RESEARCH ARTICLE

Commutative semigroups whose endomorphisms are power functions

Ryszard Mazurek[1]

Abstract

For any commutative semigroup S and positive integer m the power function $f : S \rightarrow S$ defined by $f(x) = x^m$ is an endomorphism of S. We partly solve the Lesokhin–Oman problem of characterizing the commutative semigroups whose all endomorphisms are power functions. Namely, we prove that every endomorphism of a commutative monoid S is a power function if and only if S is a finite cyclic group, and that every endomorphism of a commutative ACCP-semigroup S with an idempotent is a power function if and only if S is a finite cyclic semigroup. Furthermore, we prove that every endomorphism of a nontrivial commutative atomic monoid S with 0, preserving 0 and 1, is 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. We also prove that every endomorphism of a 2-generated commutative semigroup S without idempotents is a power function if and only if S is a subsemigroup of the infinite cyclic semigroup.

Keywords Commutative semigroup · ACCP-semigroup · Atomic monoid · Finitely generated commutative semigroup · Power function · Endomorphism

1 Introduction

Fuchs [4, Problem 45] posed the problem of characterizing the rings R that are isomorphic to the ring $End(R^+)$ of all endomorphisms of the additive group R^+ of R. Schultz [13, Lemma 6] partly solved the problem by proving that a ring R with identity is commutative and isomorphic to $End(R^+)$ if and only if every endomorphism of R^+ is a left multiplication in R; he coined the name *E-rings* for such rings R. Note that for

✉ Ryszard Mazurek
  r.mazurek@pb.edu.pl

1 Faculty of Computer Science, Bialystok University of Technology, Wiejska 45A, 15-351 Białystok, Poland

any ring R and $r \in R$ the left multiplication $f(x) = rx$ is an endomorphism of R^+. Hence one may view an E-ring as a ring in which the "canonical" endomorphisms of R^+ (i.e., the left multiplications) are the only additive endomorphisms of R.

Starting from the aforementioned seminal paper by Schultz, a great deal of research on E-rings and their generalizations has been done. Interestingly, already at the beginning of the nineteenth century A.-L. Cauchy knew that the rings of integers $\mathbb{Z}$ and rationals $\mathbb{Q}$ are E-rings, the fact applied by him in studying real functions f that satisfy the equation $f(x + y) = f(x) + f(y)$, nowadays called Cauchy's functional equation (see e.g., [9]). We refer the interested reader to [6,9,15] for more information on E-rings and related structures.

In 2013 in [12], keeping the spirit of Fuchs' original question, G. Oman changed the focus from ring addition to multiplication. Note that for *any* commutative ring R and positive integer m the power function $f(x) = x^m$ is an endomorphism of the multiplicative semigroup $(R, \cdot)$. Thus, informally, the power functions are the canonical endomorphisms of $(R, \cdot)$. In [12], Oman studied the following question: *For which commutative rings R with identity is every endomorphism of $(R, \cdot)$ canonical, i.e., equal to a power function?* He proved in [12, Theorem 1] that the rings in question are exactly finite fields.

Since the problem studied by Oman concerns endomorphisms of the multiplicative semigroup of a commutative ring, in the same paper [12] he posed an analogous problem for commutative semigroups (see Problem 1 below). It occurs that a very similar problem was posed much earlier by M. M. Lesokhin (see Problem 2 below). Before presenting those problems, we first establish some terminology and notation that will be used in the rest of the paper.

Let S be a semigroup (in this paper semigroups are written multiplicatively). We say that a map $f : S \rightarrow S$ preserves an element $s \in S$ if $f(s) = s$. By an endomorphism of S we understand a map $f : S \rightarrow S$ such that $f(xy) = f(x)f(y)$ for any $x, y \in S$; we would like to stress that if S has identity 1 (resp. zero 0), we do not assume that the endomorphism f preserves 1 (resp. 0), unless otherwise stated. A function $f : S \rightarrow S$ 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 if S is commutative, then every power function of S is an endomorphism of S.

