

On some iterative roots on the circle

By PAWEŁ SOLARZ (Kraków)

Abstract. The aim of this paper is to investigate the problem of the existence of continuous iterative roots of a homeomorphism $F : S^1 \longrightarrow S^1$ such that $F^n = \text{id}_{S^1}$, where $n \geq 2$ is a fixed integer.

Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ be the unit circle with the positive orientation. Let $u, w, z \in S^1$, then there exist unique $t_1, t_2 \in [0, 1)$ such that $we^{2\pi it_1} = z$, $we^{2\pi it_2} = u$. Define

$$u \prec w \prec z \quad \text{if and only if} \quad 0 < t_1 < t_2$$

(see [1]). Moreover, if $u, w \in S^1$ and $u \neq w$, then there exist $t_w, t_u \in \mathbb{R}$ such that $t_u < t_w < t_u + 1$ and $e^{2\pi it_u} = u$, $e^{2\pi it_w} = w$. Put $\overrightarrow{(u, w)} := \{e^{2\pi it} : t \in (t_u, t_w)\}$ (resp. $\overleftarrow{(u, w)} := \{e^{2\pi it} : t \in \langle t_u, t_w \rangle\}$). This set is said to be an open arc (resp. a closed arc). Let $F : S^1 \longrightarrow S^1$ be a continuous mapping, then there exist a continuous function $f : \mathbb{R} \longrightarrow \mathbb{R}$ called a lift of F and an integer k such that $F(e^{2\pi ix}) = e^{2\pi if(x)}$ and $f(x+1) = f(x) + k$ for $x \in \mathbb{R}$. Moreover, if F is a homeomorphism, then so is f and $k = 1$ if f increases, $k = -1$ if f decreases (see [4] Chapter 2). We say that a homeomorphism F preserves orientation if f is increasing (reverses orientation if f is decreasing) (see for example [7]). Let $u, w, z \in S^1$ and $w \in \overrightarrow{(u, z)}$, then if F preserves orientation $F(w) \in \overrightarrow{(F(u), F(z))}$. However, if F reverses orientation, then we have $F(w) \in \overrightarrow{(F(z), F(u))}$.

Mathematics Subject Classification: Primary 39B12; Secondary 26A18.

Key words and phrases: lift, iterative root.

First we prove some properties of a homeomorphism $F : S^1 \longrightarrow S^1$ such that

$$F^n = \text{id}_{S^1}, \quad (1)$$

where n is a positive integer number.

Theorem 1. *Let $F : S^1 \longrightarrow S^1$ be an orientation-preserving homeomorphism satisfying (1) for an integer $n > 0$. If F has a fixed point, then $F(z) = z$ for all $z \in S^1$.*

PROOF. To obtain a contradiction, suppose that z_0 is a fixed point of F and there exist $z \in S^1$ and an integer r , $1 < r \leq n$ such that $z \neq F(z) \neq F^2(z) \neq \dots \neq F^{r-1}(z)$ and $F^r(z) = z$. Define $a_i \in \{z, F(z), \dots, F^{r-1}(z)\}$ for $i \in \{0, 1, \dots, r-1\}$ in the following manner $a_0 = z$ and

$$0 < \text{Arg} \frac{a_1}{a_0} < \text{Arg} \frac{a_2}{a_0} < \dots < \text{Arg} \frac{a_{r-1}}{a_0}.$$

Note that $F^i(z) \neq z_0$ for every $i \in \{0, 1, \dots, r-1\}$. Set $a_r := a_0$, therefore $z_0 \in \overrightarrow{(a_i, a_{i+1})}$ for some $i \in \{0, 1, \dots, r-1\}$. Because F preserves orientation we have

$$z_0 \in \overrightarrow{(F(a_i), F(a_{i+1}))}.$$

Thus

$$\overrightarrow{(a_i, a_{i+1})} \cap \overrightarrow{(F(a_i), F(a_{i+1}))} \neq \emptyset.$$

As $F(a_i) \neq a_i$ we obtain

$$\overrightarrow{(a_i, a_{i+1})} \neq \overrightarrow{(F(a_i), F(a_{i+1}))}$$

and consequently by the definition of a_i ,

$$\overrightarrow{(a_i, a_{i+1})} \subset \overrightarrow{(F(a_{i+1}), F(a_i))}.$$

Hence $a_i \in \overrightarrow{(F(a_i), F(a_{i+1}))}$, so $F^{-1}(a_i) \in \overrightarrow{(a_i, a_{i+1})}$, but $F^{-1}(a_i) = a_j$ for an $j \in \{0, 1, \dots, r-1\}$ and we have the contradiction. $\square$

As an immediate consequence of above theorem we have

Corollary 1. *If $F : S^1 \longrightarrow S^1$ is an orientation-preserving homeomorphism such that (1) holds for an integer $n \geq 2$ and $F \neq \text{id}_{S^1}$, then*

for every integer $m \geq 2$ there is no orientation-reversing homeomorphisms $\Phi : S^1 \longrightarrow S^1$ satisfying equation

$$\Phi^m = F. \quad (2)$$

PROOF. Suppose, contrary to our claim, that $\Phi^m(z) = F(z)$ for all $z \in S^1$. Hence $m = 2l$, where l is a positive integer. Let us observe that $\Phi^2 : S^1 \longrightarrow S^1$ preserves orientation and $(\Phi^2)^{ln} = \text{id}_{S^1}$. Moreover, Φ has a fixed point since its lift $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ is a decreasing homeomorphism, thus Φ^2 has a fixed point and by Theorem 1 $\Phi^2 = \text{id}_{S^1}$, which is impossible. $\square$

Corollary 2. Let $F : S^1 \longrightarrow S^1$ and $\Phi : S^1 \longrightarrow S^1$ be orientation-reversing homeomorphisms. Assume that (1) holds for some $n \geq 2$. If there exists $m \geq 2$ such that Φ satisfies (2), then $\Phi(z) = F(z)$ for all $z \in S^1$.

