Semigroup Forum (2014) 88:67–75
DOI 10.1007/s00233-013-9501-z

RESEARCH ARTICLE

Semigroups whose endomorphisms are power functions

Ryszard Mazurek

Received: 21 February 2013 / Accepted: 4 May 2013 / Published online: 24 May 2013

Abstract For any commutative semigroup S and any positive integer m, the power function $f : S \to S$ defined by $f(x) = x^m$ is an endomorphism of S. In this paper we characterize finite cyclic semigroups as those finite commutative semigroups whose endomorphisms are power functions. We also prove that if S is a finite commutative semigroup with $1 \neq 0$, then every endomorphism of S preserving 1 and 0 is equal to a power function if and only if either S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined. Immediate consequences of the results are, on the one hand, a characterization of commutative rings whose multiplicative endomorphisms are power functions given by Greg Oman in the paper (Semigroup Forum, 86 (2013), 272–278), and on the other hand, a partial solution of Problem 1 posed by Oman in the same paper.

Keywords Cyclic semigroup · Semigroup endomorphism · Power function · Ring semigroup

1 Introduction

Let S be a commutative semigroup. A function $f : S \to S$ is called a *power function* if there exists a positive integer m such that $f(x) = x^m$ for all $x \in S$. It is easily seen that any power function is an endomorphism of the semigroup S.

In [4] Greg Oman studied commutative rings R with unity for which every endomorphism of the multiplicative semigroup $(R, \cdot)$ is equal to a power function (see [4,

Communicated by László Márki.

R. Mazurek (✉)
Faculty of Computer Science, Bialystok University of Technology, Wiejska 45A, 15-351 Białystok, Poland
e-mail: r.mazurek@pb.edu.pl

Introduction] for motivations for those studies). He proved in [4, Theorem 1] that every endomorphism of the semigroup $(R, \cdot)$ is a power function if and only if the ring R is a finite field. He also posed the natural problem [4, Problem 1] of characterizing the commutative semigroups S (with or without 0 or 1) with the property that every endomorphism of S is equal to a power function.

In this paper we solve the problem for finite semigroups. Namely, we prove that among finite commutative semigroups, cyclic semigroups are exactly those semigroups whose endomorphisms are power functions (see Theorem 2.2), extending to finite commutative semigroups a well-known characterization of finite cyclic groups via power functions. We also prove that for any finite commutative semigroup S with $1 \neq 0$, every endomorphism of S preserving 1 and 0 is equal to a power function if and only if either S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined (see Theorem 3.1). As an immediate consequence of the result we obtain Oman's aforementioned characterization of commutative rings whose multiplicative endomorphisms are power functions.

In this paper, in Sect. 2 semigroups are not assumed to have zero or identity, whereas in Sect. 3 we consider semigroups with zero 0 and identity 1. The set of positive integers is denoted by $\mathbb{N}$. If S is a semigroup and $t \in S$, then $\langle t \rangle$ denotes the subsemigroup of S generated by t, that is, $\langle t \rangle = \{t^n \mid n \in \mathbb{N}\}$, and tS^1 denotes the right ideal of S generated by t, that is, $tS^1 = \{t\} \cup tS$, where $tS = \{ts \mid s \in S\}$. A semigroup S is called a *cyclic* semigroup if S is generated by a single element, that is, $S = \langle t \rangle$ for some $t \in S$. An element s of a semigroup S with zero 0 is said to be *nilpotent* if $s^n = 0$ for some $n \in \mathbb{N}$, and a semigroup with zero is called a *nilsemigroup* if all its elements are nilpotent. If T is a nonempty subset of a semigroup S and $k \in \mathbb{N}$, then T^k denotes the set of all products $t_1 t_2 \cdots t_k$, where $t_1, t_2, \dots, t_k \in T$.

2 A characterization of finite cyclic semigroups

As the following result shows, finite cyclic groups are precisely those abelian groups whose endomorphisms are power functions.

Lemma 2.1 ([4, Lemma 1]) *Let G be an abelian group. Then G is a finite cyclic group if and only if every endomorphism $f : G \to G$ has the form $f(x) = x^m$ for some positive integer m.*

In Theorem 2.2 below we extend the above result to finite commutative semigroups, characterizing finite cyclic semigroups as those finite commutative semigroups whose endomorphisms are power functions. As we will see in Example 2.3, this characterization is no longer true for infinite commutative semigroups.

