LINEAR RECURRING SEQUENCE SUBGROUPS IN THE COMPLEX FIELD

Owen J. Brison

Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa
Bloco C1, Piso 3, Campo Grande, 1749-016 Lisboa, Portugal

J. Eurico Nogueira

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

(Submitted May 2001-Final Revision January 2002)

Let $S = (s_n)_{n\in\mathbb{Z}}$ be a "doubly infinite" recurring sequence in the complex field, $\mathbb{C}$, satisfying the recurrence

$$s_{n+2} = \sigma s_{n+1} + \rho s_n \tag{1}$$

where $\sigma,\ \rho \in \mathbb{C}$ and $\rho \neq 0$. It can happen that the elements of a minimal periodic segment (see below) of S form a subgroup of the multiplicative group $\mathbb{C}^*$ of $\mathbb{C}$ and our purpose here is to investigate this phenomenon. The analogous situation in the context of finite fields seems to have first been investigated by Somer [2], [3]; see also [1].

Write $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t], \rho \neq 0$. A sequence of complex numbers $S = (s_n)_{n\in\mathbb{Z}}$ satisfying (1) will be called an *f-sequence* in $\mathbb{C}$; f is the *characteristic polynomial* of S. If there exists $m \in \mathbb{N}$ such that $s_a = s_{a+m}$ for all $a \in \mathbb{Z}$ and if also m is minimal subject to this then S is *periodic* with *least period m*. By a *minimal periodic segment* we understand the whole sequence if S is not periodic, and any segment consisting of m consecutive members of S if S is periodic with least period m.

Definition 1: Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t],\ \rho \neq 0$. The subgroup $M \leq \mathbb{C}^*$ is said to be an *f-sequence subgroup* if either
(a) M is infinite and the underlying set of M can be written in such an order as to form a doubly infinite f-sequence $(s_n)_{n\in\mathbb{Z}}$ where $s_a \neq s_b$ if $a \neq b$, or
(b) M is finite, of order m, and the underlying set of M can be written in such an order as to coincide with a minimal periodic segment of an f-sequence $(s_n)_{n\in\mathbb{Z}}$, where $s_a = s_b$ if and only if $a \equiv b \pmod{m}$.

We will write $M = (s_n)_{n\in\mathbb{Z}}$ even if M is finite, and will say that $(s_n)_{n\in\mathbb{Z}}$ is *a representation of*, or *represents*, M as an f-sequence.

If $f(t) \in \mathbb{C}[t],\ f(0) \neq 0$, and if $g,\ h \in \mathbb{C}^*$ are roots of f, then

$$< g >= (\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots) = (g^n)_{n\in\mathbb{Z}}$$

is an "obvious" representation of $< g >\leq \mathbb{C}^*$ as an f-sequence subgroup; it can happen that $h \neq g$ but $< h >=< g >$, and then $(h^n)_{n\in\mathbb{Z}}$ is a different representation of the same subgroup. This suggests:

Definition 2: Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t], \rho \neq 0$.
(a) The f-sequence $(s_n)_{n\in\mathbb{Z}}$ in $\mathbb{C}$ is said to be *cyclic* if there exists $g \in \mathbb{C}$ such that $s_{n+1}/s_n = g$ for all $n \in \mathbb{Z}$.
(b) The f-sequence subgroup M of $\mathbb{C}^*$ is said to be *standard* if whenever M is represented as an f-sequence $M = (s_n)_{n\in\mathbb{Z}}$ then $(s_n)_{n\in\mathbb{Z}}$ is necessarily cyclic. Otherwise, M is said to be *nonstandard*.

(c) Suppose that M is a nonstandard f-sequence subgroup. If M admits representation as a cyclic f-sequence then we say that M is *nonstandard of the first type*; otherwise M is said to be *nonstandard of the second type.*

Essentially, M is standard if the "obvious" ways are the only ways of realising it as an f-sequence subgroup. If $M = (g^n)_{n\in\mathbb{Z}}$ is a representation of M as a cyclic f-sequence, then it is clear that g must be both a root of $f(t)$ and a generator of M as a group, whence M is a cyclic group. It is possible to find polynomials $f(t)$ which admit non-cyclic f-sequence subgroups: see Proposition 6(d) below.

