, \ldots, s_{k-1}\right)$. The polynomial $f_{s}(\sigma)$ in (v) is easily seen to be the monic polynomial with smallest degree
in $\mathcal{I}_{\mathbb{F}}(s)$. Finally, to see (vi), note that if $(f, g)=1$ in $\mathbb{F}[x]$, then there are $a(x), b(x) \in \mathbb{F}[x]$ for which $a(x) f(x)+b(x) g(x)=1$. Now if $s$ is both an $f$-sequence and a $g$-sequence, then by (ii) $s$ is also a 1 -sequence, hence $s=0$.
We will refer to the polynomial $f_{s}$ in (v) above as the minimal polynomial or the minimal recursion for $s$. In view of (i), in what follows we will identify $\mathbb{F}[x]$ and $\mathbb{F}[\sigma]$, and we will use $x$ instead of $\sigma$ to denote the left shift operator.

Next, we will describe the general solution of a linear recurrence relation. To this end, as in [19] we define the binomial coefficients $\binom{n}{j}$ for $n, j \in \mathbb{Z}$ by the relations $\binom{n}{j}=$ $\binom{n-1}{j}+\binom{n-1}{j-1}$ and $\binom{n+j-1}{j}=(-1)^{j}\binom{-n}{j}$ for $n, j=1,2,3, \ldots$ and in addition, $\binom{n}{0}=1$ for $n \in \mathbb{Z}$ and $\binom{0}{j}=0$ for $j \in \mathbb{Z}, j \neq 0$. It follows that $\binom{n}{-j}=0$ for $n \in \mathbb{Z}, j=1,2, \ldots$ and $\binom{n}{n+j}=0$ for $n=0,1,2, \ldots, j=1,2, \ldots$. We sketch a proof of the following.
Theorem 2.3 Suppose that $f(x) \in \mathbb{F}[x]$ has degree $m$ and factors completely over an extension $\mathbb{E}$ of $\mathbb{F}$. If $f$ has $t$ distinct zeros $\alpha_{1}, \ldots, \alpha_{t} \neq 0$ in $\mathbb{E}$, where $\alpha_{i}$ has multiplicity $e_{i}$ $(1 \leq i \leq t)$, then the collection $\mathcal{L}_{\mathbb{E}}(f)$ of $f$-sequences over $\mathbb{E}$ consists of the sequences $s=\left\{s_{n}\right\}_{n \in \mathbb{Z}}$ for which

$$
s_{n}=\sum_{i=1}^{t} \alpha_{i}^{n} \sum_{j=0}^{e_{i}-1} c_{i, j}\binom{n}{j} \quad(n \in \mathbb{Z})
$$

for suitable $c_{i, j} \in \mathbb{E}$.
Proof: By Proposition 2.2, part (iv), the vector space $\mathcal{L}_{\mathbb{E}}(f)$ of $f$-sequences over $\mathbb{E}$ has dimension $m=e_{1}+\cdots+e_{t}$, so we need to find $m$ independent solutions. As a consequence of Proposition 2.2, part (vi), it is sufficient to prove the theorem for $f(x)=(x-\alpha)^{m}$ with $\alpha \neq 0$, which follows if we show that the $m$ sequences $s^{(j)}$ with $s_{n}^{(0)}=1, s_{n}^{(1)}=$ $\binom{n}{1}, \ldots, s_{n}^{(m-1)}=\binom{n}{m-1}$ for $n \in \mathbb{Z}$ constitute $m$ independent solutions for the recursion $f(x)=(x-1)^{m}$.

Since $\left(s_{0}^{(j)}, \ldots, s_{m-1}^{(j)}\right)$ has the first nonzero entry equal to a 1 , in position $j$, it is evident that the sequences $s^{(j)}$ for $j=0, \ldots, m-1$ are independent. To complete the proof, we have to show that each sequence $s^{(j)}$ with $0 \leq j<m$ satisfies the recurrence relation $s_{n}-\binom{m}{1} s_{n-1}+\cdots+(-1)^{m-1}\binom{m}{m-1} s_{n-m+1}+(-1)^{m} s_{n-m}=0$, that is, we must show that $S(n, j)=\sum_{i=0}^{m}(-1)^{i}\binom{m}{i}\binom{n-i}{j}=0$ for $j=0, \ldots, m-1$ and for $n \geq m$.

In fact,

$$
S(n, j)= \begin{cases}0, & \text { if } 0 \leq j \leq m-1 \\ \binom{n-m}{j-m}, & \text { if } j \geq m\end{cases}
$$

Indeed, this is [19, Chapter 1, (5a)], or it follows from

$$
\sum_{j \geq 0} S(n, j) x^{j}=(1+x)^{n}(1-1 /(x+1))^{m}=(1+x)^{n-m} x^{m}=\sum_{j \geq m}\binom{n-m}{j-m} x^{j}
$$

Remark 2.4 The advantage of describing the solutions in terms of binomial coefficient sequences $\binom{n}{j}$ instead of the conventional $n^{j}$ is that the binomial solutions also work over fields with finite characteristic $p$ when $e_{i}>p$, cf. [15, Remark 8.23].

For completeness' sake, we also mention the following result.
Theorem $2.5([\mathbf{1 5}$, Theorem 8.27]) Let $f(x) \in \mathbb{F}[x]$ with $f(0) \neq 0$, where $\operatorname{char}(\mathbb{F})=$ $p>0$. Then every $f$-sequence s satisfies $\operatorname{per}(s) \mid \operatorname{ord}(f)$.

Finally, we need an expression for the minimal recursion $f_{s}$ of a periodic sequence $s$. Let $u^{(m)}$ be the periodic sequence with period $m$ for which $\left(u_{0}^{(m)}, \ldots, u_{m-1}^{(m)}\right)=(0, \ldots, 0,1)$. First we show the following.