Theorem 2.2 *Let S be a finite commutative semigroup. Then S is a cyclic semigroup if and only if every endomorphism of S is equal to a power function.*

Proof To prove the "only if" part, assume that every endomorphism of S is equal to a power function. Since the semigroup S is finite, there exists an idempotent $e = e^2 \in S$.

Obviously, the function $f : S \to S$ defined by $f(x) = e$ is an endomorphism of S. Hence f is a power function and thus there exists $n \in \mathbb{N}$ such that

$$x^n = e \quad \text{for any } x \in S. \tag{2.1}$$

Note that a consequence of (2.1) is the following property of S:

$$\text{for any } x \in S, x \in xS \text{ implies } x \in eS. \tag{2.2}$$

Indeed, if $x \in xS$, then for some $y \in S$ we have $x = xy$, so $x = xy = (xy)y = xy^2 = (xy)y^2 = xy^3$, and continuing in this way we obtain $x = xy^n$. Hence (2.1) implies $x = xe \in eS$, as desired.

It is clear from (2.1) that e is the only idempotent of S. Furthermore, e is an identity of the subsemigroup eS of S and (2.1) shows that all elements of eS are invertible. Hence eS is a group. Moreover, if $f : eS \to eS$ is any endomorphism of the group eS, then the map $\widehat{f} : S \to S$ defined by $\widehat{f}(x) = f(ex)$ is an endomorphism of the semigroup S, and thus $\widehat{f}$ is a power function on S. Hence f is a power function on eS, which shows that all endomorphisms of the group eS are power functions. Thus Lemma 2.1 implies that eS is a finite cyclic group. Therefore, if $S = eS$, then S is a cyclic semigroup.

We are left with the case where $eS \subsetneq S$. We show that $S^2 \subsetneq S$ in this case. First, we claim that

$$\text{for any } x \in S^2 \setminus eS \text{ there exists } y \in S \setminus eS \text{ such that } xS^1 \subsetneq yS^1. \tag{2.3}$$

Indeed, since $x \in S^2$, for some $y \in S$ we have $x \in yS$. Clearly $xS^1 \subseteq yS^1$, and since $x \notin eS$, also $y \notin eS$. If $y \in xS^1$, then from $x \in yS$ it follows that $x \in xS$ and (2.2) implies $x \in eS$, a contradiction. Hence $xS^1 \subsetneq yS^1$, which proves our claim (2.3). Now, if $S = S^2$, then starting from any element $x \in S \setminus eS$ and using (2.3) repeatedly, we get an infinite strictly increasing chain $xS^1 \subsetneq x_1S^1 \subsetneq x_2S^1 \subsetneq \ldots$ of subsets of S, which contradicts S being finite. Hence $S^2 \subsetneq S$.

Since $eS \subseteq S^2 \subsetneq S$, it follows from (2.1) that there exists a smallest positive integer k such that $a^k \notin eS$ and $a^{k+1} \in eS$ for some $a \in S \setminus S^2$. We will show that such an element a generates S. We first show that the following function $g : S \to S$ is an endomorphism of S:

$$g(x) = \begin{cases} a^k & \text{if } x = a \\ ex^k & \text{if } x \neq a. \end{cases} \tag{2.4}$$

Note that since $a \notin S^2$, for any $x, y \in S$ we have $xy \neq a$ and thus $g(xy) = e(xy)^k$. Hence to show that g is an endomorphism of S, it suffices to show that $g(x)g(y) = e(xy)^k$ for any $x, y \in S$. Since $2k \geq k + 1$ and $a^{k+1} \in eS$, $a^{2k} \in eS$ and thus $a^{2k} = ea^{2k}$. Hence, if $x = y = a$, then $g(x)g(y) = g(a)g(a) = a^{2k} = ea^{2k} = e(aa)^k = g(xy)$. The remaining cases (where $x \neq a$ or $y \neq a$) are easy to verify.