Our main results are Propositions 4 and 6. Suppose that $f(t) \in \mathbb{C}[t]$ and that f has roots $g,\ h \in \mathbb{C}^*$. Except in the case

$$|g| = |h| \neq 1 \text{ and } g \neq \pm h,$$

which remains open, we prove that an f-sequence subgroup must be standard unless $g = -h$; when $g = -h$ we classify the nonstandard subgroups.

Observations 3: Suppose $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t]$, $\rho \neq 0$, with roots $g,\ h \in \mathbb{C}^*$, and let $(s_n)_{n\in\mathbb{Z}}$ be an f-sequence in $\mathbb{C}$.
(a) Suppose firstly that $g \neq h$. By linear algebra, there exist $\alpha, \beta \in \mathbb{C}$ with $s_0 = \alpha + \beta$ and $s_1 = \alpha g + \beta h$. By induction, $s_n = \alpha g^n + \beta h^n$ for all integers $n \geq 0$, and because $\rho \neq 0$ this may be extended to cover the case of negative n.
(b) Suppose next that $g = h$. There exist $\alpha, \beta \in \mathbb{C}$ such that $s_0 = \alpha$ and $s_1 = g(\alpha + \beta)$. Again, we have $s_n = (\alpha + n\beta)g^n$ for all $n \in \mathbb{Z}$.
(c) The reciprocal polynomial of $f(t)$ is $(-\rho)f^*(t)$ where $f^*(t) = t^2 + (\sigma/\rho)t - (1/\rho)$. The roots of $f^*(t)$ are $g^{-1}, h^{-1} \in \mathbb{C}^*$.

If $(s_n)_{n\in\mathbb{Z}}$ is an f-sequence in $\mathbb{C}$ then $(r_n)_{n\in\mathbb{Z}}$ is an f^*-sequence where $r_n = s_{-n}$. If $M = (s_n)_{n\in\mathbb{Z}}$ is an f-sequence subgroup of $\mathbb{C}^*$ then $M = (r_n)_{n\in\mathbb{Z}}$ is also an f^*-sequence subgroup. Thus M is standard as an f-sequence subgroup if and only if it is standard as an f^*-sequence subgroup. Further, if $s_n = \alpha g^n + \beta h^n$ for all $n \in \mathbb{Z}$ then $r_n = \alpha(g^{-1})^n + \beta(h^{-1})^n$ for all n.

Before continuing, we fix some notation. If $z \in \mathbb{C}$ then $|z|$ will always denote the modulus of z. We will use $\mathrm{ord}(z)$ to denote the multiplicative order of $z \in \mathbb{C}^*$, if z is a root of unity, and $\mathrm{ord}(M)$ to denote the order of the group M, if finite.

Proposition 4: *Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t]$, $\rho \neq 0$. Suppose that f has distinct roots $g,\ h \in \mathbb{C}^*$. Let $M = (s_n)_{n\in\mathbb{Z}} \leq \mathbb{C}^*$ be an f-sequence subgroup and write $s_n = \alpha g^n + \beta h^n$ for all n, for suitable $\alpha, \beta \in \mathbb{C}$. Suppose that either*
(1) $|g| \neq |h|$, *or*
(2) $|g| = |h| \neq 1$, *g/h is not a root of unity and $|\alpha| \neq |\beta|$.*
Then $\alpha\beta = 0$. Further, M is standard.

Proof: Suppose for a contradiction that $\alpha\beta \neq 0$. We may assume that $s_0 = 1$, while by Observation 3(c) we may also assume that $|g| \geq |h|$ and that $|g| > 1$. Write $\gamma = h/g$, so $0 < |\gamma| \leq 1$ and $s_m = g^m(\alpha + \beta\gamma^m)$. Suppose m is positive. Then $|(\alpha + \beta\gamma^m)|$ is bounded above by $|\alpha| + |\beta|$. If $|\gamma| < 1$ or if $|\gamma| = 1$ and $|\alpha| \neq |\beta|$ then $|(\alpha + \beta\gamma^m)|$ is bounded below (away from 0).