If A is a subset of a semigroup S, then $\langle A \rangle$ denotes the subsemigroup of S generated by A. In particular, if $a \in S$, then $\langle a \rangle$ is the subsemigroup of S generated by a, i.e., $\langle a \rangle = \{a^n : n \in \mathbb{N}\}$, where $\mathbb{N}$ is the set of positive integers. A semigroup S is called a *cyclic* semigroup if S is generated by a single element, that is, $S = \langle a \rangle$ for some $a \in S$ (let us note that a group S is a cyclic semigroup if and only if S is a finite cyclic group). An element s of a semigroup S with 0 is said to be *nilpotent* if $s^n = 0$ for some $n \in \mathbb{N}$, and S is called a *nilsemigroup* if all its elements are nilpotent. A semigroup S is called a *cyclic group with zero adjoined* if S is obtained from a cyclic group by adjoining a zero, i.e., S is a semigroup with zero 0 and $S \backslash \{0\}$ 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, i.e., S has an identity 1 and $S \backslash \{1\}$ is a cyclic nilsemigroup.

Let S be a commutative semigroup. For an element $a \in S$, the ideal generated by a is denoted by (a), i.e., $(a) = \{a\} \cup aS$; such an ideal is called a *principal ideal*

of S. The semigroup S is said to satisfy the *ascending chain condition on principal ideals* (ACCP for short) if there does not exist an infinite strictly ascending chain of principal ideals of S (cf. [5, Definition 1.1.3]). Semigroups that satisfy the ACCP are called *ACCP-semigroups*.

Let S be a commutative monoid with 0 (i.e., S is a commutative semigroup with 1 and 0). Let $U(S)$ denote the group of units of S, and $T(S) = S \backslash U(S)$ the set of nonunits of S. We say that an element $a \in S$ is an *atom* of S if $a \in T(S) \backslash T(S)^2$, i.e., $a \in T(S)$ and a cannot be written in the form $a = bc$ with $b, c \in T(S)$. The monoid S is *atomic* if every element $a \in T(S) \backslash \{0\}$ can be written in the form $a = a_1 a_2 \cdots a_n$, where $n \in \mathbb{N}$ and all the elements $a_1, a_2, \ldots, a_n$ are atoms of S (cf. [2,5]).

As we mentioned above, in [12] Oman proved that if R is a commutative ring with identity $1 \neq 0$, then every endomorphism of the multiplicative semigroup $(R, \cdot)$ preserving 0 and 1 is a power function if and only if R is a finite field. Since the result concerns endomorphisms of the multiplicative semigroup of a commutative ring, he posed the following more general problem.

Problem 1 (Oman [12, Problem 1]) *Characterize the commutative semigroups S (with or without 0 or 1) such that every endomorphism of S is a power function.*

It occurs that the Oman problem is not quite new, which was pointed out to the author by M. Volkov. Namely, the following very similar problem was posed more than forty years earlier by Lesokhin in the Sverdlovsk Tetrad [14], which is a collection of unsolved problems of the semigroup theory.

Problem 2 (Lesokhin [14, Problem T34]) *Describe commutative semigroups having no endomorphisms different from φ_n (n = 1, 2, \ldots) which to each element associates its n-th power.*

Borisov [1] solved the Lesokhin problem for finite commutative semigroups by proving the following result (also this result was pointed out to the author by M. Volkov).

Theorem 1.1 [1] *For a finite commutative semigroup S the following conditions are equivalent:*

 (i) Every endomorphism of S is a power function.
 (ii) S is a cyclic semigroup.
(iii) The semigroup of endomorphisms of S under pointwise multiplication is cyclic.

Independently, in 2014 for finite commutative semigroups the equivalence of the above conditions (i) and (ii) was proved in [11, Theorem 2.2]. In the same paper the Oman problem for finite commutative monoids with 0 was solved in the following theorem.

Theorem 1.2 ([11, Theorem 3.1]) *Let S be a finite commutative monoid with $0 \neq 1$. Then every endomorphism of S preserving 0 and 1 is a power function if and only if S is either a cyclic group with zero adjoined or a cyclic nilsemigroup with identity adjoined.*

Since Problem 1 posed by Oman is very similar to Problem 2 posed earlier by Lesokhin, in what follows Problem 1 is called the *Lesokhin–Oman problem*.