Since g is an endomorphism of S, g is a power function and thus there exists $m \in \mathbb{N}$ such that $g(x) = x^m$ for any $x \in S$. If $k < m$, then $a^k = g(a) = a^m = a^k a^{m-k} \in a^k S$, and from (2.2) we obtain $a^k \in eS$, a contradiction. If $k > m$, then $a^m = a^k = a^m a^{k-m} \in a^m S$, so $a^k = a^m \in eS$ by (2.2), again a contradiction. Hence, it must be that $k=m$ and thus $x^k=g(x)$ for any $x\in S$. Now we infer from the definition of g that $x^k\in eS$ for every $x\in S\setminus\{a\}$, and consequently it follows from our choice of k that

$$S\setminus\{a\}\subseteq S^2. \tag{2.5}$$

The observation (2.5) will help us to prove that the element a generates the semigroup S, i.e., $S=\langle a\rangle$. We first show that

$$S\setminus eS\subseteq\langle a\rangle. \tag{2.6}$$

Suppose towards a contradiction that there exists $x\in S\setminus eS$ such that $x\notin\langle a\rangle$. Then $x\neq a$ and by (2.5) we have $x=b_1b_2\in S^2$ for some $b_1,b_2\in S$. Since $x\notin\langle a\rangle$, it follows that $b_1\neq a$ or $b_2\neq a$. Hence (2.5) implies that $b_1\in S^2$ or $b_2\in S^2$, and thus $x\in S^3$. Consequently, $x=c_1c_2c_3$ for some $c_1,c_2,c_3\in S$. Since $x\notin\langle a\rangle$, for some $i\in\{1,2,3\}$ we have $c_i\neq a$, which, together with (2.5), implies that $x\in S^4$. Continuing in this manner, we see that $x\in S^d$ for any $d\in\mathbb{N}$. Now take $d=nc$, where n satisfies (2.1) and c is the cardinality of S. Then in any product $y_1y_2\cdots y_d$ of d elements of S, at least n of the elements $y_1,y_2,\dots,y_d$ have to be equal, and (2.1) implies that $y_1y_2\cdots y_d\in eS$. Hence $S^d\subseteq eS$, but this is impossible because $x\in S^d$ and $x\notin eS$. This contradiction establishes the containment (2.6).

We continue with the proof that $S=\langle a\rangle$. Suppose, to derive a contradiction, that $S\neq\langle a\rangle$. Then (2.6) implies $eS\nsubseteq\langle a\rangle$. Since eS is a cyclic group, we can choose a generator q of this group, and since $eS\nsubseteq\langle a\rangle$, it follows that $q\notin\langle a\rangle$. We claim that

$$\text{for any positive integer } j,\ a^j=e \text{ implies } q^j=e. \tag{2.7}$$

To prove (2.7), assume that $a^j=e$ and consider the following function $h:S\to S$:

$$h(x)=\begin{cases} x & \text{if } x\in\langle a\rangle\\ x^{j+1} & \text{if } x\notin\langle a\rangle.\end{cases}$$

Since S is commutative, to verify that h is an endomorphism of S, it suffices to consider the following three cases. When considering these cases, let us remember that $x^j=e$ for any $x\in\langle a\rangle$ (which is a consequence of $a^j=e$) and that $x=ex$ for any $x\notin\langle a\rangle$ (which is a consequence of (2.6)).

Case 1: $x,y\in\langle a\rangle$. Then $xy\in\langle a\rangle$, so $h(xy)=xy=h(x)h(y)$.

Case 2: $x\in\langle a\rangle$, $y\notin\langle a\rangle$. Then $xy\notin\langle a\rangle$. Indeed, otherwise $xy=a^i$ for some $i\in\mathbb{N}$. Since $x\in\langle a\rangle$, we have $x=a^p$ for some $p\in\mathbb{N}$ and using that $a^j=e$, we get $xa^l=e$ for some $l\in\mathbb{N}$. Hence $ey=xa^ly=(xy)a^l=a^ia^l=a^{i+l}$. But $y\notin\langle a\rangle$ and thus $y=ey$. Hence we obtain $y=a^{i+l}\in\langle a\rangle$, and this contradiction shows that $xy\notin\langle a\rangle$. Thus $h(xy)=(xy)^{j+1}=x^jxy^{j+1}=exy^{j+1}=x(ey)^{j+1}=xy^{j+1}=h(x)h(y)$.