Now $s_m s_n \in M$ for all $m, n \in \mathbb{Z}$ because M is a group. Thus there exists a function $u : \mathbb{Z}^2 \to \mathbb{Z} : (m,n) \mapsto u(m,n)$ such that $s_m s_n = s_{u(m,n)}$ for all $m,\ n$. Thus, for all $m,\ n \in \mathbb{Z}$,

$$s_m s_n = g^{m+n}(\alpha + \beta\gamma^m)(\alpha + \beta\gamma^n) = g^{u(m,n)}(\alpha + \beta\gamma^{u(m,n)}). \tag{2}$$

The boundedness of $|\alpha+\beta\gamma^m|_{m>0}$ implies that $|g|^{m+n-u(m,n)}$ is bounded above and below whenever $m, n, u(m,n) \geq 0$. But $|g| > 1$ and so there exists a constant K such that

$$|m + n - u(m,n)| < K \tag{3}$$

whenever $m, n, u(m,n) \geq 0$.

Now fix $i \geq 0$ and suppose that $u(n+i, n-i) \geq 0$ for infinitely many n. By (3), there exists a fixed j with $|j| \leq K$ such that $u(n+i, n-i) = 2n + j$ for infinitely many n. Thus

$$s_{n+i}s_{n-i} = g^{2n}(\alpha + \beta\gamma^{n+i})(\alpha + \beta\gamma^{n-i}) = g^{2n+j}(\alpha + \beta\gamma^{2n+j}),$$

or

$$(\alpha^2 - \alpha g^i) + \alpha\beta(\gamma^i + \gamma^{-i})\gamma^n + (\beta^2 - \beta\gamma^j g^j)\gamma^{2n} = 0$$

for infinitely many n. Now $\alpha\beta \neq 0$, while $(\gamma^i + \gamma^{-i}) \neq 0$ because γ is not a root of unity. Thus, for infinitely many n, γ^n is a root of a fixed polynomial, independent of n, of degree either 1 or 2. Thus infinitely many of the γ^n must coincide, which is impossible because γ is neither zero nor a root of unity.

Thus for fixed $i \geq 0$, $u(n+i, n-i) < 0$ for all positive n but a finite number. Now (2) gives

$$g^{2n}(\alpha + \beta\gamma^{n+i})(\alpha + \beta\gamma^{n-i}) = h^{u(n+i,n-i)}(\alpha\gamma^{-u(n+i,n-i)} + \beta)$$

and so $|g|^{2n}|h|^{-u(n+i,n-i)}$ is bounded, independent of i and of n, provided just that $n > i \geq 0$ and $u(n+i, n-i) < 0$. But given $i \geq 0$, these conditions hold for infinitely many $n > i$, and so $|h| < 1$. It then follows that there exists a positive integer K_1 such that whenever $n > i \geq 0$ and $u(n+i, n-i) < 0$ we have

$$\left|\frac{u(n+i,n-i)}{2n} - \frac{\log|g|}{\log|h|}\right| < \frac{K_1}{2n}. \tag{4}$$

Let $\mathcal{R} = \{0, 1, \ldots, 4K_1 + 2\}$. For each $i \geq 0$, $u(n+i, n-i) < 0$ for all but finitely many positive n and so there exists N such that if $n > N$ we have $u(n+i, n-i) < 0$ for all $i \in \mathcal{R}$ simultaneously. Thus for distinct $i_1, i_2 \in \mathcal{R}$, (4) gives

$$|u(n+i_1, n-i_1) - u(n+i_2, n-i_2)| < 2K_1$$

whenever $n > N$. So for fixed $n_0 > N$, all integers $u(n_0+i, n_0-i)$ for $i \in \mathcal{R}$ belong to an interval of length at most $4K_1$ centered on $u(n_0, n_0)$. By the pigeon hole principle, there exist $i_1 \neq i_2$ such that $u(n_0+i_1, n_0-i_1) = u(n_0+i_2, n_0-i_2)$. Thus

$$s_{n_0+i_1}s_{n_0-i_1} = s_{n_0+i_2}s_{n_0-i_2}$$

and so

$$\alpha\beta(\gamma^{i_1}+\gamma^{-i_1})(gh)^{n_0}=\alpha\beta(\gamma^{i_2}+\gamma^{-i_2})(gh)^{n_0}.$$