PROOF. Since $\Phi^m = F$ and F, Φ reverse orientation we get $m = 2l + 1$ for some integer l . On the other hand, there exists an integer k such that $n = 2k$. Thus

$$(\Phi^2)^{k(2l+1)} = \text{id}_{S^1},$$

so by Theorem 1 $\Phi^2 = \text{id}_{S^1}$, since similarly as in the previous proof Φ has a fixed point. Therefore, $F = \Phi^{2l+1} = \Phi^{2l} \circ \Phi = \Phi$. $\square$

We are left with the task of determining orientation-preserving solutions of the equation (2), where F is an orientation-preserving homeomorphism. The following remark is well known.

Remark 1. Let positive integers m, n fulfil $m < n$ and $\gcd(m, n) = 1$. Then there exists a unique $k \in \{1, \dots, n-1\}$ such that $1 = km \pmod{n}$.

Definition 1. Let integers q, n satisfy $1 \leq q < n$. By $\mathcal{M}_{q,n}$ define the set of all orientation-preserving homeomorphisms $F : S^1 \longrightarrow S^1$ such that

$$F(z) = \Psi^{-1} \left(e^{2\pi i \frac{q}{n}} \Psi(z) \right), \quad (3)$$

where $z \in S^1$ and $\Psi : S^1 \longrightarrow S^1$ is an orientation-preserving homeomorphism.

Remark 2. Suppose that $F \in \mathcal{M}_{q,n}$ and $F \in \mathcal{M}_{q',n}$, then $q = q'$.

PROOF. By Definition 1 we have

$$F(z) = \Psi^{-1} \left(e^{2\pi i \frac{q}{n}} \Psi(z) \right) = \Lambda^{-1} \left(e^{2\pi i \frac{q'}{n}} \Lambda(z) \right), \quad z \in S^1,$$

where $\Psi, \Lambda : S^1 \rightarrow S^1$ are orientation-preserving homeomorphisms. Thus $q = q' + jn$ for some integer j . But $0 < q < n$, so $q = q'$. $\square$

Remark 3. Let $F \in \mathcal{M}_{q,n}$, then n is the minimal number such that $F^n = \text{id}_{S^1}$ if and only if $\gcd(q, n) = 1$.

PROOF. Assume that $\gcd(q, n) = p > 1$. By Definition 1 we have

$$F(z) = \Psi^{-1} \left(e^{2\pi i \frac{q_1 p}{n_1 p}} \Psi(z) \right) = \Psi^{-1} \left(e^{2\pi i \frac{q_1}{n_1}} \Psi(z) \right), \quad z \in S^1,$$

where $\Psi : S^1 \rightarrow S^1$ is an orientation-preserving homeomorphism and $q = q_1 p$, $n = n_1 p$. Thus $F^{n_1} = \text{id}_{S^1}$ and $n_1 < n$. Conversely, let $\gcd(q, n) = 1$ and $F^k = \text{id}_{S^1}$ for some positive integer $k < n$. Hence

$$F^k(z) = \Psi^{-1} \left(e^{2\pi i \frac{qk}{n}} \Psi(z) \right) = z, \quad z \in S^1,$$

so the factor $\frac{kq}{n}$ is integer, which is impossible. $\square$

Proposition 1 (see [3]). Assume that $n \geq 2$ is an integer. For every homeomorphism $F : S^1 \rightarrow S^1$ without fixed points satisfying (1) there exists an integer q , $1 \leq q < n$ such that $F \in \mathcal{M}_{q,n}$.

Suppose that $F : S^1 \rightarrow S^1$ satisfies (1), where $n \geq 2$ is the minimal such a number. Then by Theorem 1 and Proposition 1 $F \in \mathcal{M}_{q,n}$ for some integer q such that

$$\gcd(q, n) = 1. \quad (4)$$

Fix a $b_0 \in S^1$, then from (3) $F^i(b_0) \neq F^j(b_0)$ for $i \neq j$, $i, j \in \{0, 1, \dots, n-1\}$. By (4) and Remark 1 we know that there exists a unique $d \in \{1, \dots, n-1\}$ such that $1 = qd \pmod{n}$. Define $b_k := F^{kd}(b_0)$ for $k \in \{1, \dots, n-1\}$. Using (3) we have

$$b_k = F^{kd}(b_0) = \Psi^{-1} \left(e^{2\pi i \frac{qkd}{n}} \Psi(b_0) \right) = \Psi^{-1} \left(e^{2\pi i \frac{k}{n}} \Psi(b_0) \right)$$

and, in consequence, since Ψ preserves orientation

$$\text{Arg} \frac{b_k}{b_0} < \text{Arg} \frac{b_{k+1}}{b_0}, \quad k \in \{0, 1, \dots, n-2\}. \quad (5)$$

Let $u : \{0, 1, \dots, n-1\} \longrightarrow \{0, 1, \dots, n-1\}$ be defined by

$$u(k) = (k + q) \pmod{n}.$$

Function u is a bijection. Moreover, $u(k+1) = u(k) + 1$ for $u(k) \neq n-1$ and $u(k+1) = 0$ for $u(k) = n-1$. Now, note that

$$F(b_k) = \Psi^{-1} \left(e^{2\pi i \frac{k+q}{n}} \Psi(b_0) \right) = b_{u(k)}, \quad k \in \{0, 1, \dots, n-1\} \quad (6)$$

and since F preserves orientation

$$F \left[\overrightarrow{(b_k, b_{k+1})} \right] = \overrightarrow{(F(b_k), F(b_{k+1}))} = \overrightarrow{(b_{u(k)}, b_{u(k+1)})} \quad (7)$$

for $k \in \{0, 1, \dots, n-2\}$. Thus we have proved the following

Lemma 1. *Let integers $1 \leq q < n$ be relatively prime and $F \in \mathcal{M}_{q,n}$. Then for every $b_0 \in S^1$ there exist unique $b_1, \dots, b_{n-1} \in S^1$ satisfying (5) and (6).*

Now note a few simple facts about an orientation-preserving homeomorphism $\Phi : S^1 \longrightarrow S^1$ satisfying (2), where $F \in \mathcal{M}_{q,n}$ and m is a positive integer.