Having the Lesokhin–Oman problem solved for finite commutative semigroups, it is natural, as a next step, to consider it for finitely generated commutative semigroups. In this paper, for commutative semigroups with idempotents we go much further, solving Lesokhin–Oman's problem completely for commutative monoids, commutative atomic monoids with 0, and commutative ACCP-semigroups. Namely, in Theorem 2.1 we prove that every endomorphism of a commutative monoid S is a power function if and only if S is a finite cyclic group, and in Theorem 2.3 we show that every endomorphism of a commutative ACCP-semigroup S with an idempotent is a power function if and only if S is a finite cyclic semigroup. Furthermore, in Theorem 3.1 we prove that every endomorphism of a nontrivial commutative atomic monoid S with 0, preserving 0 and 1, is 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. Regarding commutative semigroups without idempotent, we solve the Lesokhin–Oman problem for 2-generated commutative semigroups in Theorem 4.2, where we prove that every endomorphism of a 2-generated commutative semigroup S without idempotent is a power function if and only if S is a subsemigroup of an infinite cyclic semigroup. In this paper we also prove some necessary conditions (e.g., Proposition 2.1 and Lemma 2.3) as well as some sufficient conditions (e.g., Theorem 4.1) for a commutative semigroup to have power functions as the only endomorphisms.

We close this section with a remark on the organization of the paper. Let us note that in fact the Lesokhin–Oman problem splits into few problems, as we can see from its formulation. Indeed, the problem requires to consider the following cases: (i) no assumption on the existence 0 or 1 in S; (ii) S with 0; (iii) S with 1 (i.e., S is a monoid); (iv) S with $1 \neq 0$ (i.e., S is a nontrivial monoid with 0). Furthermore, in case (ii) it is necessary to consider two subcases: (A) where all endomorphisms of S are assumed to preserve 0, and (B) where are not. Fortunately, by Corollary 2.1, for the Lesokhin–Oman problem the subcases (A) and (B) are equivalent (the same holds for the appropriate two subcases of (iii)). In case (iv) it is necessary to consider the subcases: (C) where all endomorphisms are assumed to preserve 0 and 1, and (D) where are not. From Proposition 2.1(c) and Corollary 2.1 it follows that in subcase (D) there exists no nontrivial monoid S with 0 whose all endomorphisms are power functions. Hence in case (iv) the Lesokhin–Oman problem reduces to subcase (C). These observations caused that the rest of the paper is organized as follows: Sect. 2 is devoted to commutative semigroups with idempotents (which includes the cases (ii), (iii) and a "half" of case (i)), Sect. 3 focuses on nontrivial monoids with 0 whose endomorphisms preserve 0 and 1 (case (iv)), and in Sect. 4 we consider commutative semigroups without idempotent (the remaining "half" of case (i)). Some results of Sects. 2 and 3 develop ideas from the author's paper [11].

The author would like to thank Professor M. Volkov for drawing attention to Lesokhin's problem and Borisov's results on the problem, both unknown to the author earlier.

2 Commutative semigroups with idempotents whose endomorphisms are power functions

In this section we study Lesokhin–Oman's problem for commutative semigroups with idempotents. A special case of such semigroups are abelian groups. Abelian groups whose endomorphisms are power functions are characterized in the following result.

Lemma 2.1 ([12, Lemma 1]) *Let G be an abelian group. Then every endomorphism of G is a power function if and only if G is a finite cyclic group.*

As we show in the lemma below, the "if" part of Lemma 2.1 is valid for any cyclic semigroup. The result follows by the argument presented in the first part of the proof of [12, Lemma 1]. We include a proof for sake of completeness.