Lemma 2.6 The sequence $u^{(m)}$ has minimal recursion $x^{m}-1$.
Proof: Since $\left(x^{m}-1\right) u^{(m)}=0$, the minimal recursion divides $x^{m}-1$. Conversely, from (2) we immediately see that any recursion for $u^{(m)}$ must have order $k \geq m$.

Lemma 2.7 The sequence $s$ is periodic with period $m$ if and only if $s=\tilde{s}(x) u^{(m)}$ with $\tilde{s}(x)=s_{0} x^{m-1}+\cdots+s_{m-2} x+s_{m-1}$.

Proof: Obvious from the definition of $u^{(m)}$.
The next theorem can also be derived using the approach in [15, Theorem 8.25].
Theorem 2.8 Let $s$ be periodic with period $m$ over $\mathbb{F}$. Then

$$
\begin{equation*}
f_{s}(x)=\left(x^{m}-1\right) /\left(x^{m}-1, \tilde{s}(x)\right), \tag{3}
\end{equation*}
$$

where $\tilde{s}(x)$ is defined as in Lemma [2.7, in particular, $f_{s}(x) \in \mathbb{F}[x]$.
Proof: By Lemma 2.7 we have that $s=\tilde{s}(x) u^{(m)}$; then using Lemma 2.6, we conclude that $f(x) s=0$ if and only if $x^{m}-1$ divides $f(x) \tilde{s}(x)$. The latter condition holds if and only if every zero of $x^{m}-1$ with multiplicity $e$ that occurs with multiplicity $h<e$ in $\tilde{s}(x)$ occurs in $f(x)$ with multiplicity at least $e-h$. This is the case precisely when the right hand side of (3) divides $f(x)$; now (3) follows from Proposition [2.2, part (v). Finally, note that the polynomial $f_{s}(x)$ defined by (3) is automatically contained in $\mathbb{F}[x]$.

The following basic result on periodic sequences can be obtained by combining various known results, but we prefer to give a simple direct proof.

Theorem 2.9 Let $f(x)=\prod_{i=1}^{t}\left(x-\alpha_{i}\right)^{e_{i}}$ be a polynomial in a field $\mathbb{F}$ with $p=\operatorname{char}(\mathbb{F})$, with distinct zeros $\alpha_{1}, \ldots, \alpha_{t} \neq 0$ in some extension $\mathbb{E}$ of $\mathbb{F}$, and let $s=\left\{s_{n}\right\}_{n \in \mathbb{Z}}$ be a nonzero $f$-sequence of period $m$ in $\mathbb{F}$, for which $(m, p)=1$ if $p>0$. Define $J=\{i \in$ $\left.\{1, \ldots, t\} \mid \alpha_{i}^{m}=1\right\}$. Then the following hold.
(i) The sequence $s$ has minimal recursion $f_{s}$, where $f_{s}$ is as defined in Theorem 2.8. In
particular, $f_{s}$ divides $f$ and $f_{s}$ has no multiple zeros.
(ii) There are $c_{i} \in \mathbb{E}(i \in J)$ such that

$$
\begin{equation*}
s_{n}=\sum_{i \in J} c_{i} \alpha_{i}^{n} \quad(n \in \mathbb{Z}) \tag{4}
\end{equation*}
$$

moreover, $f_{s}(x)=\prod_{\left\{i \mid c_{i} \neq 0\right\}}\left(x-\alpha_{i}\right)$. (iii) $m=\operatorname{lcm}\left(\operatorname{ord}\left(\alpha_{i}\right) \mid i \in J\right\}=\operatorname{lcm}\left(\operatorname{ord}\left(\alpha_{i}\right) \mid \alpha_{i}\right.$ is zero of $\left.f_{s}\right\}$.

Proof: (i) Under the conditions on $m$, the polynomial $x^{m}-1$ has no multiple zeros, hence the claim is a direct consequence of Proposition [2.2, part (v) and Theorem [2.8.
(ii) Since $f_{s}$ divides $f$ and $f_{s}(x) \mid x^{m}-1$ (see part (i)), we conclude that every zero of $f_{s}$ is of the form $\alpha_{i}$ with $i \in J$. Since $s$ is an $f_{s}$-sequence, the expression (4) follows from Theorem [2.3, Finally, again by Theorem [2.3, a sequence $s$ of the form (4) satisfies the recurrence $\prod_{\left\{i \mid c_{i} \neq 0\right\}}\left(x-\alpha_{i}\right)$ but not one of smaller degree.
(iii) Let $r=\operatorname{lcm}\left(\operatorname{ord}\left(\alpha_{i}\right) \mid i \in J\right)$ and $r^{\prime}=\operatorname{lcm}\left(\operatorname{ord}\left(\alpha_{i}\right) \mid \alpha_{i}\right.$ is zero of $\left.f_{s}\right\}$. By part (ii), by (4), and by the definition of $f_{s}$, every $\alpha_{i}$ actually occurring in the expression (4) for $s_{n}$ is in fact a zero of $f_{s}$, hence $r^{\prime}$ is a period of $s$, and as a consequence $m \mid r^{\prime}$. Conversely, since $\alpha_{i}^{m}=1$ for every $i \in J$, we have ord $\left(\alpha_{i}\right) \mid m$ for $i \in J$, hence $r^{\prime}|r| m$. We conclude that $r=m$.

## 3 General results for $f$-subgroups

We now investigate the relation between the characteristic polynomial $f$ of a recurrence relation and the period of an $f$-sequence presenting an $f$-subgroup. The following fundamental result may be considered as a generalization of [5, Lemma 2.1] and [8, Lemma 2.2].

Theorem 3.1 Let $f(x) \in \mathbb{F}[x]$ and let $M$ be a finite $f$-subgroup of size $m$ in some extension of $\mathbb{F}$, presented by an $f$-sequence $s$ with minimal recursion $f_{s}$. Then $f_{s}$ has no multiple zeros and $M$ is the group generated by the zeros of $f_{s}$, and hence is generated by a subset of the zeros of $f$.