Since $\alpha\beta gh\neq 0$, it follows that

$$\gamma^{i_1}-\gamma^{i_2}=\frac{\gamma^{i_1}-\gamma^{i_2}}{\gamma^{i_1}\gamma^{i_2}},$$

so that either $\gamma^{i_1}=\gamma^{i_2}$ or $\gamma^{i_1}\gamma^{i_2}=1$, both of which are impossible because γ is neither zero nor a root of unity. We conclude that $\alpha\beta=0$; it follows that M is standard. □

Lemma 5: *Let $f(t)=t^2-\sigma t-\rho\in\mathbb{C}[t]$, where $|\rho|=1$. Suppose that $f(t)$ has roots $g,h\in\mathbb{C}^*$. Let $M=(s_n)_{n\in\mathbb{Z}}\leq\mathbb{C}^*$ be an f-sequence subgroup.*
(a) *If $g\neq h$, then $|g|=|h|=1$ if and only if $|s|=1$ for all $s\in M$.*
(b) *If $g=h$, then $|g|=1$ and $|s|=1$ for all $s\in M$.*

Proof: (a) Suppose $g\neq h$. By Observation 3(a), there exist $\alpha,\beta\in\mathbb{C}$ with $s_n=\alpha g^n+\beta h^n$ for all $n\in\mathbb{Z}$. Now $|gh|=|\rho|=1$, so $|g|=1$ if and only if $|h|=1$. Suppose $|g|=|h|=1$ and that there exists $s\in M$ with $|s|\neq 1$. Then the cyclic subgroup $<s>\leq M$ contains elements of arbitrarily large modulus. But $|s_n|=|\alpha g^n+\beta h^n|\leq|\alpha|+|\beta|$ for all n, a contradiction.

Suppose next that $|s_n|=1$ for all $n\in\mathbb{Z}$. Assume $|g|>1$, so that $|h|<1$. If $\alpha=0$ then $\beta\neq 0$ and $1=|s_n|=|\beta h^n|$ for all n, which is absurd because β is fixed and $|h|<1$. Thus $\alpha\neq 0$. Now $||\alpha g^n|-|\beta h^n||\leq|\alpha g^n+\beta h^n|=|s_n|=1$. But $|\beta h^n|\leq|\beta|$, while $|\alpha g^n|$ is unbounded as n increases, a contradiction.
(b) Suppose $g=h\in\mathbb{C}^*$ is a double root of $f(t)$, so that $|g|=1$. By Observation 3(b), there exist $\alpha,\beta\in\mathbb{C}$ with $s_n=(\alpha+n\beta)g^n$ for all $n\in\mathbb{Z}$. As $0\notin M$ then not both α,β can be zero. Suppose there exists $s\in M$ with $|s|\neq 1$. Then the subgroup $<s>\leq M$ contains elements of arbitrarily small modulus. But $s_n=(\alpha+n\beta)g^n$, whence $|s_n|\geq||\alpha|-|n\beta||$. Since α,β are fixed and not both zero then $||\alpha|-|n\beta||\neq 0$ whenever $n\in\mathbb{Z}$ is such that $n|\beta|\neq|\alpha|$, and then

$$\{||\alpha|-|n\beta||:n\in\mathbb{Z},\ n|\beta|\neq|\alpha|\}$$

is bounded away from 0, a contradiction. □

Proposition 6: *Let $f(t)=t^2-\sigma t-\rho\in\mathbb{C}[t]$, where $\rho\neq 0$, and suppose that f has roots $g,h\in\mathbb{C}^*$. Let $M\leq\mathbb{C}^*$ be an f-sequence subgroup. Then*
(a) *If $|g|=|h|=1$ and $g\neq\pm h$ then M is standard.*
(b) *If $g=h$ then M is standard.*
(c) *If $g=-h$ then M is finite if and only if ρ is a root of unity.*
(d) *If $g=-h$ and if M is infinite then M has one of the forms:*