Lemma 2.2 *If S is a cyclic semigroup, then every endomorphism of S is a power function.*

Proof Assume S is a cyclic semigroup. Let $f : S \to S$ be an arbitrary endomorphism of S and let a be a generator of S. Then $f(a) = a^m$ for some $m \in \mathbb{N}$. Hence for any $x \in S$, since $x = a^k$ for some $k \in \mathbb{N}$, we obtain

$$f(x) = f(a^k) = f(a)^k = (a^m)^k = (a^k)^m = x^m.$$

Thus f is a power function. □

As we have already said, in this section we study the Lesokhin–Oman problem for commutative semigroups with idempotents. The following easy observation will be useful.

Proposition 2.1 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$. Assume that every endomorphism of S preserving e is a power function. Then*

(a) *There exists $m \in \mathbb{N}$ such that for any $a \in S$ we have $a^m = e$, and consequently $\langle a \rangle = \{a, a^2, \ldots a^{2m-1}\}$.*
(b) *For any $a \in S$ and $k, n \in \mathbb{N}$, if $a^k \notin eS$, then $a^k = a^n$ if and only if $k = n$.*
(c) *e is the only idempotent of S.*
(d) *Every endomorphism of S preserves e.*
(e) *eS is a finite cyclic group.*

Proof Consider the function $g : S \to S$ defined by $g(x) = e$ for any $x \in S$. Since g is an endomorphism of S preserving e, by hypothesis g is a power function and thus there exists $m \in \mathbb{N}$ such that for any $a \in S$ we have $a^m = g(a) = e$. Hence $a^{2m} = e^2 = e = a^m$ and thus $\langle a \rangle = \{a, a^2, \ldots a^{2m-1}\}$, which proves (a). To prove (b), assume $a \in S$ and $a^k = a^n$ with $k \neq n$, say $k < n$. Then for $y = a^{n-k}$ and m as in (a) we have $a^k = a^k y = a^k y^2 = \ldots = a^k y^m = a^k e \in eS$ and (b) follows. Part (c) is an immediate consequence of (a). To prove (d), let $f : S \to S$ be any endomorphism of S and let m be as in (a). Then $f(e) = f(e^m) = f(e)^m = e$, so f preserves e. We are left with (e). Since (a) implies that eS is an abelian group, it follows from Lemma 2.1 that to prove (e), it suffices to show that if $f : eS \to eS$ is an endomorphism of eS,

then f is a power function. It is easy to verify that since f is an endomorphism of the group eS, the function $h : S \to S$ defined by $h(x) = f(ex)$ (for all $x \in S$) is an endomorphism of S preserving e. Hence by hypothesis, h is a power function and thus so is f. □

As a consequence of Proposition 2.1 we obtain the following corollary.

Corollary 2.1 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving e is a power function.*

Proof The implication (i) $\Rightarrow$ (ii) is obvious. The opposite implication follows immediately from Proposition 2.1(d). □

The following theorem solves Lesokhin–Oman's problem for all commutative semigroups with 1.

Theorem 2.1 *Let S be a commutative monoid. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving 1 is a power function.*
(iii) *S is a finite cyclic group.*

Proof By Corollary 2.1, conditions (i) and (ii) are equivalent. To prove (ii) $\Rightarrow$ (iii), it suffices to apply Proposition 2.1(e) with $e = 1$. The implication (iii) $\Rightarrow$ (i) is an immediate consequence of Lemma 2.1. □

Recall that a semigroup S is said to be *regular* if for any $s \in S$ there exists $t \in S$ such that $s = sts$. As a consequence of Theorem 2.1 we obtain the following result of A. I. Kuptsov [10].

Corollary 2.2 ([10]) *Let S be a commutative regular semigroup. Then all endomorphisms of S are power functions if and only if S is a finite cyclic group.*

Proof To prove the "only if" part of the result, assume that all endomorphisms of S are power functions and let s be an element of S. Since the semigroup S is regular, for some idempotent $e = e^2 \in S$ we have $s = es$ (indeed, since $s = sts$ for some $t \in S$, it suffices to put $e = st$). By Proposition 2.1(c), e is the only idempotent of S and thus $s = es$ for any $s \in S$, i.e., e is an identity of S. Hence S is finite cyclic group by Theorem 2.1, which completes the proof of the "only if" part. The "if" part follows immediately from Lemma 2.1. □

In the following two lemmas we prove some necessary conditions for a commutative semigroup S with an idempotent to have the power functions as the only endomorphisms.