Lemma 2. *Assume that $F \in \mathcal{M}_{q,n}$, where $1 \leq q < n$ are relatively prime. If an orientation-preserving homeomorphism $\Phi : S^1 \longrightarrow S^1$ satisfies (2) for some integer $m \geq 2$, then there exists a unique $j = j(\Phi) \in \{0, 1, \dots, m-1\}$ such that*

$$\Phi \in \mathcal{M}_{q+jn, mn}. \quad (8)$$

Moreover, m is the minimal number for which (2) holds if and only if $n > \gcd(q + jn, m)$.

PROOF. Note that $\Phi^{mn} = \text{id}_{S^1}$. Hence by Proposition 1 and Remark 2 $\Phi \in \mathcal{M}_{q', mn}$ for some unique $q' \in \{1, \dots, mn-1\}$. By Definition 1 and (2) we have

$$\Phi^m(z) = \Gamma^{-1} \left(e^{2\pi i \frac{q'}{n}} \Gamma(z) \right), \quad z \in S^1$$

and by (2) since $F \in \mathcal{M}_{q,n}$

$$e^{2\pi i \frac{q'}{n}} z = \Gamma \circ \Psi^{-1} \left(e^{2\pi i \frac{q}{n}} \Psi \circ \Gamma^{-1}(z) \right), \quad z \in S^1,$$

where $\Psi, \Gamma : S^1 \rightarrow S^1$ are orientation-preserving homeomorphisms. Thus $q' = q + jn$, for some $j \in \{0, \dots, m-1\}$. Hence, since q' is unique, we get that j is also unique.

Since $\gcd(q, n) = 1$ we have $\gcd(q + jn, n) = 1$ taking

$$k_\Phi = \frac{m}{\gcd(q + jn, m)} \quad (9)$$

and

$$q_\Phi = \frac{q + jn}{\gcd(q + jn, m)} \quad (10)$$

we obtain

$$\Phi \in \mathcal{M}_{q+jn, mn} = \mathcal{M}_{q_\Phi, k_\Phi n} \quad \text{and} \quad \gcd(q_\Phi, k_\Phi n) = 1.$$

From this and Remark 3 we get that

$$\Phi^{k_\Phi n} = \text{id}_{S^1} \quad (11)$$

and $k_\Phi n$ is the minimal number such that (11) holds.

Note that q_Φ, k_Φ do not depend on j and m . Indeed, if $\Phi \in \mathcal{M}_{q+j'n, m'n}$ for some $j' \in \{0, \dots, m'-1\}$, $j' \neq j$ and $m' \neq m$, then

$$\Phi \in \mathcal{M}_{q'_\Phi, k'_\Phi n} \quad \text{and} \quad \gcd(q'_\Phi, k'_\Phi n) = 1,$$

where

$$q'_\Phi = \frac{q + j'n}{\gcd(q + j'n, m')}, \quad k'_\Phi = \frac{m'}{\gcd(q + j'n, m')}.$$

It follows that $k'_\Phi n$ is the minimal number such that

$$\Phi^{k'_\Phi n} = \text{id}_{S^1},$$

thus $k'_\Phi = k_\Phi$ and by Remark 2 $q'_\Phi = q_\Phi$.

Now we can prove the second assertion. Suppose that $n \leq \gcd(q + jn, m)$. Of course, $n \neq \gcd(q + jn, m)$, since $\gcd(q + jn, n) = 1$. Consequently, from (9) $k_\Phi n < m$. On the other hand, by (11) and (2) we obtain

$$F(z) = \Phi^m(z) = \Phi^{k_\Phi n} \circ \Phi^{m-k_\Phi n}(z) = \Phi^{m-k_\Phi n}(z), \quad z \in S^1.$$

Conversely, suppose that there exists a positive integer $m' < m$ such that $\Phi^{m'}(z) = F(z)$ for $z \in S^1$. Consequently, by (2) we get

$$\Phi^{m-m'} = \text{id}_{S^1}.$$

Since $k_\Phi n$ is the minimal number such that (11) holds we get $m-m' \geq k_\Phi n$, so $m > k_\Phi n$. Hence by (9) $n < \gcd(q+jn, m)$. $\square$

Corollary 3. *Let F, Φ satisfy the assumptions of Lemma 2 and k_Φ be defined by (9), then*

$$m' := m - tk_\Phi n, \quad t = \left\lfloor \frac{m}{k_\Phi n} \right\rfloor, \quad (12)$$

where $[x]$ denotes the entire part of x , is the minimal number such that (2) holds.