Case 3: $x\notin\langle a\rangle$, $y\notin\langle a\rangle$. If $xy\in\langle a\rangle$, then $(xy)^j=e$ and since $x=ex$, we obtain $h(xy)=xy=exy=(xy)^jxy=x^{j+1}y^{j+1}=h(x)h(y)$. If $xy\notin\langle a\rangle$, then $h(xy)=(xy)^{j+1}=x^{j+1}y^{j+1}=h(x)h(y)$.

We have shown that h is an endomorphism of S. Hence h is a power function, and thus there exists $m\in\mathbb{N}$ such that $h(x)=x^m$ for any $x\in S$. If $m\geq 2$, then $a=h(a)=a^m\in aS$ and thus $a\in eS$ by (2.2), a contradiction with our choice of a. Hence $m=1$ and since $q\notin\langle a\rangle$, we obtain $q^{j+1}=h(q)=q$, which implies $q^j=e$, proving (2.7).

We now come to the required contradiction. Let t be the smallest positive integer such that $a^t = a^r$ for some positive integer $r < t$, and let $w = t - r$. Then

$$G = \{a^r, a^{r+1}, a^{r+2}, \ldots, a^{r+w-1}\}$$

is a group of order w. Since e is the unique idempotent of S, it follows that e is the identity element of G and thus G is a subgroup of the group eS. Since e is the identity element of G, we have $a^u = e$ for some $u \in \{r, r+2, \ldots, r+w-1\}$ and from $a^t = a^r$ it follows that also $a^{u+w} = e$. Hence (2.7) implies that $q^u = e$ and $q^{u+w} = e$, and thus $q^w = q^{u+w}q^{-u} = e$. Since q is a generator of the group eS, and $q^w = e$, and w is the order of the group G, it follows that $eS = G$. But obviously $G \subseteq \langle a\rangle$, so we obtain $eS \subseteq \langle a\rangle$ and this contradiction completes the proof of the "only if" part of the theorem.

Now we prove the "if" part. Let S be a cyclic semigroup, let z be a generator of S, and let $f : S \to S$ be any endomorphism of the semigroup S. Then $f(z) = z^m$ for some positive integer m. Now, if x is any element of S, then $x = z^i$ for some $i \in \mathbb{N}$ and thus $f(x) = f(z^i) = f(z)^i = (z^m)^i = (z^i)^m = x^m$. Hence f is a power function. □

As we have just proved in Theorem 2.2, every finite commutative semigroup S whose endomorphisms are power functions must be cyclic, that is, S is generated by a single element x subject to a defining relation of the form $x^i = x^j$ with $i \neq j \in \mathbb{N}$. The example below shows that Theorem 2.2 cannot be extended to infinite commutative semigroups.

Example 2.3 Let S be the multiplicative semigroup consisting of the numbers

$$2^2, 2^3, 2^4, 2^5, \ldots,$$

that is, $S = \{2^n \mid n \in \mathbb{N}, n \geq 2\}$. Clearly, the semigroup S is not cyclic.

We show that every endomorphism of the semigroup S is equal to a power function. Let $f : S \to S$ be any endomorphism of S. Then $f(2^2) = 2^k$ and $f(2^3) = 2^n$ for some $k, n \in \mathbb{N}$. Since $f(2^6) = f(2^2)^3 = 2^{3k}$ and $f(2^6) = f(2^3)^2 = 2^{2n}$, it follows that $3k = 2n$, and consequently $k = 2m$ and $n = 3m$ for some $m \in \mathbb{N}$. Hence for any $i \in \mathbb{N}$ we have $f(2^{2i}) = f(2^2)^i = (2^k)^i = (2^{2m})^i = (2^{2i})^m$ and thus $f(x) = x^m$ for all numbers in S of the form 2^t with t even. Furthermore $f(2^3) = (2^3)^m$ and thus for any $i \in \mathbb{N}$ we have $f(2^{3+2i}) = f(2^3)f(2^{2i}) = (2^3)^m(2^{2i})^m = (2^{3+2i})^m$, which shows that also $f(x) = x^m$ for all numbers in S of the form 2^t with t odd. Hence f is a power function.