Lemma 2.3 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$. If all endomorphisms of S are power functions, then the set $S\backslash S^2$ contains no more than one element.*

Proof If $S = S^2$, then there is nothing to prove. Hence we assume $S^2 \subsetneq S$. It follows from Proposition 2.1(a) that there exists a smallest positive integer k such that $a^k \notin eS$ and $a^{2k} \in eS$ for some $a \in S \backslash S^2$. We will show that a is the only element of $S \backslash S^2$. We first show that the following function $g : S \to S$ is an endomorphism of S:

$$g(x) = \begin{cases} a^k & \text{if } x = a \\ ex^k & \text{if } x \neq a. \end{cases} \tag{2.1}$$

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 $x, y \in S$. If $x = y = a$, then since $a^{2k} \in eS$, we obtain $g(x)g(y) = g(a)g(a) = a^{2k} = ea^{2k} = e(aa)^k = g(xy)$. 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 $x \in S$. Since $a^k \notin eS$ and $a^k = g(a) = a^m$, Proposition 2.1(b) yields $k = m$ 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 $x \in S \backslash \{a\}$, and consequently it follows from our choice of k that $S \backslash \{a\} \subseteq S^2$. Hence $S \backslash S^2 = \{a\}$. □

Lemma 2.4 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$ such that $eS \neq S$. If all endomorphisms of S are power functions, then for any $j \in \mathbb{N}$ the following conditions are equivalent.*

(i) $s^j = e$ for any $s \in S \backslash eS$.
(ii) $s^j = e$ for any $s \in S$.

Proof We assume (i) and prove (ii). For that, we show that the following function $h : S \to S$ is an endomorphism of S:

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

Since S is commutative, to verify that h is an endomorphism of S, it suffices to consider the following three cases for $x, y \in S$.

Case 1: $x, y \in eS$. Then $xy \in eS$, so $h(xy) = (xy)^{j+1} = x^{j+1}y^{j+1} = h(x)h(y)$.

Case 2: $x \in eS$, $y \notin eS$. Then $xy \in eS$ and $y^j = e$ and thus $h(xy) = (xy)^{j+1} = x^{j+1}y^jy = ex^{j+1}y = x^{j+1}y = h(x)h(y)$.

Case 3: $x \notin eS$, $y \notin eS$. Then $x^j = y^j = e$. If $xy \in eS$, then $h(xy) = (xy)^{j+1} = x^jxy^jjy = exy = xy = h(x)h(y)$. If $xy \notin eS$, then $h(xy) = xy = h(x)h(y)$.

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 $x \in S$. By assumption, there exists an element $a \in S \backslash eS$. Since $a = h(a) = a^m$, Proposition 2.1(b) implies $m = 1$ and thus for any $x \in eS$ we obtain

$$x^{j+1} = h(x) = x. \tag{2.2}$$

By Proposition 2.1(e), eS is a group with identity e. Hence it follows from (2.2) that $x^j = e$ for any $x \in eS$, which proves (ii). Since the implication (ii) $\Rightarrow$ (i) is obvious, the proof is complete. $\square$

To state the main result of this section, we adapt for semigroups with idempotents the definition of an atom and an atomic monoid with 0, given in the Introduction. Let S be a commutative semigroup with an idempotent $e = e^2 \in S$. We say that an element $a \in S$ if an *atom* of S if $a \in S \backslash S^2$, i.e., a cannot be written in the form $a = bc$ with $b, c \in S$. We say that the semigroup S is *e-atomic* if every element $a \in S \backslash eS$ can be written in the form $a = a_1 a_2 \cdots a_n$ where $n \in \mathbb{N}$ and all the elements $a_1, a_2, \ldots, a_n$ are atoms of S. By comparing the definitions in this paragraph with those in the Introduction, we can see that a commutative monoid S with 0 is atomic if and only if the semigroup $T(S) = S \backslash U(S)$ is 0-atomic.