PROOF. From (8) and (9) we obtain that Φ satisfies (11). Thus

$$F(z) = \Phi^m(z) = \Phi^{m'+tk_\Phi n}(z) = \Phi^{m'}(z), \quad z \in S^1.$$

Hence by Lemma 2 there exists $j' \in \{0, \dots, m' - 1\}$ such that $\Phi \in \mathcal{M}_{q+j'n, m'n}$. Similary as in the previous proof we get $k_\Phi = \frac{m'}{\gcd(q+j'n, m')}$. Moreover, by (12) $k_\Phi n > m'$, therefore $n > \gcd(q+j'n, m')$ and by Lemma 2 we get our claim. $\square$

The factor $\gcd(q+jn, m)$ has another property, it determines the number of solutions of the equation (2). Indeed, when $\gcd(q+jn, m) = m$ for some $j \in \{0, \dots, m-1\}$, then there is exactly one solution of (2). To show this fact we first prove the following

Lemma 3. *Let $(G, *)$ be a group, $a, b \in G$ be elements of order n , $n \geq 2$. If $a^m = b$ for some positive integer m , then there exists a unique $l \in \{1, \dots, n-1\}$ such that $b^l = a$.*

PROOF. Since b is an element of order n we have

$$b^i \neq b^j, \quad 1 \leq i < j \leq n-1.$$

Thus

$$a^{mi} \neq a^{mj}, \quad 1 \leq i < j \leq n-1,$$

but the order of a is n , so there exists $l \in \{1, \dots, n-1\}$ such that $a^{lm} = a$. $\square$

As a simple consequence of above lemma we have

Corollary 4. *Let $F \in \mathcal{M}_{q,n}$ and $\Phi \in \mathcal{M}_{q',n}$, where $\gcd(q, n) = \gcd(q', n) = 1$. Let (2) holds for some integer $m > 0$, then there exists an integer $l > 0$ such that*

$$\Phi(z) = F^l(z), \quad z \in S^1.$$

To avoid solutions described in Corollary 4 from now on we define the following set. Let integer q, n be such that $0 < q < n$, $\gcd(q, n) = 1$. For every $m \geq 2$ put

$$A_m := \{j \in \{0, \dots, m-1\} : \gcd(q + jn, m) \neq m\}. \quad (13)$$

Since $\gcd(n, q) = 1$, we get $\gcd(q + jn, m) < m$ for at least one $j \in \{0, \dots, m-1\}$, so $A_m \neq \emptyset$.

Let $F \in \mathcal{M}_{q,n}$, $\gcd(q, n) = 1$ and $j \in A_m$. By Remark 1 there exists a unique $d \in \{1, \dots, n-1\}$ such that $qd \equiv 1 \pmod{n}$. Set

$$k_j = \frac{m}{\gcd(q + jn, m)}. \quad (14)$$

Define the following sequence $(c_i)_{i \in \{0, \dots, k_j n - 1\}}$ satisfying two conditions

$$\begin{aligned} (G_1) \quad & c_0, c_1, \dots, c_{k_j-1} \in S^1 \text{ are arbitrary fixed and such that} \\ & c_0 \prec c_1 \prec \dots \prec c_{k_j-1} \text{ and } c_1, \dots, c_{k_j-1} \in \overrightarrow{(c_0, F^d(c_0))}, \\ (G_2) \quad & c_{i+k_j} = F^d(c_i) \text{ for } i \in \{0, \dots, k_j(n-1) - 1\}. \end{aligned}$$

Let $\{I_i\}_{i \in \{0, \dots, k_j n - 1\}}$ be a family of arcs such that

$$(H) \quad I_i := \overrightarrow{\langle c_{v^i(0)}, c_{v^i(1)} \rangle},$$

where $v(l) = (l + q_j) \pmod{k_j n}$, $l \in \{0, \dots, k_j n - 1\}$ and

$$q_j = \frac{q + jn}{\gcd(q + jn, m)}. \quad (15)$$

Now we can prove our main result.

Theorem 2. *Assume that $F \in \mathcal{M}_{q,n}$, $\gcd(q, n) = 1$, $m \geq 2$ and $j \in A_m$. Let $(c_i)_{i \in \{0, \dots, k_j n - 1\}}$ satisfies (G₁), (G₂), $\{I_i\}_{i \in \{0, \dots, k_j n - 1\}}$ fulfils (H)*

and $\Phi_i : I_i \longrightarrow I_{i+1}$ for $i \in \{0, \dots, k_j - 2\}$ be orientation-preserving homeomorphisms. Then there exists a unique orientation-preserving homeomorphism $\Phi : S^1 \longrightarrow S^1$ satisfying (2) and such that

$$\Phi|_{I_i} = \Phi_i \quad \text{for } i \in \{0, \dots, k_j - 2\}.$$

Moreover, $j = j(\Phi)$.

PROOF. Since $j \in A_m$, we have $k_j \neq 1$. Of course, by (14) and (15) $\gcd(k_j n, q_j) = 1$. It follows by (14) and (15) that

$$\frac{q_j}{q + jn} = \frac{k_j}{m},$$

thus

$$k_j q = m q_j \pmod{k_j n}. \quad (16)$$

Let

$$m' := m - t_j k_j n, \quad t_j = \left\lfloor \frac{m}{k_j n} \right\rfloor, \quad (17)$$

than $k_j n > m'$. By (17) and (16) we conclude that

$$k_j q = m' q_j \pmod{k_j n}. \quad (18)$$

Let $d \in \{1, \dots, n-1\}$ and $qd = 1 \pmod{n}$. From (G₂) and (1) we have

$$F^d(c_{i+k_j(n-1)}) = F^d \circ F^{d(n-1)}(c_i) = F^{dn}(c_i) = c_i$$

for $i \in \{0, \dots, k_j - 1\}$. From this and (G₂) it follows that

$$F^d(c_i) = c_{(i+k_j) \pmod{k_j n}}, \quad i \in \{0, \dots, k_j n - 1\}. \quad (19)$$