Proof: If $s$ presents $M$, where $M$ has size $m$, then $s$ is periodic with smallest period $m$, and $(|M|, \operatorname{char}(\mathbb{F}))=1$ if $\operatorname{char}(\mathbb{F})>0$. Now the claims follow from Theorem 2.9,

Example 1: Here we show how the above can be used to investigate $f$-subgroups where $f \in \mathbb{F}[x]$ has degree 2. Suppose that $f$ has two distinct zeros $a, b \in \mathbb{F}$ (for the case $a=b$, see Theorem 3.3 below). By Theorem 3.1, an $f$-subgroup is one of $\langle a, b\rangle,\langle a\rangle$, or $\langle b\rangle$. Moreover, if the $f$-subgroup is smaller than $\langle a, b\rangle$, then by the same theorem, any $f$-sequence presenting it must have a minimal recursion of degree 1 , so is cyclic; hence the $f$-subgroup is standard. We conclude that $\langle a, b\rangle$ is the only candidate to be a nonstandard $f$-subgroup.

Remark 3.2 Let $p$ be a prime. Suppose that $h>\nu_{p}(j!)$, where $\nu_{p}(n)$ denotes the largest power of $p$ dviding $n$. Then for every integer $u$ we have that

$$
\begin{equation*}
\binom{p^{h} u+n}{j}=\frac{\left(p^{h} u+n\right)\left(p^{h} u+n-1\right) \cdots\left(p^{h} u+n-j+1\right)}{j!} \equiv\binom{n}{j} \bmod p \tag{5}
\end{equation*}
$$

As a consequence, if every zero $\alpha_{i}$ of the minimal polynomial $f_{s}(x)$ of a sequence $s$ satisfies $\alpha_{i}^{m}=1$, then $(m, p)=1$ and by Theorem 2.3 the sequence $s$ has a period $p^{h} m$ (this need not be the minimal period). This fact can be used for an alternative approach to Theorem [2.9, along the lines of [24, Theorem 3.2.1.]. Note that (5) and Theorem 2.9 together show that a linear recurring sequence is periodic in characteristic $p$ precisely when either $p>0$ or when $p=0$ and every zero of its minimal recursion has finite order and multiplicity 1.

For completeness' sake, we remark that a much more precise result is available. Indeed, [21, Lemma 1] (see also [10, Section 4]) implies that if $p^{r-1} \leq j<p^{r}$, then the sequence $s^{(j)}$ in $\mathbb{F}_{p}$ with $s_{n}^{(j)}=\binom{n}{j}$ for $n \in \mathbb{Z}$ has minimal period $p^{r}$. As a consequence, we can obtain an alternative proof for Theorem [2.5. To this end, note that if $q=p^{s}$ and $f(x) \in \mathbb{F}_{q}[x]$ has $\operatorname{per}(f)=n=n_{0} p^{r}$ with $\left(n_{0}, p\right)=1$, then the general expression for an $f$-sequence $s$ in Theorem 2.3 immediately implies that such a sequence has $n_{0} p^{r}=n=\operatorname{ord}(f)$ as a period: indeed, $f(x) \mid x^{n}-1=\left(x^{n_{0}}-1\right)^{p^{r}}$, hence $n_{0}$ is a period of all the $\alpha_{i}$, and $p^{r}$ is a period of all the binomial coefficients that occur.

We now present an application of the above results. In [8, Theorem 2.3], the authors showed that an $f$ subgroup for $f(x)=(x-a)^{k} \in \mathbb{F}_{p^{e}}$ is standard provided that $k \leq p$. We will use the above results to eliminate the extra condition on $k$ and to simplify the proof.

Theorem 3.3 Let $a \in \mathbb{F}_{q}^{*}$, where $q=p^{e}$ with $p$ a prime, and let $f(x)=(x-a)^{k} \in \mathbb{F}_{q}[x]$ with $k \geq 1$. Then an $f$-subgroup $M$ is necessarily of the form $M=\langle a\rangle$ and is standard as an $f$-subgroup.

Proof: Suppose that $s$ is an $f$-sequence with smallest period $m$ such that $M=\left\{s_{0}=\right.$ $\left.1, \ldots, s_{m-1}\right\}$ has size $m$ and is an $f$-subgroup in some extension $\mathbb{E}$ of $\mathbb{F}_{q}$. Then we may assume that $|\mathbb{E}|$ is finite, and since $m$ divides $|\mathbb{E}|-1$, we have $(m, p)=1$. The minimal polynomial $f_{s}(x)$ of $s$ divides $f(x)$, hence is of the form $(x-a)^{e}$, and by Theorem 2.9, we have $e=1$, hence $s$ is cyclic with $s_{n+1} / s_{n}=a(n \in \mathbb{Z})$ and $M=\langle a\rangle$ is standard.

## 4 Automatically non-standard $f$-subgroups

In this section, we answer a question that was implicitly raised in [3], Observation 1.5, namely whether it is always true that an $f$-subgroup is generated by a zero of $f$. We need some preparation.

For positive integers $m$, define the $m$ th cyclotomic polynomial $\phi_{m}(x)$ inductively by letting

$$
\begin{equation*}
x^{m}-1=\prod_{d \mid m} \phi_{d}(x) \tag{6}
\end{equation*}
$$

So, for example, $\phi_{1}(x)=x-1, \phi_{2}(x)=x+1, \phi_{3}(x)=x^{2}+x+1$, and $\phi_{4}(x)=x^{2}+1$. It is well-known and not difficult to prove(see, e.g., [11]) that in fact every $\phi_{m}(x)$ is a polynomial with integer coefficients, that is, $\phi_{m}(x) \in \mathbb{Z}[x]$, and $\operatorname{deg}\left(\phi_{m}\right)=\varphi(m)$, where $\varphi$ is the Euler function defined by $\varphi(m)=\left|\mathbb{Z}_{m}^{*}\right|$, the number of integers $k$ with $1 \leq k<m$ for which $(k, m)=1$.