$$M=(\ldots,\rho^{-1},\varepsilon\rho^{k-1}\sqrt{\rho},1,\varepsilon\rho^{k}\sqrt{\rho},\rho,\ldots)\quad or$$
$$M=(\ldots,\rho^{-1},-\rho^{k-1},1,-\rho^{k},\rho,\ldots),$$

where $\varepsilon\in\{1,-1\}$ and $k\in\mathbb{Z}$. In the first case, $M=<\varepsilon\sqrt{\rho}>$ is cyclic and nonstandard of the first type. In the second case, $M=<-1>\times<\rho>$ is non-cyclic and nonstandard of the second type.
(e) *Suppose $g=-h$ and M is finite of order m. Write $r=$*ord(ρ),*by* (c).

If r is even then $m = 2r$ and M is nonstandard of the first type unless $\rho = -1$ when M is standard.

If r is odd then either $m = r$ and

$$M = (\dots, 1, \rho^{(r+1)/2}, \rho, \dots)$$

is standard, or else $m = 2r$ and

$$M = (\dots, 1, -g^j, g^2, \dots).$$

where $g = \rho^{(r+1)/2}$ and $1 \le j \le r$. Further, M is nonstandard of the first type unless $\rho = 1$, when M is standard.

Proof: Write $M = (s_n)_{n\in\mathbb{Z}}$. Without loss, suppose $s_0 = 1$.
(a) Suppose $|g| = |h| = 1$ and $g \neq \pm h$; then $\sigma \neq 0$ and $|\rho| = 1$. By Lemma 5, M lies on the unit circle.

Write $\tau = \sigma/2 \neq 0$. Then $\{g, h\} = \{\tau \pm \sqrt{\tau^2 + \rho}\}$ and $\tau^2 + \rho \neq 0$. If $u, v \in \mathbb{C}^*$ are such that $|u + v| = |u - v|$ then the segments $0u$ and $0v$ are perpendicular, whence $|u \pm v| = \sqrt{|u|^2 + |v|^2}$. Here, $|g| = |h| = 1 = \sqrt{|\tau^2| + |\tau^2 + \rho|}$, and so $1 = |\tau^2| + |\tau^2 + \rho|$. Then

$$1 = |\rho| = | \; -\tau^2 + \tau^2 + \rho| \le |\tau^2| + |\tau^2 + \rho| = 1,$$

whence $-\tau^2$ and $\tau^2 + \rho$ are parallel; that is, $\rho = k\tau^2$ where $k \in \mathbb{R}$ and $k < -1$. Thus, $|\tau| < 1$, so $0 < |\sigma| < 2$. Now $s_1 = \sigma 1 + \rho s_{-1}$ and because $|s_{-1}| = 1$, then $|s_1 - \sigma| = |\rho s_{-1}| = 1 = |s_1|$. But given a circle of radius 1, a fixed diameter l and $\lambda \in \mathbb{R}$ with $0 < \lambda < 2$, the circle has exactly two chords of length λ parallel to l. Thus, for σ fixed, there are just two $s \in \mathbb{C}$ such that $|s - \sigma| = |s| = 1$. But the roots $g \neq h$ of $f(t)$ satisfy $|g - \sigma| = |g| = |h - \sigma| = |h| = 1$. Thus the only f-sequence subgroups are $(\dots, 1, g, \dots)$ and $(\dots, 1, h, \dots)$, and M is standard in this case.
(b) Suppose that $g = h$. By Observation 3(b), there exist $\alpha, \beta \in \mathbb{C}$ with $s_n = g^n(\alpha + \beta n)$ for $n \in \mathbb{Z}$, while $\alpha = 1$ because $s_0 = 1$.