Hence since $qd = 1 \pmod{n}$ and $F^n = \text{id}_{S^1}$

$$F(c_i) = (F^d)^q(c_i) = c_{(i+k_j q) \pmod{k_j n}}, \quad i \in \{0, \dots, k_j n - 1\}. \quad (20)$$

Moreover, by (19), (G₁) and (G₂), since F^d preserves orientation, we get

$$\begin{aligned} c_0 < c_1 < \dots < c_{k_j-1} < F^d(c_0) = c_{k_j} < F^d(c_1) = c_{k_j+1} \\ < \dots < F^d(c_{k_j(n-1)-1}) = c_{k_j n-1} < F^d(c_{k_j(n-1)}) = c_0, \end{aligned}$$

thus

$$\operatorname{Arg} \frac{c_i}{c_0} < \operatorname{Arg} \frac{c_{i+1}}{c_0}, \quad i \in \{0, 1, \dots, k_j n - 2\}.$$

From (14) and (17) follows that there exists an integer h such that

$$m' = hk_j. \quad (21)$$

Since $k_j n > m'$ we conclude that $hk_j n > hm'$ and $n > h$. Put $h' := \gcd(m, q + jn)$. As $\gcd(n, q + jn) = 1$ we must have $\gcd(n, h') = 1$. On the other hand, by (17) $h = h' - t_j n$, so we see that $\gcd(h, n) = 1$. Thus from Remark 1 there exists a unique pair of integers a, a' such that

$$ah = a'n + 1. \quad (22)$$

Define

$$\Phi_i := F^a \circ \Phi_{i-k_j+1}^{-1} \circ \dots \circ \Phi_{i-2}^{-1} \circ \Phi_{i-1}^{-1} \quad (23)$$

for $i \in \{k_j - 1, k_j, \dots, k_j n - 1\}$. It is easy to see that Φ_i , defined above, preserve orientation. Next observe that, by (23) for $i \in \{k_j - 1, \dots, k_j n - 2\}$

$$\begin{aligned} \Phi_i[I_i] &= F^a[I_{i-k_j+1}] = F^a \left[\overrightarrow{\langle c_{v^{i-k_j+1}(0)}, c_{v^{i-k_j+1}(1)} \rangle} \right] \\ &= \overrightarrow{\langle F^a(c_{v^{i-k_j+1}(0)}), F^a(c_{v^{i-k_j+1}(1)}) \rangle}, \end{aligned}$$

but from the definition of v and (20) we get

$$F^a(c_{v^{i-k_j+1}(0)}) = c_{((i-k_j+1)q_j + ak_j q) \pmod{k_j n}}.$$

Applying (18) we see that

$$((i - k_j + 1)q_j + ak_j q) \pmod{k_j n} = ((i - k_j + 1)q_j + am'q_j) \pmod{k_j n}.$$

Hence by (21) and (22)

$$\begin{aligned} &((i - k_j + 1)q_j + am'q_j) \pmod{k_j n} \\ &= ((i - k_j + 1)q_j + k_j q_j + a'q_j k_j n) \pmod{k_j n} = ((i + 1)q_j) \pmod{k_j n}. \end{aligned}$$

Thus

$$F^a(c_{v^{i-k_j+1}(0)}) = c_{v^{i+1}(0)}.$$

Similary $F^a(c_{v^{i-k_j+1}(1)}) = c_{v^{i+1}(1)}$, so

$$\Phi_i[I_i] = I_{i+1}, \quad i \in \{k_j - 1, \dots, k_j n - 2\}. \quad (24)$$

In the same manner we can show that, if $i = k_j n - 1$ we get

$$\Phi_{k_j n - 1}[I_{k_j n - 1}] = I_0. \quad (25)$$

From (23) we have

$$F_{|I_{i+1}}^{-a} = \Phi_{i-k_j+1}^{-1} \circ \dots \circ \Phi_{i-2}^{-1} \circ \Phi_{i-1}^{-1} \circ \Phi_i^{-1} \quad (26)$$

for $i \in \{k_j - 1, \dots, k_j n - 1\}$. Fix an $i \in \{k_j, \dots, k_j n - 1\}$, thus combining (23) with (26) we obtain

$$\begin{aligned} \Phi_i &= F^a \circ \Phi_{i-k_j} \circ \Phi_{i-k_j}^{-1} \circ \Phi_{i-k_j+1}^{-1} \circ \dots \circ \Phi_{i-2}^{-1} \circ \Phi_{i-1}^{-1} \\ &= F^a \circ \Phi_{i-k_j} \circ F_{|I_i}^{-a}. \end{aligned} \quad (27)$$

We may write the index i in the form $i = pk_j + r$, where $p \geq 1$ is an integer and $r \in \{0, 1, \dots, k_j - 1\}$. Using (27) p times we get

$$\Phi_i = F^{pa} \circ \Phi_r \circ F_{|I_i}^{-pa} \quad (28)$$

for $i \in \{k_j, \dots, k_j n - 1\}$.