Now let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F})=p$, and let $m$ be a positive integer with $(m, p)=1$ if $p>0$, so that $x^{m}-1$ has no multiple zeros. The mth cyclotomic polynomial $\phi_{p, m}$ over $\mathbb{F}$ is the polynomial $\phi_{m}$, reduced modulo $p$ if $p>0$. By its definition, $\phi_{p, m}$ has as its zeros precisely those $m$ th roots of unity that have order $m$, that is, the primitive mth roots of unity. Indeed, let $\alpha$ be a zero of $\phi_{p, m}$ in a suitable extension of $\mathbb{F}$. By assumption, $(m, p)=1$, so $\alpha$ has order $m$. Then the zeros of $x^{m}-1$ are $\alpha^{k}(0 \leq k<m)$, and $\alpha^{k}$ is a primitive root of unity precisely when $(k, m)=1$. As a consequence,

$$
\phi_{p, m}(x)=\prod_{k \in \mathbb{Z}_{m}^{*}}\left(x-\alpha^{k}\right)
$$

where the product is over all integers $k$ with $1 \leq k<m$ for which $(k, m)=1$.
Now assume that $f(x) \in \mathbb{F}[x]$, where $p=\operatorname{char}(\mathbb{F})$, and that $M$ is an $f$-subgroup of (finite) size $m$, that is, there exists an $f$-sequence $s$ of minimal period $m$ in some finite extension $\mathbb{E}$ of $\mathbb{F}$ such that $M=\left\{s_{0}, \ldots, s_{m-1}\right\}$. Then $(m, p)=1$ if $p>0$, and Theorem [2.9] applies: the sequence $s$ has a minimal polynomial $f_{s}(x)$ in $\mathbb{F}[x]$ that has no multiple zeros, where $f_{s}$ divides $f$ and $M$ is generated by the zeros of $f_{s}$. Now if $s$ is cyclic, say $s_{n+1} / s_{n}=\alpha(n \in \mathbb{Z})$, then $M=\langle\alpha\rangle$, so $\alpha$ has order $m$, and since $s$ satisfies $f_{s}$ we see from (2) that $f_{s}(\alpha)=0$, and hence $f(\alpha)=0$. But this cannot happen if $f$ does not have a primitive $m$ th root of unity as a zero. Observe also that since $M=\left\{s_{0}, \ldots, s_{m-1}\right\}$ is a group, we have that $s_{0}+\cdots+s_{m-1}=0$, hence $x-1 \mid \tilde{s}(x)$ (with $\tilde{s}(x)$ as defined in Lemma [2.7). With Theorem 2.8 in mind, this motivates the following definition.

Definition 4.1 Let $\mathbb{F}$ be a field with $p=\operatorname{char}(\mathbb{F})$, and let $m>1$ be an integer satisfying $(m, p)=1$ if $p>0$.
(i) If the polynomial $f(x)$ in $\mathbb{F}[x]$ divides $\left(x^{m}-1\right) /(x-1) \phi_{p, m}(x)$ and if $s$ is an $f$-sequence for which $M=\left\{s_{0}, s_{1}, \ldots, s_{m-1}\right\}$ is a subgroup of size $m$ in some extension of $\mathbb{F}$, then we refer to $M$ as an automatically non-standard $f$-subgroup.
(ii) If $s_{0}, \ldots, s_{m-1}$ are such that $M=\left\{s_{0}, \ldots, s_{m-1}\right\}$ is a subgroup of size $m$ in some extension of $\mathbb{F}$ and if $\phi_{p, m}(x)$ divides $\tilde{s}(x)=s_{m-1}+s_{m-2} x+\cdots+s_{0} x^{m-1}$, then we say that the subgroup $M$ is automatically non-standard.

By the discussion preceding this definition, the following should come as no surprise.

Theorem 4.2 (i) An automatically non-standard subgroup $M=\left\{s_{0}, \ldots, s_{m-1}\right\}$ is automatically non-standard $f$-subgroup with $f(x)=\left(x^{m}-1\right) /\left(x^{m}-1, \tilde{s}(x)\right)$.
(ii) An automatically non-standard $f$-subgroup is a non-standard $f$-subgroup.

Proof: (i) The periodic sequence $s$ with period $m$ defined by $s_{0}, \ldots, s_{m-1}$ generates $M$ and has minimal polynomial $f_{s}(x)=f(x)$ by Theorem 2.8. By definition, $\phi_{p, m} \mid \tilde{s}(x)$, and since $M$ is a group also $s_{0}+\cdots+s_{m-1}=0$ and $x-1 \mid \tilde{s}(x)$; since $m>1$, we conclude that $f(x) \mid\left(x^{m}-1\right) /(x-1) \phi_{p, m}(x)$ so $M$ is automatically non-standard $f$-subgroup.
(ii) Let the automatically non-standard $f$-subgroup $M$ have order $m>1$. By the definition of $\phi_{p, m}$, no zero of $\left(x^{m}-1\right) /(x-1) \phi_{p, m}(x)$, hence no zero of $f$, generates $M$. Hence $M$ cannot be generated by a cyclic $f$-sequence, so must be non-standard. (See [7, Lemma 1.3 (b)] for more details.)

A priori, it is not evident that automatically non-standard objects even exist. Moreover, we have the following simple negative result.

Theorem 4.3 A subgroup $M$ with $|M|=r^{e}$ with $r$ prime is never automatically nonstandard.

Proof: Let $M$ be an $f$-subgroup, for some polynomial $f$. By Theorem [2.9, we may assume that $f$ has distinct zeros $\alpha_{1}, \ldots, \alpha_{k}$ and that $M=\left\langle\alpha_{1}, \ldots, \alpha_{k}\right\rangle$. Every $\alpha_{i}$ has order $r^{h}$ for some integer $h \leq e$, hence $M$ can only be generated by the $\alpha_{i}$ if some $\alpha^{i}$ has order $r^{e}$, that is, if it generates $M$.