Theorem 2.2 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$ such that S is e-atomic. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving e is a power function.*
(iii) *S is a finite cyclic semigroup.*

Proof (i) and (ii) are equivalent by Corollary 2.1, and (iii) $\Rightarrow$ (i) follows from Lemma 2.2. To complete the proof, it suffices to show that (ii) implies (iii).

Assume (ii). If $S = eS$, then it follows from Proposition 2.1(e) that S is a finite cyclic group, so S is a finite cyclic semigroup as well. We are left with the case where $eS \subsetneq S$. Then, since S is e-atomic, S contains at least one atom a, and Lemma 2.3 implies that a is the only atom of S. Hence, again since S is e-atomic, it follows that

$$S \backslash eS \subseteq \langle a \rangle, \tag{2.3}$$

where furthermore $\langle a \rangle$ is finite by Proposition 2.1(a). To complete the proof, it suffices to show that $eS \subseteq \langle a \rangle$; then $S = \langle a \rangle$ will follow from (2.3), proving that S is a finite cyclic semigroup.

By Proposition 2.1(e), eS is a finite cyclic group. Let b be a generator of eS. Since $\langle a \rangle$ is finite, there exist $r, p \in \mathbb{N}$ with $r < p$ such that $a^r = a^p$. Let p be chosen as small as possible and let $k = p - r$. By [3, Theorem 1.9], the set

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

is a group of order k, whereas by Proposition 2.1(c), e is the unique idempotent of S. Hence it follows that e is the identity element of G and thus G is a subgroup of the group eS. Since $e \in G$, we have $a^u = e$ for some $u \in \{r, r+1, \ldots, r+k-1\}$, and since $a^r = a^p$, we obtain that also $a^{u+k} = a^{p+(u-r)} = a^{r+(u-r)} = a^u = e$. Hence (2.3) and Lemma 2.4 imply that $b^u = e$ and $b^{u+k} = e$, and thus $b^k = eb^k = b^u b^k = b^{u+k} = e$. Since b is a generator of the group eS, and $b^k = e$, and k is the order of the group G, it follows that for the orders of the groups eS and G we have that $|eS| \leq k = |G|$. Since furthermore G is a subgroup of eS, we deduce that $eS = G$. Clearly $G \subseteq \langle a \rangle$, so we obtain $eS \subseteq \langle a \rangle$, as desired. $\square$

To apply Theorem 2.2 to ACCP-semigroups, we need the following observation.

Proposition 2.2 *Let S be a commutative semigroup with an idempotent $e = e^2 \in S$ such that for any $s \in S$ there exists $m \in \mathbb{N}$ with $s^m \in eS$. If S is an ACCP-semigroup, then S is e-atomic.*

Proof If $S = eS$, then S is trivially e-atomic. In the remaining case where $S \neq eS$ we proceed similarly to the proof of [5, Proposition 1.1.4]. Suppose, for contradiction, that $S \neq eS$ and S is not e-atomic. Let A be the set of all $a \in S \backslash eS$ which are not a product of atoms. Hence $A \neq \emptyset$ and if $a \in A$, then $a = bc$ for some $b, c \in S \backslash eS$, and necessarily $b \in A$ or $c \in A$. We can assume that $b \in A$. Obviously we have $(a) \subseteq (b)$. If $(a) = (b)$, then $b = a$ or $b = ad$ for some $d \in S$, so $a = bc = as$ for some $s \in S$. Hence $a = as^m$ for any $m \in \mathbb{N}$. Since by hypothesis $s^m \in eS$ for some $m \in \mathbb{N}$, it follows that $a \in eS$, and this contradiction proves that $(a) \subsetneq (b)$. We have shown that for any $a \in A$ there exists $a' \in A$ such that $(a) \subsetneq (a')$. Hence starting with some $a_1 \in A$ and defining $a_{n+1} = a'_n$ for any $\mathbb{N}$, we obtain a strictly ascending chain of principal ideals $(a_1) \subsetneq (a_2) \subsetneq \dots$. Thus S is not an ACCP-semigroup, a contradiction. □

Now we are in a position to solve the Lesokhin–Oman problem for commutative ACCP-semigroups with idempotents.