Suppose firstly that $|g| = 1$. Now $\sigma = 2g$ and $\rho = -g^2$, so $|\rho| = 1$ and then $|s| = 1$ for all $s \in M$ by Lemma 5(b). But $s_1 = 2g - g^2 s_{-1}$ because $s_0 = 1$. Thus, $|s_1 - 2g| = |g^2 s_{-1}| = 1$, so s_1 and $s_1 - 2g$ lie on the unit circle at distance $|2g| = 2$ from each other. Thus $s_1 = g$ and $M = (\dots, 1, g, \dots)$ is standard.

By Observation 3(c) we may now suppose $|g| > 1$. It is easy to check that

$$\lim_{n\to\infty} |s_n| = \infty \text{ and } \lim_{n\to\infty} |1 + \beta n|/|1 + \beta(n+1)| = 1;$$

in the second limit, the denominator is equal to $|s_{n+1}/g^{n+1}|$ and so is non-zero. Therefore there exists $N_1 \in \mathbb{N}$ such that both $|g| > |1+\beta n|/|1+\beta(n+1)|$ and $|s_n| > 1$ whenever $n > N_1$. Thus $|s_{n+1}| > |s_n| > 1$ for $n > N_1$. Similarly, there exists $N_2 \in \mathbb{N}$ such that $|s_{n-1}| < |s_n| < 1$ whenever $n < -N_2$ and so there exists $K \in \mathbb{N}$ with $K > N_1$ such that

$$|s_n| > \max\{|s_j|, 1/|s_j| : -N_2 \le j \le N_1\}$$

whenever $n \geq K$, in particular, $|s_K| > |s_j|$ if $j < K$. Thus, $s_K^{-1} = s_L$ for some $L < -N_2$. The monotonicity of $|s_n|$ with respect to n outside the interval $[-N_2, N_1]$ and the fact that M is a group now guarantee that $s_{K+j}^{-1} = s_{L-j}$ for all $j \in \mathbb{N}_0$. It follows that

$$g^{K+j}(\alpha + \beta(K+j))g^{L-j}(\alpha + \beta(L-j)) = 1, \ j = 0, 1, 2.$$

Simplification gives

$$g^{K+L}\beta^2 KL = g^{K+L}\beta^2(K+1)(L-1) = g^{K+L}\beta^2(K+2)(L-2).$$

Now $g \neq 0$ because $\rho \neq 0$. If $\beta \neq 0$ then both $L - K - 1 = 0$ and $2(L-K) - 4 = 0$, which is absurd. Thus $\beta = 0$ and M is standard, proving (b).

We now assume for the rest of the proof that $g = -h$, so that $\sigma = 0$, $f(t) = t^2 - \rho$, $g^2 = \rho$ and $\{g, h\} = \{\sqrt{\rho}, -\sqrt{\rho}\}$. Then $s_{n+2} = \rho s_n$ for all $n \in \mathbb{Z}$, and so $M = (\ldots, 1, x, \rho, x\rho, \ldots)$ where $x = s_1$: we will fix this interpretation for x.

(c) If M is infinite then $\rho^i \neq \rho^j$ whenever $i \neq j$ and so ρ is not a root of unity. If M is finite then the powers of ρ cannot be all distinct, whence ρ is a root of unity.

(d) Suppose that M is infinite. Then the elements ρ^j and $x\rho^j$ are all distinct as j runs over $\mathbb{Z}$. Now $x^2 \in M$ and so either $x^2 = x\rho^j$ or $x^2 = \rho^j$, for suitable j. If $x^2 = x\rho^j$ then $x = \rho^j$, contrary to distinctness; thus $x^2 = \rho^j$. There are two cases:

(1) Suppose $j = 2k+1$ is odd. Then $x = \varepsilon\rho^k\sqrt{\rho}$, where $\varepsilon \in \{1, -1\}$ and

$$M = (\ldots, \rho^{-1}, \varepsilon\rho^{k-1}\sqrt{\rho}, 1, \varepsilon\rho^k\sqrt{\rho}, \rho, \ldots).$$

We may shift the subsequence $(s_n)_{n \text{ odd}}$ relative to $(s_n)_{n \text{ even}}$ any number of places to the left or right and obtain different representations of M as an f-sequence: this corresponds to taking different values of k. With $k = 0$ we obtain a cyclic representation of M as an f-sequence, and so M is nonstandard of the first type.