Define

$$\Phi(z) := \Phi_i(z) \quad z \in I_i, \quad i \in \{0, \dots, k_j n - 1\}. \quad (29)$$

It follows from the properties of Φ_i , $i \in \{0, \dots, k_j n - 1\}$ and the definition of I_i for $i \in \{0, \dots, k_j n - 1\}$ that Φ is an orientation-preserving homeomorphism. We next prove that $\Phi^m = F$. For this purpose note that from (26) we get

$$F_{|I_i}^a = \Phi_{i+k_j-1} \circ \dots \circ \Phi_{i+2} \circ \Phi_{i+1} \circ \Phi_i \quad (30)$$

for $i \in \{0, \dots, k_j(n-1)\}$. Now fix a $z \in I_l$, $l \in \{0, \dots, nk_j - m'\}$, then by (29), (30), (22) and (21) we obtain

$$\begin{aligned} \Phi^{m'}(z) &= (\Phi_{l+m'-1} \circ \dots \circ \Phi_{l+m'-k_j}) \circ (\Phi_{l+m'-k_j-1} \circ \dots \circ \Phi_{l+m'-2k_j}) \\ &\quad \circ \dots \circ (\Phi_{l+k_j-1} \circ \dots \circ \Phi_{l+1} \circ \Phi_l)(z) = F^{ah}(z) = F^{a'n+1}(z) \\ &= F(z). \end{aligned}$$

Let $l \in \{nk_j - m' + 1, \dots, k_j n - 1\}$ and $z \in I_l$, then by (24) and (25) we can get

$$\begin{aligned} \Phi^{m'}(z) &= \left(\Phi_{m'-k_j n+l-1} \circ \dots \circ \Phi_{m'-k_j(n+1)+l} \right) \circ \dots \circ \left(\Phi_{k_j-1} \circ \dots \circ \Phi_0 \right) \\ &\quad \circ \left(\Phi_{k_j n-1} \circ \dots \circ \Phi_{k_j(n-1)} \right) \circ \dots \circ \left(\Phi_{l+k_j-1} \circ \dots \circ \Phi_l \right)(z) \end{aligned}$$

or

$$\begin{aligned} \Phi^{m'}(z) &= \left(\Phi_{m'-k_j n+l-1} \circ \dots \circ \Phi_{m'-k_j(n+1)+l} \right) \\ &\quad \circ \dots \circ \left(\Phi_{r-1} \circ \dots \circ \Phi_0 \circ \Phi_{k_j n-1} \circ \dots \circ \Phi_{k_j(n-1)+r} \right) \\ &\quad \circ \dots \circ \left(\Phi_{l+k_j-1} \circ \dots \circ \Phi_l \right)(z), \end{aligned} \quad (31)$$

where $r \in \{1, 2, \dots, k_j - 1\}$. In the first case, similary as above, we have $\Phi^{m'}(z) = F(z)$, $z \in I_l$, straight from (30), (22) and (21). In the second case it suffices to show that $\Phi^{k_j}(z) = F^a(z)$, where $z \in I_{(n-1)k_j+r}$ for $r \in \{1, \dots, k_j - 1\}$, thus

$$\Phi^{k_j}(z) = \Phi_{r-1} \circ \Phi_{r-2} \circ \dots \circ \Phi_1 \circ \Phi_0 \circ \Phi_{k_j n-1} \circ \dots \circ \Phi_{k_j(n-1)+r}(z),$$

$$z \in I_{k_j(n-1)+r}.$$

Replacing all Φ_i for $i \in \{k_j(n-1)+r, \dots, k_j n - 1\}$ by (28) with $p = n-1$ we obtain

$$\begin{aligned} \Phi^{k_j}(z) &= \Phi_{r-1} \circ \Phi_{r-2} \circ \dots \circ \Phi_1 \circ \Phi_0 \circ F^{(n-1)a} \circ \Phi_{k_j-1} \circ F^{-(n-1)a} \\ &\quad \circ F^{(n-1)a} \circ \Phi_{k_j-2} \circ F^{-(n-1)a} \circ \dots \circ F^{(n-1)a} \circ \Phi_r \circ F^{-(n-1)a}(z) \\ &= \Phi_{r-1} \circ \Phi_{r-2} \circ \dots \circ \Phi_1 \circ \Phi_0 \circ F^{na} \circ F^{-a} \circ \Phi_{k_j-1} \circ \Phi_{k_j-2} \\ &\quad \circ \dots \circ \Phi_{r-1} \circ \Phi_r \circ F^{-(n-1)a}(z), \quad z \in I_{k_j(n-1)+r}. \end{aligned}$$

Now using (1) and (26) for $i = k_j - 1$ we get

$$\begin{aligned} \Phi^{k_j}(z) &= \left(\Phi_{r-1} \circ \Phi_{r-2} \circ \dots \circ \Phi_1 \circ \Phi_0 \circ \Phi_0^{-1} \circ \Phi_1^{-1} \circ \dots \circ \Phi_{r-1}^{-1} \right) \\ &\quad \circ \left(\Phi_r^{-1} \circ \dots \circ \Phi_{k_j-1}^{-1} \circ \Phi_{k_j-1} \circ \Phi_{k_j-2} \circ \dots \circ \Phi_r \right) \circ F^{-(n-1)a}(z) \\ &= F^{-(n-1)a}(z) = F^{-na} \circ F^a(z) = F^a(z), \quad z \in I_{k_j(n-1)+r}. \end{aligned}$$

Applying this and (30) to (31) in view of (21) and (22) we get $\Phi^{m'} = F$. From (30) and (29) we see that $F^a = \Phi^{k_j}$. Hence by (1)

$$\Phi^{k_j n} = F^{an} = \text{id}_{S^1}. \quad (32)$$

Finally, using (17) we have $\Phi^m = \Phi^{m'+k_j t_j n} = F$.