As a consequence, there are no automatically non-standard subgroups of sizes $2,3,4,5,7,8,9,11,13,16$ and 17 , but there could be automatically non-standard subgroups of size $6,10,12,14$, and 15 .

Example 2: Suppose that $M$ is an automatically non-standard multiplicative subgroup of size 6 in some finite field $\mathbb{F}_{q}$ of characteristic $p$ (so with $p \neq 2,3$ ). Let $M=\left\{s_{0}=1, \ldots, s_{5}\right\}$, where $\tilde{s}(x)=x^{5}+s_{1} x^{4}+\cdots+s_{5}$ is a multiple of the polynomial $\phi_{6}(x)=x^{2}-x+1$ containing all primitive 6 th roots of unity. With $\alpha^{2}=\alpha-1$ we have $\alpha^{3}=-1, \alpha^{4}=-\alpha, \alpha^{5}=-\alpha+1$, and so $M=\{1, \alpha, \alpha-1,-1,-\alpha,-\alpha+1\}$; moreover, $\tilde{s}(x) \equiv 0 \bmod x^{2}-x+1$ and $\tilde{s}(x) \equiv 0 \bmod x-1($ since $M$ is a subgroup), hence

$$
(-x+1)+s_{1}(-x)+s_{2}(-1)+s_{3}(x-1)+s_{4} x+s_{5}=0
$$

or equivalently,

$$
1-s_{2}-s_{3}+s_{5}=0, \quad-1-s_{1}+s_{3}+s_{4}=0
$$

and

$$
1+s_{1}+s_{2}+s_{3}+s_{4}+s_{5}=0
$$

By a careful examination of all possibilities, it can be shown [24] that necessarily the characteristic $p$ of the field satisfies $p=7$, with $M=\mathbb{F}_{7}^{*}$ and $s=(1,3,4,6,5,2)$ (or one of the other 5 sequences such as $(1,5,3,4,2,6)$ obtained from this one by multiplying
by $s_{i}^{-1}$ and shifting); the first sequence $s$ has $\tilde{s}(x)=x^{5}+3 x^{4}+4 x^{3}+6 x^{2}+5 x+2=$ $\left(x^{3}-2 x^{2}+2 x-1\right)\left(x^{2}+5 x+5\right)$ and $\left(x^{2}+5 x+5, x^{6}-1\right)=1$; hence this $s$ is an $f$-sequence with $f(x)=(x+1)\left(x^{2}+x+1\right)=x^{3}+2 x^{2}+2 x+1$ and generates the automatically non-standard $f$-subgroup $\mathbb{F}_{7}^{*}$.

The above example can be generalized as follows.
Theorem 4.4 Let $m=p-1=2 r$ with $r \geq 3$ odd and $p$ prime (that is, $p$ prime, $p \equiv 3 \bmod 4$ with $p \geq 7$ ). Then the subgroup $M=\mathbb{F}_{p}^{*}$ is automatically non-standard with respect to the polynomial $f(x)=(x+1)\left(x^{r}-1\right) /(x-1)$.

Proof: Let $m=p-1=2 r$ with $r \geq 3$ odd, and let $s$ be the sequence with period $m=p-1=2 r$ defined by

$$
s_{0}, \ldots, s_{m-1}=1,-2,3,-4, \ldots,-(r-1), r,-r, r-1,-(r-2), \ldots, 2,-1
$$

Then

$$
\tilde{s}(x)=x^{2 r-1}-2 x^{2 r-2}+\cdots-(r-1) x^{r+1}+r x^{r}-r x^{r-1}+(r-1) x^{r-2}+\cdots+2 x-1 .
$$

Let

$$
a(x)=1-2 x+3 x^{2}-\cdots-(r-1) x^{r-2}+r x^{r-1} .
$$

Then $a(x)=b^{\prime}(x)$ with

$$
b(x)=x-x^{2}+x^{3}-\cdots-x^{r-1}+x^{r}=x\left(x^{r}+1\right) /(x+1)=\left(x^{r+1}+x\right) /(x+1),
$$

hence
$\left.a(x)=\left((r+1) x^{r}+1\right)(x+1)-\left(x^{r+1}+x\right) \cdot 1\right) /(x+1)^{2}=\left(r x^{r+1}+(r+1) x^{r}+1\right) /(x+1)^{2}$.
and

$$
\begin{aligned}
\tilde{s}(x) & =-a(x)+x^{2 r-1} a\left(x^{-1}\right) \\
& =\left(\left(-r x^{r+1}-(r+1) x^{r}-1\right)+\left(r x^{r}+(r+1) x^{r+1}+x^{2 r+1}\right)\right) /(x+1)^{2} \\
& =\left(x^{2 r+1}+x^{r+1}-x^{r}-1\right) /(x+1)^{2}=\left(x^{r+1}-1\right)\left(x^{r}+1\right) /(x+1)^{2} .
\end{aligned}
$$

Now if $\xi$ is a primitive $m$ th root of unity in $\mathbb{F}_{p}$, then $\xi^{2 r}=1$ but $\xi^{r} \neq 1$ (since $r \geq 3$ ) and $\xi^{2} \neq 1$, so $\xi^{r}=-1$ and $\xi$ is a zero of $\left(x^{r}+1\right) /(x+1)$. As a consequence, $\tilde{s}(x)$ contains all primitive $m$ th roots of unity and $M=\left\{s_{0}, \ldots, s_{m-1}\right\}=\mathbb{F}_{p}^{*}$ is automatically non-standard in $\mathbb{F}_{p}$.