(2) Suppose $j = 2k$ is even. Then $x \in \{\rho^k, -\rho^k\}$, whence $x = -\rho^k$ by distinctness. Then

$$M = (\ldots, \rho^{-1}, -\rho^{k-1}, 1, -\rho^k, \rho, \ldots),$$

so that $M = < -1 > \times < \rho >$ is a non-cyclic group; thus M is nonstandard of the second type.

(e) Suppose M is finite of order m. We have $\rho = g^2$, while $x^2 = \rho^j$ with $1 \leq j \leq r$ by distinctness. Thus $x = \varepsilon g^j$ where $\varepsilon \in \{-1, 1\}$, and so $s_{2k} = g^{2k}$ and $s_{2k+1} = \varepsilon g^{2k+j}$ for all k. Then

$$M = (\ldots, 1, \varepsilon g^j, g^2, \varepsilon g^{j+2}, \ldots, g^{2k}, \varepsilon g^{2k+j}, \ldots).$$

The distinct elements of M are just the terms from $s_0 = 1$ to s_{m-1}, where s_m is the first occurence of 1 after s_0.

Suppose firstly that r is even. Then $\varepsilon \in < \rho >$, $\text{ord}(g) = 2r$ and $< \rho >$ contains no odd power of g. Thus j is odd as otherwise $s_{2k+1} = \varepsilon g^{2k+j}$ would be an even power of g, against distinctness. But now $s_{2k+1} = \varepsilon g^{2k+j} \neq 1$ for all k, so s_{2r} is the first occurrence of 1 and $m = 2r$; we may shift $(s_n)_{n \text{ odd}}$ to obtain r distinct sequences, with that for $j = 1$ being cyclic. Thus M is nonstandard of the first type unless $r = 2$ when $M = (\ldots, 1, \varepsilon i, -1, -\varepsilon i, 1, \ldots)$ is standard.

Suppose next that r is odd. Then $-1 \notin < \rho >$ and $< \rho >$ contains a unique square-root of ρ, namely $\rho^{(r+1)/2}$. We may suppose that $g = \rho^{(r+1)/2}$; then ord(g) =ord$(\rho) = r$.

Suppose $\varepsilon = 1$. Then j is odd, by distinctness. Write $d = (r-j)/2 \geq 0$. Then $s_{2d+1} = g^{2d+j} = 1$ and this is evidently the first occurrence of 1 after s_0, whence $m = 2d+1$. But now $g^{2d+2} = s_{2d+2} = s_1 = g^j$ and so $r - j + 2 = 2d + 2 \equiv j (\mathrm{mod}\ r)$. It follows that $j = 1$, $m = r$ and

$$M = (\ldots, 1, g, g^2, \ldots) = (\ldots, 1, \rho^{(r+1)/2}, \rho, \ldots)$$

is standard.

Suppose $\varepsilon = -1$. As $g \in < \rho >$ but $-1 \notin < \rho >$ then no term $s_{2k+1} = -g^{2k+j}$ belongs to $< \rho >$; thus the first occurrence of 1 after s_0 is $s_{2r} = g^{2r} = 1$, and so $m = 2r$. Again we may shift $(s_n)_{n \text{ odd}}$ to obtain r distinct sequences, with that for $j = 1$ being cyclic, so that M is nonstandard of the first type unless $r = 1$ and $M = (\ldots, 1, -1, 1, \ldots)$, which is standard. □

Examples 7: (a) Let $f(t) = t^2 - 2$. As in Proposition 6(d), the following are f-sequence subgroups of $\mathbb{C}^*$, where $\varepsilon \in \{-1, 1\}$ and $k \in \mathbb{Z}$:

$$M_{1,\varepsilon} = (\ldots, 2^{-1}, \varepsilon 2^{k-1}\sqrt{2}, 1, \varepsilon 2^k \sqrt{2}, 2, \ldots) \text{ and}$$
$$M_2 = (\ldots, 2^{-1}, -2^{k-1}, 1, -2^k, 2, \ldots).$$

The groups $M_{1,\varepsilon} =< \varepsilon\sqrt{2} >$ are cyclic and nonstandard of the first type, while $M_2 =< -1 > \times < 2 >$ is non-cyclic and nonstandard of the second type.