3 A characterization of finite commutative semigroups with $1 \neq 0$ whose endomorphisms preserving 0 and 1 are power functions

As we mentioned in the Introduction, the main motivation for this paper was Oman's problem of characterizing the commutative semigroups (with or without 0 or 1) whose endomorphisms are power functions. In Theorem 2.2 we solved the problem for finite commutative semigroups S, with no assumptions about the existence 0 or 1 in S. It is also clear from the proof of Theorem 2.2 that if S is a finite commutative semigroup, then

- if S has an identity 1, then all endomorphisms of S are power functions if and only if S is a cyclic group;
- if S has a zero 0, then all endomorphisms of S are power functions if and only if S is a cyclic nilsemigroup.

To give a complete solution of Oman's problem for finite commutative semigroups, in this section we consider the remaining case where the semigroups have both an identity 1 and a zero 0. In fact, just commutative semigroups with 1 and 0 are closest to the context of Oman's paper [4], where multiplicative semigroups of commutative rings with unity were studied (obviously, every such multiplicative semigroup has 1 and 0).

To state the main result of this section, which solves Oman's problem for finite commutative semigroups with 1 and 0, we introduce the following terminology. If S is a semigroup with identity 1 and zero 0, then we say that an endomorphism $f : S \to S$ of S *preserves* 0 *and* 1 if f satisfies the conditions $f(0) = 0$ and $f(1) = 1$. We say that a semigroup S is a *cyclic group with zero adjoined* if S is the result of adjoining a zero to a cyclic group. In other words, S is a cyclic group with zero adjoined if S is a semigroup with zero 0 and $S \setminus \{0\}$ is a cyclic group. A semigroup S is called a *cyclic nilsemigroup with identity adjoined* if S is the result of adjoining an identity to a cyclic nilsemigroup. Hence, a semigroup S is a cyclic nilsemigroup with identity adjoined if S has an identity 1 and $S \setminus \{1\}$ is a cyclic nilsemigroup.

Theorem 3.1 *Let S be a finite commutative semigroup with $1 \neq 0$. Then every endomorphism of S preserving* 0 *and* 1 *is equal to a power function if and only if either S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined.*

Proof Throughout the proof U will denote the group of invertible elements of the semigroup S.

To prove the "only if" part of the theorem, assume that every endomorphism of S preserving 0 and 1 is equal to a power function. Let $T = S \setminus U$, i.e., T is the subsemigroup of S consisting of all noninvertible elements of S. The function $f : S \to S$ defined by

$$f(x) = \begin{cases} 1 & \text{if } x \in U, \\ 0 & \text{if } x \in T, \end{cases}$$

is easily seen to be an endomorphism of S preserving 0 and 1, and thus there exists a positive integer n such that

$$x^n = 0 \quad \text{for any } x \in T. \tag{3.1}$$

Hence, since T is finite and commutative, $T^d = \{0\}$ for some positive integer d (e.g. for $d = nc$, where n satisfies (3.1) and c is the cardinality of T).

If $T = T^2$, then $T = T^2 = T^3 = \cdots = T^d = \{0\}$ and thus $S = U \cup \{0\}$. Furthermore, if $f : U \to U$ is an arbitrary endomorphism of the group U, then the map $\widehat{f} : S \to S$ defined by $\widehat{f}(x) = f(x)$ for $x \in U$ and $\widehat{f}(0) = 0$, is an endomorphism of the semigroup S preserving 0 and 1. Hence $\widehat{f}$ is a power function of S, and consequently f is a power function of U. Thus every endomorphism of the group U is a power function, so Lemma 2.1 implies that U is a finite cyclic group. Therefore, in this case $S = U \cup \{0\}$ is a finite cyclic group with zero adjoined.

Now we consider the remaining case where $T \neq T^2$, that is, $T^2 \subsetneq T$. Since $x^n = 0$ for any $x \in T$, there exists a smallest positive integer k such that $a^k \neq 0$ and $a^{k+1} = 0$ for some $a \in T \setminus T^2$. For this a and any positive integer i we set $a^i U = \{a^i u : u \in U\}$. We claim that

$$\text{for any positive integers } i, j, \text{ if } a^i \neq 0, a^j \neq 0 \text{ and } i \neq j, \text{ then } a^i U \cap a^j U = \emptyset. \tag{3.2}$$

To see this, assume that $a^i \neq 0$, $a^j \neq 0$ and $i \neq j$, but $a^i U \cap a^j U \neq \emptyset$. Then $a^i u = a^j v$ for some $u, v \in U$. Without loss of generality we may assume that $i < j$. Then $a^i = a^j v u^{-1} = a^i t$ with $t = a^{j-i} v u^{-1}$, and an easy induction argument shows that $a^i = a^i t^l$ for any $l \in \mathbb{N}$. Since by (3.1) the element t is nilpotent, we obtain $a^i = 0$ and this contradiction completes the proof of (3.2).