Since $r$ is odd, we have that

$$
\begin{aligned}
\left(x^{2 r}-1, \tilde{s}(x)\right) & =\left(x^{2 r}-1,\left(x^{r+1}-1\right)\left(x^{r}+1\right) /(x+1)^{2}\right) \\
& =\left((x+1)\left(x^{r}-1\right),\left(x^{r+1}-1\right) /(x+1)\right)\left(x^{r}+1\right) /(x+1) \\
& =(x-1)\left(x^{r}+1\right) /(x+1),
\end{aligned}
$$

hence by Theorem [2.8, the minimal polynomial for the sequence $s$ is

$$
f_{s}(x)=\left(x^{2 r}-1\right) /\left(x^{2 r}-1, \tilde{s}(x)\right)=(x+1)\left(x^{r}-1\right) /(x-1) .
$$

Example 3: There is another way to show that for $m=p-1=2 r$ with $r \geq 3$ odd the group $\mathbb{F}_{p}^{*}$ is automatically non-standard. Indeed, let $s$ be the sequence with period $m=p-1$ defined by

$$
s_{0}, \ldots, s_{m-1}=1,-1,3,-3, \ldots, r-2,-(r-2) ; r ; 2,-2,4,-4, \ldots, r-1,-(r-1) ; r+1
$$

Then

$$
\tilde{s}(x)=x^{2 r-1}-2 x^{2 r-2}+\cdots-(r-1) x^{r+1}+r x^{r}-r x^{r-1}+(r-1) x^{r-2}+\cdots+2 x-1 .
$$

In [24] it is shown that in fact

$$
\begin{aligned}
\tilde{s}(x) & =\left[(x+1)\left(x^{r-2}+3 x^{r-4}+5 x^{r-6}+\cdots+(r-2) x\right)+r\right](x-1)\left(x^{r}+1\right) /(x+1) \\
& =a(x)(x-1)\left(x^{r}+1\right) /(x+1)
\end{aligned}
$$

with $a(x)=(x+1)\left(x^{r-2}+3 x^{r-4}+5 x^{r-6}+\cdots+(r-2) x\right)+r$ (it is not too difficult to check this directly). Note that a primitive (2r)th root of unity $\xi$ satisfies $\xi^{r}=-1$ and $\xi \neq-1$ for $r \geq 3$, hence every generator of $M=\mathbb{F}_{p}^{*}$ is a zero of $\tilde{s}(x)$; as a consequence, $\mathbb{F}_{p}^{*}$ is automatically non-standard. In order to compute the minimal polynomial $f_{s}(x)$ for the sequence $s$, we use Theorem 2.8. We have that

$$
\left(x^{2 r}-1, \tilde{s}(x)\right)=\left((x-1)\left(x^{r}+1\right) /(x+1)\right)\left((x+1)\left(x^{r}-1\right) /(x-1), a(x)\right)
$$

Now $(x+1, a(x))=(x+1, r)=1$, and it is not difficult to verify [24] that

$$
\left(x^{2}-1\right) a(x)-\left(x^{2}+1\right)\left(x^{r}-1\right) /(x-1)=-(r-1) x-(r+1)=-(r-1)(x-1 / 3) .
$$

Hence

$$
\left((x+1)\left(x^{r}-1\right) /(x-1), a(x)\right)=\left(x^{r}-1, x-1 / 3\right) .
$$

Now $1 / 3$ is zero of $x^{r}-1$ when $3^{r}=3^{(p-1) / 2}=1$ in $\mathbb{F}_{p}$, that is, when 3 is a (nonzero) square in $\mathbb{F}_{p}$. If $p \neq 2,3$, then by quadratic reciprocity, see, e.g., 13 , this happens precisely when $p \equiv \pm 1 \bmod 12$. In our case, $p \equiv 3 \bmod 4$ and $p \geq 7$, so $p \not \equiv 1 \bmod 12$ (and certainly not $p \equiv 3 \bmod 12)$ and we have that

$$
f_{s}(x)= \begin{cases}(x+1)\left(x^{r}-1\right) /(x-1), & \text { if } p \equiv 7 \bmod 12 \\ (x+1)\left(x^{r}-1\right) /(x-1)(x-1 / 3), & \text { if } p \equiv 11 \bmod 12\end{cases}
$$

## 5 Extension for automatically non-standard subgroups

In this section, we will prove the following extension theory.
Theorem 5.1 If $M$ is an automatically non-standard $f$-subgroup in some field $\mathbb{E}$, then every finite multiplicative subgroup of $\mathbb{E}$ that contains $M$ is again automatically nonstandard, with respect to the polynomial $g(x)=f\left(x^{k}\right)$.
Proof: By our assumptions on $M$, there exists an $f$-sequence $s$ with period $m=|M|$ over $\mathbb{E}$ such that $M=\left\{s_{0}, \ldots, s_{m-1}\right\}$, where $f(x) \mid\left(x^{m}-1\right) /\left((x-1) \phi_{p, m}(x)\right.$. Since the minimal recursion $f_{s}$ for $s$ satisfies $f_{s}(x) \mid f(x)$, we conclude from Theorem [2.8] that $(x-$ 1) $\phi_{p, m}(x) \mid \tilde{s}(x)$, where $\tilde{s}(x)$ is the polynomial associated with the sequence $s$. Now let $L$ be a subgroup with $M \leq L$ and $|L|=k|M|$, say. Suppose that $e_{0}, e_{1}, \ldots, e_{k-1}$ are a system of distinct coset representatives of $L / M$. Now consider the presentation for $L$ as

$$
e_{0} s_{0}, e_{1} s_{0}, \ldots, e_{k-1} s_{0}, e_{0} s_{1}, \ldots, e_{0} s_{m-1}, \ldots, e_{k-1} s_{m-1}
$$

that is, $L=\left\{t_{0}, \ldots, t_{k m-1}\right\}$ with $t_{k j+i}=e_{i} s_{j}$ for $0 \leq i<k, 0 \leq j<m$. For the associated polynomial $\tilde{t}(x)$ of the sequence $t$ (extended with period $k m$ ) we now find

$$
\begin{aligned}
\tilde{t}(x) & =\sum_{u=0}^{k m-1} t_{u} x^{k m-1-u}=\sum_{i=0}^{k-1} \sum_{j=0}^{m-1} e_{i} s_{j} x^{m k-1-j k-i} \\
& =\sum_{i=0}^{k-1} e_{i} x^{k-1-i} \sum_{j=0}^{m-1} s_{j} x^{k(m-1-j)}=\tilde{e}(x) \tilde{s}\left(x^{k}\right)
\end{aligned}
$$