The proof is completed by showing that $j = j(\Phi)$. To do this note that (H), the definition of the function v and (31) give $\Phi \in \mathcal{M}_{q_j, k_j n}$ but according to (14) and (15) we obtain $\mathcal{M}_{q_j, k_j n} = \mathcal{M}_{q+jn, mn}$, so $j = j(\Phi)$. $\square$

Theorem 3. Let $F \in \mathcal{M}_{q, n}$, $\gcd(q, n) = 1$, $d \in \{1, \dots, n-1\}$ be such that $qd = 1 \pmod{n}$ and $\Phi: S^1 \rightarrow S^1$ be an orientation-preserving homeomorphism satisfying (2), where integer $m \geq 2$ is the minimal such a number and such that $\Phi^n \neq \text{id}_{S^1}$ or $\Phi^k = \text{id}_{S^1}$ for an integer $k < n$. Then for every $c_0 \in S^1$ there exists a sequence $c_1, \dots, c_{k_\Phi n-1} \in S^1$ fulfils $c_0 \prec c_1 \prec \dots \prec c_{k_\Phi n-1}$ and (G₂), where $k_j = k_\Phi$ and k_Φ is given by (9) for some $j = j(\Phi) \notin A_m$. Moreover, if $\{I_i\}_{i \in \{0, \dots, k_\Phi n-1\}}$ fulfils (H) with $q_j = q_\Phi$, then $\Phi[I_i] = I_{(i+1)}$, $i \in \{0, \dots, k_\Phi n-2\}$, $\Phi[I_{k_\Phi n-1}] = I_0$, and taking $\Phi_i := \Phi|_{I_i}$ we get

$$\Phi_i = F^a \circ \Phi_{i-k_\Phi+1}^{-1} \circ \dots \circ \Phi_{i-1}^{-1}$$

for $i \in \{k_\Phi - 1, \dots, k_\Phi n - 1\}$ and some integer a .

PROOF. From Lemma 2 we get $\Phi \in \mathcal{M}_{q+jn, mn}$ for some $j \in \{0, \dots, m-1\}$. Thus $\Phi \in \mathcal{M}_{q_\Phi, k_\Phi n}$, where $\gcd(q_\Phi, k_\Phi n) = 1$ and k_Φ, q_Φ are defined in (9) and (10). Fix a $c_0 \in S^1$. From Lemma 1 we get $c_0 \prec c_1 \prec \dots \prec c_{k_\Phi n-1} \prec c_0$ and

$$\Phi(c_i) = c_{(i+q_\Phi) \pmod{k_\Phi n}} \quad i \in \{0, \dots, k_\Phi n - 1\}.$$

It follows from (9) and (10) that $(mq_\Phi = k_\Phi q) \pmod{k_\Phi n}$, thus

$$F(c_i) = \Phi^m(c_i) = c_{(i+mq_\Phi) \pmod{k_\Phi n}} = c_{(i+k_\Phi q) \pmod{k_\Phi n}}$$

for $i \in \{0, \dots, k_\Phi n - 1\}$. Hence

$$F^d(c_i) = c_{(i+k_\Phi dq) \pmod{k_\Phi n}} = c_{(i+k_\Phi) \pmod{k_\Phi n}}, \quad i \in \{0, \dots, k_\Phi n - 1\},$$

as $k_\Phi dq = k_\Phi \pmod{k_\Phi n}$, so (G₂) holds. Moreover, by (7)

$$\begin{aligned} \Phi[I_i] &= \overrightarrow{\langle \Phi(c_{v^i(0)}), \Phi(c_{v^i(1)}) \rangle} = \overrightarrow{\langle \Phi(c_{v^{i+1}(0)}), \Phi(c_{v^{i+1}(1)}) \rangle} \\ &= I_{(i+1) \pmod{k_\Phi n}}, \quad i \in \{0, \dots, k_\Phi n - 1\}. \end{aligned}$$

Now let us observe that, since $\Phi^n \neq \text{id}_{S^1}$ we get $k_\Phi > 1$. On the other hand, from Lemma 2, as m is the minimal number such that (2) holds we have $k_\Phi n > m$. Thus, symilarly as in the proof of Theorem 2, we know that $ah = a'n + 1$ for some unique integer a , a' and $h = \frac{m}{k_\Phi}$. It follows from (2) that

$$\Phi^{k_\Phi h}(z) = F(z), \quad z \in S^1.$$

But $\Phi^{k_\Phi a'n} = \text{id}_{S^1}$ since $\Phi \in \mathcal{M}_{q_\Phi, k_\Phi n}$, thus

$$F^a(z) = \Phi^{k_\Phi ha}(z) = \Phi^{k_\Phi a'n + k_\Phi}(z) = \Phi^{k_\Phi}(z), \quad z \in S^1.$$

Using the definition of Φ_i we get

$$F^a(z) = \Phi_{i+k_\Phi-1} \circ \Phi_{i+k_\Phi-2} \circ \cdots \circ \Phi_i(z),$$

where $z \in I_i$, $i \in \{0, \dots, (n-1)k_\Phi\}$. Put $l := i + k_\Phi - 1$, then

$$\Phi_l(z) = F^a \circ \Phi_{l-k_\Phi+1}^{-1} \circ \cdots \circ \Phi_{l-2}^{-1} \circ \Phi_{l-1}^{-1}(z)$$

for $z \in I_l$ and $l \in \{k_\Phi - 1, \dots, k_\Phi n - 1\}$. This ends the proof. $\square$

Corollary 5. *Every orientation-preserving homeomorphic solution of (2) may be obtained in the manner described in proof of Theorem 2 or by Corollary 4.*

Theorem 4. *Let $F \in \mathcal{M}_{q,n}$ and $\gcd(q, n) = 1$. A homeomorphism $\Phi : S^1 \rightarrow S^1$ satisfies (2) for some integer $m \geq 2$ if and only if there exist $j \in \{0, \dots, m-1\}$ and an orientation-preserving homeomorphism $\gamma : \mathbb{R} \rightarrow \mathbb{R}$ such that*

$$\Phi(e^{2\pi i x}) = e^{2\pi i \gamma^{-1}\left(\frac{q+jn}{m} + \gamma(x)\right)}, \quad x \in \mathbb{R} \quad (33)$$

and γ is an increasing solution of

$$\gamma\left(f^p(x) - \frac{pq-1}{n}\right) = \gamma(x) + 1, \quad x \in \mathbb{R}, \quad (34)$$

where f is the lift of F such that $0 \leq f(0) < 1$, $p < n$ and $pq \equiv 1 \pmod{n}$.