Set $C = T \setminus aU$ and define $g : S \to S$ as follows:

$$g(x) = \begin{cases} 1 & \text{if } x \in U, \\ a^k & \text{if } x \in aU, \\ 0 & \text{if } x \in C = T \setminus aU. \end{cases}$$

It is clear that the sets U, aU and $C = T \setminus aU$ are pairwise disjoint and $S = U \cup aU \cup C$, so g is well defined. It is also clear that $g(1) = 1$. To show that g is an endomorphism of S, we first observe that

$$T^2 \subseteq C. \tag{3.3}$$

Indeed, if $T^2 \nsubseteq C$, then since $T^2 \subseteq T$, there exist $t_1, t_2 \in T$ with $t_1 t_2 \in aU$, that is, $t_1 t_2 = au$ for some $u \in U$. Hence $a = t_1(t_2 u^{-1}) \in T^2$, and this contradiction proves (3.3). Note that (3.3) implies also that $g(0) = 0$.

We are now ready to show that $g(xy) = g(x)g(y)$ for any $x, y \in S$. For this, since S is commutative, it suffices to consider the following four cases.

Case 1: $x, y \in T$. Then $xy \in C$ by (3.3), and thus $g(xy) = 0$. On the other hand, from the definition of g it follows that $g(x), g(y) \in \{0, a^k\}$, and since $a^{k+1} = 0$, we obtain $g(x)g(y) = 0 = g(xy)$ in this case.

Case 2: $x, y \in U$. Then $xy \in U$, so $g(xy) = 1 = 1 \cdot 1 = g(x)g(y)$.

Case 3: $x \in U$, $y \in aU$. Then $xy \in aU$, so $g(xy) = a^k = 1 \cdot a^k = g(x)g(y)$.

Case 4: $x \in U$, $y \in C$. Then $xy \in C$, so $g(xy) = 0 = 1 \cdot 0 = g(x)g(y)$.

As we have just shown, g is an endomorphism of S preserving 0 and 1, and thus there exists a positive integer m such that $g(x) = x^m$ for every $x \in S$. In particular, $a^k = g(a) = a^m$, and since $a^k \neq 0$, (3.2) implies that $k = m$. Hence we conclude from the definition of g that $x^k = 0$ for every $x \in C$, and consequently it follows from our choice of k that $C \subseteq T^2$. Combining this with (3.3), we obtain $T^2 = C = T \setminus aU$ and thus

$$T \setminus T^2 = aU. \tag{3.4}$$

Now it is clear that

$$T^p \setminus T^{p+1} \subseteq a^p U \quad \text{for any positive integer } p. \tag{3.5}$$

In particular, $T^{k+1} \setminus T^{k+2} \subseteq a^{k+1}U = \{0\}$ and thus $T^{k+1} = T^{k+2}$. Hence $T^{k+1} = T^l$ for any $l \in \mathbb{N}$ such that $l \geq k+1$, and since $T^d = \{0\}$, it follows that $T^{k+1} = \{0\} = a^{k+1}U$. This and (3.5) show that

$$T^2 \setminus T^3 \subseteq a^2U, T^3 \setminus T^4 \subseteq a^3U, \ldots, T^k \setminus T^{k+1} \subseteq a^kU, T^{k+1} = a^{k+1}U = \{0\}. \tag{3.6}$$

Combining (3.6) with (3.4) we conclude that $T = aU \cup a^2U \cup a^3U \cup \cdots \cup a^kU \cup a^{k+1}U$. Now we define the following function h on S:

$$h(x) = \begin{cases} 1 & \text{if } x \in U, \\ a^i & \text{if } x \in a^iU \text{ for some positive integer } i \leq k+1. \end{cases}$$

From (3.2) it follows that the sets $U, aU, a^2U, a^3U, \ldots, a^kU, a^{k+1}U$ are pairwise disjoint and thus h is well-defined. Since obviously h is an endomorphism of S preserving 0 and 1, there exists a positive integer m such that $h(x) = x^m$ for every $x \in S$. In particular, $a^m = h(a) = a$, so (3.2) implies that $m = 1$. Hence it follows from the definition of h that $U = \{1\}$, and thus

$$S = U \cup aU \cup a^2U \cup \cdots \cup a^kU \cup a^{k+1}U = \{1\} \cup \left\{a, a^2, a^3, \ldots, a^k, a^{k+1}\right\},$$

where $a^{k+1} = 0$. Therefore, S is a cyclic nilsemigroup with identity adjoined.