where $\tilde{e}(x)=\sum_{i=0}^{k-1} e_{i} x^{k-1-i}$. Now since $\tilde{s}\left(x^{k}\right) \mid \tilde{t}(x)$ and $\phi_{p, k m}(x)\left|\phi_{p, m}\left(x^{k}\right)\right| \tilde{s}\left(x^{k}\right)$, we conclude from Theorem 2.8 that $f_{t}(x) \mid f_{s}\left(x^{k}\right)$, hence $f_{t}(x) \mid f\left(x^{k}\right)$. Finally, using again that $\phi_{p, k m}(x) \mid \phi_{p, m}\left(x^{k}\right)$, we have that $f\left(x^{k}\right)\left|\left(x^{k m}-1\right) /\left(x^{k}-1\right) \phi_{p, m}\left(x^{k}\right)\right|\left(x^{k m}-1\right) /(x-1) \phi_{p, k m}$. So with $g(x)=f\left(x^{k}\right)$, the subgroup $L$ is presented by the $g$-sequence $t$, hence $L$ is an automatically non-standard $g$-subgroup.

Remark 5.2 So far, we have only constructed automatically non-standard groups $\mathbb{F}_{p}^{*}$ of size $p-1$ for primes $p \equiv 3 \bmod 4$, and their extensions (in the sense of Theorem 5.1) of size $m=k(p-1)$ with $k>0$ an integer with $(k, p)=1$. Note also that this type of extension to an automatically non-standard group $M=\mathbb{F}_{q}^{*}$ for $q$ a prime power is not always possible, since for example $M=\mathbb{F}_{9}^{*}$, of size $8=2^{3}$, is ruled out by Theorem 4.3., However, there seems to be no obvious reason why there cannot be an automatically non-standard subgroup of every size $m$ of the form $m=r s$ with $r, s>1$ and $(r, s)=1$, although we do not know an example in every such case. Taking $M=\mathbb{F}_{11}^{*}$ provides a automatically non-standard group for $m=10$. Extension of the $m=6$ example in characteristic $p=7$ by taking $k=2$ gives a non-standard group of size 12 in $\mathbb{F}_{7^{2}}^{*}$, so the smallest undecided case is $m=14$. This size may still be small enough to be handled by an exhaustive search, if needed with the help of a computer.

## 6 Discussion and open problems

Trivially, there are no non-standard subgroups of order $m \leq 3$; however every subgroup $M \leq \mathbb{F}^{*}$ of size $m \geq 4$ is a non-standard $f$-subgroup for $f(x)=\left(x^{m}-1\right) /(x-1)=x^{m-1}+$ $\cdots+x+1$ in any characteristic $p$, provided that $(m, p)=1$. Indeed, let $M=\langle\alpha\rangle$ with $\alpha$ in some extension $\mathbb{F}_{q}$ of $\mathbb{F}_{p}$ (such an element exists if $(m, p)=1$ ), and let $\pi$ be a permutation of $1,2, \ldots, m-1$. Then $s_{0}=1, s_{1}=\alpha^{\pi(1)}, \ldots, s_{m-1}=\alpha^{\pi(m-1)}$ is a presentation of $M$ by a periodic $f$-sequence $s$ with period $m$. Indeed, if $s_{n}, s_{n+1}, \ldots, s_{n+m-2}$ are $m-1$ distinct elements of $M$, then $s_{n+m-1}=-s_{n}-s_{n+1}-\cdots-s_{n+m-2}$ is the remaining element in $M$ distinct from $s_{n}, \ldots, s_{n+m-2}$. So there are at least $(m-1)$ ! $f$-sequences $s$ with $s_{0}=1$ presenting $M$, and there are only $\varphi(m)$ presentations $1, \beta, \beta^{2}, \ldots$ with $\beta=\alpha^{k},(k, m)=1$, a primitive $m$ th root of 1 in $M$. Now $(m-1)!>m-1 \geq \varphi(m)$ for $m \geq 4$. For example, if $m=4$ and $p$ is odd, there exists a primitive 4th root of unity, say $\alpha$, in $\mathbb{F}_{p}^{*}($ if $p \equiv 1 \bmod 4)$ or in $\mathbb{F}_{p^{2}} \backslash \mathbb{F}_{p}($ if $p \equiv 3 \bmod 4)$. By Theorem 2.8, both presentations $s_{0}, s_{1}, s_{2}, s_{3}=1,-1, \alpha,-\alpha$ and $1, \alpha,-\alpha,-1$ have minimal polynomial $f_{s}(x)=x^{3}+x^{2}+x+1=(x+1)\left(x^{2}+1\right)$.

In order to avoid such slightly trivial examples, we need to put further constrants on the polynomial $f$. One possibility is to require that $f(x)$ is irreducible over some field $\mathbb{F}_{q}$, and to take $M=\langle\alpha\rangle$ for some zero $\alpha$ of $f(x)$ in view of Theorem 2.9, Another possibility is to require that no zero of $f(x)$ generates $M$, which leads to the automatically non-standard subgroups considered here in Sections 4 and 5 ,

In view of the above, and given Theorem 2.9, the most ambitious goal would be to determine, for every prime $p$, all minimally non-standard polynomials in characteristic $p$, that is, all polynomials $f$ over a field of characteristic $p$ for which the subgroup $M$ generated by the zeros of $f$ can be presented as $M=\left\{s_{0}, s_{1}, \ldots, s_{m-1}\right\}$ with $m=|M|$ for a non-cyclic sequence $s$ with minimal period $m$ and minimal recursion $f_{s}=f$ (an even more ambitious goal would be to count the number of such presentations). Note that every minimally non-standard polynomial has degree at least 2 , as every polynomial $f(x)=x-a$ of degree 1 is of course standard.