PROOF. Since Φ fulfils (2), then by Lemma 2 there exists a unique $j \in \{0, \dots, m-1\}$ such that $\Phi \in \mathcal{M}_{q+jn, mn}$. Hence and from Definition 1

$$\Phi(z) = \Psi^{-1}\left(e^{2\pi i \frac{q+jn}{mn}} \Psi(z)\right), \quad z \in S^1, \quad (35)$$

where $\Psi : S^1 \longrightarrow S^1$ is an orientation-preserving homeomorphism. Using (2) once more we get

$$F(z) = \Psi^{-1} \left(e^{2\pi i \frac{q}{n}} \Psi(z) \right), \quad z \in S^1. \quad (36)$$

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be the lift of F such that $0 \leq f(0) < 1$, than by (36) we have

$$e^{2\pi i \psi(f(x))} = e^{2\pi i \psi(x) + \frac{q}{n}}, \quad x \in \mathbb{R} \quad (37)$$

and

$$\psi(f(x)) = \psi(x) + \frac{q}{n} + k, \quad x \in \mathbb{R}, \quad (38)$$

where k is an integer and $\psi : \mathbb{R} \longrightarrow \mathbb{R}$ is an increasing lift of Ψ such that

$$\psi(x+1) = \psi(x) + 1, \quad x \in \mathbb{R}. \quad (39)$$

Since $0 \leq f(0) < 1$ from the properties of ψ follows that $\psi(0) \leq \psi(f(0)) < \psi(1) = \psi(0) + 1$, thus

$$0 \leq \psi(f(0)) - \psi(0) < 1.$$

We conclude from this and (38) that $k = 0$. Therefore (38) gives

$$\psi(f(x)) = \psi(x) + \frac{q}{n}, \quad x \in \mathbb{R}. \quad (40)$$

Put

$$\gamma := n\psi, \quad (41)$$

then by (39) and (40) we have

$$\begin{aligned} \gamma(x+1) &= \gamma(x) + n, \quad x \in \mathbb{R}, \\ \gamma(f(x)) &= \gamma(x) + q, \quad x \in \mathbb{R}. \end{aligned} \quad (42)$$

According to Lemma 7 in [8] the above system of equations is equivalent to the equation (34), where $p < n$ is such that $pq \equiv 1 \pmod{n}$. It follows from (35) and (41) that Φ satisfies (33). Let us note that if $j \notin A_m$ i.e. $\gcd(q + jn, m) = m$, than $q + jn = mh$ for some integer h and (33) gives

$$\Phi(e^{2\pi i x}) = e^{2\pi i \gamma^{-1}(h + \gamma(x))}, \quad x \in \mathbb{R}.$$

Now suppose that Φ satisfies (33) and γ fulfils (34). Thus

$$\Phi^m(e^{2\pi i x}) = e^{2\pi i \gamma^{-1}(q + jn + \gamma(x))}, \quad x \in \mathbb{R}.$$

But (34) and (42) are equivalent, so using (42) we get

$$\Phi^m(e^{2\pi i x}) = e^{2\pi i \gamma^{-1}(q+\gamma(x))} = e^{2\pi i f(x)} = F(e^{2\pi i x}), \quad x \in \mathbb{R},$$

which proves the theorem. $\square$

ACKNOWLEDGEMENT. The author wishes to express his thanks to Professor M. C. ZDUN for suggesting the problem and for stimulating conversations.

References

- [1] M. BAJGER, On the structure of some flows on the unit circle, *Aequationes Math.* **55** (1998), 106–121.
- [2] K. CIEPLIŃSKI, On the embeddability of a homeomorphism of the unit circle in disjoint iteration groups, *Publ. Math. Debrecen* **55** (1999), 363–383.
- [3] K. CIEPLIŃSKI and M. C. ZDUN, On a system of Schröder equations on the circle (*to appear*).
- [4] I. P. CORNFELD, S. V. FOMIN and Y. G. SINAI, Ergodic theory, Grundlehren 245, *Springer Verlag, Berlin, Heidelberg, New York*, 1982.
- [5] M. KUCZMA, On the functional equation $\varphi^n(x) = g(x)$, *Ann. Polon. Math.* **11** (1961), 161–175.
- [6] M. KUCZMA, B. CHOCZEWSKI and R. GER, Iterative functional equations, Encyclopaedia of Mathematics and its Applications 32, *Cambridge Univ. Press, Cambridge, New York, Port Chester, Melbourne, Sydney*, 1990.
- [7] P. WALTERS, An Introduction to Ergodic Theory, Graduate Text in Mathematics, *Springer-Verlag, New York–Heidelberg–Berlin*, 1982.
- [8] M. C. ZDUN, On embedding of homeomorphisms of the circle in continuous flow, Iteration theory and its functional equations, (Proceedings, Schloss Hofen, 1984), Lecture Notes in Mathematics 1163, *Springer-Verlag, Heidelberg, New York*, 1985, 218–231.

PAWEŁ SOLARZ
 PEDAGOGICAL UNIVERSITY
 INSTITUTE OF MATHEMATICS
 UL. PODCHORĄŻYCH 2
 PL-30-084 KRAKÓW
 POLAND

E-mail: psolarz@wsp.krakow.pl

(Received July 4, 2002; revised January 3, 2003)