Now we prove the "if" part of the theorem. We first consider the case where the semigroup S is a finite cyclic group with zero adjoined, that is, $U = S \setminus \{0\}$ and the group U is finite and cyclic. If $f : S \to S$ is an endomorphism of the semigroup S preserving 0 and 1, then $f(1) = 1 \neq 0$, which implies that $f(U) \subseteq U$. Hence the restriction $\bar{f}$ of f to U is an endomorphism of the group U, and thus it follows from Lemma 2.1 that $\bar{f}$ is a power function of U. Therefore, f is a power function of S, as desired.

We are left with the case where S is a cyclic nilsemigroup with identity adjoined. Then there exists a nilpotent element $a \in S$ such that all elements of $S \setminus \{1\}$ are of the form a^i, where i is a positive integer. Let $f : S \to S$ be an arbitrary endomorphism of S preserving 0 and 1. Since a is nilpotent and $f(0) = 0 \neq 1$, it follows that $f(a) \neq 1$ and thus $f(a) = a^m$ for some positive integer m. Hence if $x \in S \setminus \{1\}$, then $x = a^i$ for some $i \in \mathbb{N}$, and thus

$$f(x) = f\left(a^i\right) = f(a)^i = \left(a^m\right)^i = \left(a^i\right)^m = x^m.$$

Since furthermore $f(1) = 1 = 1^m$, f is a power function. $\square$

Recall that a semigroup $(S, \cdot)$ is said to be a *ring semigroup* provided that there exists an addition $+$ on S such that $(S, +, \cdot)$ is a ring. Such semigroups are well studied in the literature. We refer the reader to [1–3] and [5] for sampling of what is known on ring semigroups. In particular, it is well known that every cyclic ring semigroup (with $1 \neq 0$) is isomorphic to the multiplicative semigroup of a finite field, i.e., to a multiplicative semigroup of the form $\mathbb{F}_{p^n}$, where p is a prime number and n is a positive integer (e.g. see [1, Corollary 1.2]). It is also known that every commutative ring semigroup (with $1 \neq 0$) whose endomorphisms are power functions has to be finite (see [4, Proposition 1]). Hence as an immediate consequence of Theorem 3.1 we obtain the following result of Oman.

Corollary 3.2 ([4, Theorem 2]) *Let S be a commutative ring semigroup with $1 \neq 0$. Then every endomorphism of S preserving 0 and 1 is equal to a power function if and only if S is a cyclic group with zero adjoined of order p^n for some prime number p and positive integer n.*

By applying Corollary 3.2 to the multiplicative semigroup $(R, \cdot)$ of a commutative ring R we obtain the main result of [4].

Corollary 3.3 ([4, Theorem 1]) *Let R be a commutative ring with unity $1 \neq 0$. Then every multiplicative endomorphism $f : R \to R$ has the form $f(x) = x^m$ for some positive integer m if and only if R is a finite field.*

Acknowledgements The author is grateful to Professor László Márki for his suggestion to consider Oman's problem also for semigroups without zero and identity, which has led to the results presented in Sect. 2.

This research was supported by the Polish National Center of Science Grant No DEC-2011/03/B/ST1/04893.

References

1. Mazurek, R.: On semigroups admitting ring structure. Semigroup Forum **83**(2), 335–342 (2011)
2. Oman, G.: Ring semigroups whose subsemigroups form a chain. Semigroup Forum **78**(2), 374–377 (2009)
3. Oman, G.: Ring semigroups whose subsemigroups intersect. Semigroup Forum **79**(2), 413–416 (2009)
4. Oman, G.: Rings whose multiplicative endomorphisms are power functions. Semigroup Forum **86**(2), 272–278 (2013)
5. Peinado, R.E.: On semigroups admitting ring structure. Semigroup Forum **1**, 189–208 (1970)