With this point of view, all minimally non-standard polynomials $f(x) \in \mathbb{F}_{q}$ of degree 2 and of the form $f(x)=(x-\xi)\left(x-\xi^{q}\right)$ for some $\xi \in \mathbb{F}_{q^{2}} \backslash \mathbb{F}_{q}$ (that is, irreducible over $\mathbb{F}_{q}$ ) have been determined in [12]; there is a relation with irreducible cyclic codes having extra automorphisms. In [7] and in [12], various other classes of irreducible nonstandard polynomials are described; obviously these are all minimally non-standard. So besides classifying all irreducible non-standard polynomials (which might be possible at least for degree at most 3), now one of the main open problems is the determination of the minimally non-standard polynomials $f(x) \in \mathbb{F}_{q}$ of degree 2 , of the form $f(x)=$ $(x-a)(x-b)$ with $a, b \in \mathbb{F}_{q} \backslash\{0,1\}, a \neq b$, with $M=\langle a, b\rangle$. To the best of our knowledge, the only known examples are the polynomials $f(x)=x^{2}-a^{2} \in \mathbb{F}_{q}[x]$ with $q$ odd, $a \in \mathbb{F}_{q}$ of even order $m>4$ (where $\langle a\rangle$ is indeed a non-standard $f$-subgroup [3, Proposition 2.3]). In a subsequent paper, we will describe some new examples of degree 2 .

## 7 Acknowledgments

We wish to thank Owen Brison and Eurico Nogueira for their careful reading of a draft version of this work. Their comments greatly helped to improve the paper. Part of this work has been initiated during a visit of the first author to Brison and Nogueira in 2013. Both authors wish to acknowledge the support of Nanyang Technological University, Singapore, where the first part of this research was carried out. The research of H.D.L. Hollmann is in part supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03, and in part by the Estonian Research Council grant PRG49.

## References

[1] Owen J. Brison, Complete Fibonacci sequences in finite fields, Fib. Quart., vol. 30, no. 4, 1992, 295-304.
[2] Owen J. Brison and J. Eurico Nogueira, Linear Recurring Sequence Subgroups in the Complex Field, Fib. Quart., vol. 41, nr. 5, 2003, 397-404.
[3] Owen J. Brison and J. Eurico Nogueira, Linear recurring sequence subgroups in finite fields, Finite Fields Appl. 9 (2003), 413-422.
[4] Owen J. Brison and J. Eurico Nogueira, Matrices and Linear Recurrences in Finite Fields, The Fibonacci Quarterly, vol. 44, no. 2, 2006, pp. 103-108.
[5] Owen J. Brison and J. Eurico Nogueira, Second order linear sequence subgroups in finite fields, Finite Fields Appl., vol. 14, 2008, pp. 277-290.
[6] Owen J. Brison and J. Eurico Nogueira, Second order linear sequence subgroups in finite fields - II, Finite Fields Appl. 15 (2009) 40-53.
[7] Owen J. Brison and J. Eurico Nogueira, Non-standard sequence subgroups in finite fields, Finite Fields and Their Applications 16, 2010 :187-203.
[8] Owen J. Brison and J. Eurico Nogueira, Standard Sequence Subgroups in Finite Fields, Finite Fields Appl. 25 (2014), 326-340.
[9] J.P. Fillmore and M.L. Marx, Linear Recursive Sequences, SIAM 1968, SIAM Review, Vol. 10, No. 3, July 1968, 342-352.
[10] R.D. Fray, Congruence properties of ordinary and $q$-binomial coefficients, Duke Math. J., Sept. 1967.
[11] Paul B. Garrett, Abstract Algebra, Chapman and Hall/CRC, 2007.
[12] Henk D.L. Hollmann, Non-standard linear recurring sequence subgroups in finite fields and automorphisms of cyclic codes, submitted to Finite Fields and their Applications. See also http://arxiv.org/abs/0807.0595v1, 2008.
[13] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Graduate Texts in Mathematics 84, Springer Verlag, New York, 1990.
[14] D. Laksov, Linear Recurring Sequences over Finite Fields, Mathematica Scandinavica 16, 1965, 181-196.
[15] R. Lidl, H. Niederreiter, Finite fields (2ed), Cambridge UniversityPress, 1997.
[16] R.J. McEliece, Linear Recurring Sequences over Finite Fields, Ph.D. thesis, Caltech, 1967.
[17] G.H. Norton, On the minimal realizations of a finite sequence, J. Symbolic Comp. 20 (1995), 93-115.
[18] G.H. Norton, Minimal Polynomial Algorithms for Finite Sequences, IEEE Trans. on Inform. Theory, vol. 56, 2010, 4643-4745.
[19] J. Riordan, Combinatorial Identities, John Wiley and Sons, New York, 1968.
[20] A. Salagean, An Algorithm for Computing Minimal Bidirectional Linear Recurrence Relations, IEEE Trans. on Inform. Theory, vol. 55, 2009, 4695-4700.
[21] W.F.Trench, On the periodicities of certain sequences of residues, Amer. Math. Monthly, 67 (1960), 652-656.
[22] Andre Weil, Basic Number Theory (3rd ed.), Springer-Verlag, New York, Heidelberg, and Berlin, 1974.
[23] Medet Zhanbulatuly, Bernhard Schmidt, Henk D.L. Hollmann, Linear Recurring Sequence Subgroups In Finite Fields, Proceedings of the URECA@NTU, 2013-2014, Ureca project, Nanyang Technological University (2014).
[24] Medet Zhanbulatuly, Linear Recurring Sequence Subgroups In Finite Fields, Final Year Project, Nanyang Technological University, November 2014, supervisor Frederique Elise Oggier, co-supervisor Henk D.L. Hollmann.
[25] N. Zierler, Linear recurring sequences, J. Soc. Indust. Appl. Math. (SIAM), vol. 7, no. 1, March 1959, 31-48.