(b) Let $f(t) = t^2 - \omega$ where $\omega = e^{2\pi i/3} \in \mathbb{C}$. As in Proposition 6(e), the following are f-sequence subgroups:

$$M_1 = (\ldots, 1, \omega^2, \omega, 1, \ldots), \text{ and}$$
$$M_{-1} = (\ldots, 1, -\omega^j, \omega, -\omega^{j+1}, \omega^2, -\omega^{j+2}, 1, \ldots), \text{ where } 1 \leq j \leq 3.$$

The group M_1, of order 3, is standard, while M_{-1}, of order 6, is nonstandard of the first type (because the sequence with $j = 2$ is cyclic).

(c) Let $f(t) = t^2 - i$. The following are f-sequence subgroups of $\mathbb{C}^*$:

$$M_\varepsilon = (\ldots, 1, \varepsilon i^l \sqrt{i}, i, \varepsilon i^{l+1}\sqrt{i}, -1, \varepsilon i^{l+2}\sqrt{i}, -i, \varepsilon i^{l+3}\sqrt{i}, \ldots),$$

where $\varepsilon \in \{1, -1\}$ and $1 \leq l \leq 4$. The sequences with $l = 4$ are cyclic and so each M_ε is nonstandard of the first type.

Lemma 8: *Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t]$, where $\rho \neq 0$, and suppose that f has roots $g, h \in \mathbb{C}^*$ with $|g| = |h| \neq 1, g \neq \pm h$. Suppose that $M = (s_n)_{n\in\mathbb{Z}}$ is an f-sequence subgroup of $\mathbb{C}^*$. Then M is infinite.*

Proof: By Observation 3(c), we may suppose that $|g| = |h| > 1$. Write $\gamma = h/g$; then $|\gamma| = 1$ but $\gamma \neq \pm 1$. By Observation 3(a), there exist $\alpha, \beta \in \mathbb{C}$ such that $s_n = g^n(\alpha + \beta\gamma^n)$ for $n \in \mathbb{Z}$. If M were finite then $1 = |s_n| = |g|^n |\alpha + \beta\gamma^n|$ for all n. But $|g|^n$ increases with n, and so $|\alpha + \beta\gamma^n|$ decreases. As n increases, the points $\alpha + \beta\gamma^n$ move (as $\gamma \neq 1$) around the circle with centre α and radius $|\beta|$. Thus $|\alpha + \beta\gamma^n|$ cannot decrease and so M cannot be finite. □

Proposition 9: *Let $f(t) = t^2 - \sigma t - \rho \in \mathbb{C}[t]$, where $\rho \neq 0$. Suppose M is a finite f-sequence subgroup of $\mathbb{C}^*$. Then M is standard unless both $\sigma = 0$ and $\mathrm{ord}(M)$ is even and at least 6, in which case it is nonstandard of the first type.*

Proof: The result follows from Propositions 4 and 6 together with Lemma 8. □

ACKNOWLEDGMENT

We thank the referee for valuable suggestions, including a simpler proof of Proposition 4.

The first author wishes to acknowledge the partial support of the "Centro de Estruturas Lineares e Combinatórias" and of the Praxis Program (Praxis/2/2.1/mat/73/94).

REFERENCES

[1] Owen J. Brison. "Complete Fibonacci Sequences in Finite Fields." *The Fibonacci Quarterly* **30** (1992): 295-304.

[2] Lawrence E. Somer. "The Fibonacci Group and a New Proof that $F_{p-(s/p)} \equiv 0 \pmod{p}$. *The Fibonacci Quarterly* **10** (1972): 345-348 and 354.

[3] Lawrence E. Somer. "Fibonacci-Like Groups and Periods of Fibonacci-Like Sequences." *The Fibonacci Quarterly* **15** (1977): 35-41.

AMS Classification Numbers: 11B37, 11B39

✠ ✠ ✠