Theorem 2.3 *Let S be a commutative ACCP-semigroup with an idempotent $e = e^2 \in S$. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving e is a power function.*
(iii) *S is a finite cyclic semigroup.*

Proof The implications (iii) $\Rightarrow$ (i) $\Leftrightarrow$ (ii) follow from Lemma 2.2 and Corollary 2.1. To prove (i) $\Rightarrow$ (iii) it suffices to combine Propositions 2.1(a) and 2.2, and Theorem 2.2. □

The following result solves Lesokhin–Oman's problem in the class of finitely generated commutative semigroups with idempotents.

Corollary 2.3 *Let S be a finitely generated commutative semigroup with an idempotent $e = e^2 \in S$. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving e is a power function.*
(iii) *S is a finite cyclic semigroup.*

Proof It is well known that every finitely generated commutative semigroup is an ACCP-semigroup (see, e.g., [7, Corollary 1.4]). Hence the result follows from Theorem 2.3. □

Obviously, any finite semigroup contains an idempotent. Thus the equivalence of conditions (i) and (ii) in Theorem 1.1 is an immediate consequence of Corollary 2.3 (this equivalence is one of the main results of [11]).

We close this section with another consequence of Theorem 2.3.

Corollary 2.4 *Let S be a commutative ACCP-semigroup with* 0. *Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function.*
 (ii) *Every endomorphism of S preserving* 0 *is a power function.*
(iii) *S is a finite cyclic nilsemigroup.*

Proof The implications (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) follow from Theorem 2.3. Furthermore by Theorem 2.3, (ii) implies that S is a finite cyclic semigroup, and Proposition 2.1(a) shows that S is a nilsemigroup. Hence (ii) implies (iii).   □

3 Commutative monoids with 0 whose endomorphisms preserving 0 and 1 are power functions

We start this section with a result which provides examples of semigroups specified in the title of the section. Recall that for a monoid S with 0 (i.e., for a semigroup S with 1 and 0), we denote the set of units of S by $U(S)$, and the ideal of nonunits by $T(S)$, i.e., $T(S) = S \backslash U(S)$.

Proposition 3.1 *If S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined, then S is a commutative monoid with* 0 *and every endomorphism of S preserving* 0 *and* 1 *is a power function.*

Proof Assume that S is a finite cyclic group with zero adjoined, i.e., $U(S) = S \backslash \{0\}$ and the group $U(S)$ is finite and cyclic. If $f : S \to S$ is an endomorphism of S preserving 0 and 1, then $f(1) = 1 \neq 0$, which implies that $f(U(S)) \subseteq U(S)$. Hence the restriction $\bar{f}$ of f to $U(S)$ is an endomorphism of the group $U(S)$, and thus it follows from Lemma 2.1 that $\bar{f}$ is a power function of $U(S)$. Therefore, f is a power function of S, as desired.

To complete the proof, we consider the remaining case where S is a cyclic nilsemigroup with identity adjoined. Then there exists a nilpotent element $a \in S$ such that all elements of $S \backslash \{1\}$ are of the form a^i with $i \in \mathbb{N}$. 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 $m \in \mathbb{N}$. Hence if $x \in S \backslash \{1\}$, then $x = a^i$ for some $i \in \mathbb{N}$, and thus

$$f(x) = f(a^i) = f(a)^i = (a^m)^i = (a^i)^m = x^m.$$

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

The following result will be useful in the rest of this section.

Proposition 3.2 *Let S be a nontrivial commutative monoid with* 0 *such that every endomorphism of S preserving* 0 *and* 1 *is a power function. Then*

(a) *$U(S)$ is a finite cyclic group.*
(b) *There exists $m \in \mathbb{N}$ such that $a^m = 0$ for any $a \in T(S)$. In particular, $T(S)$ is a nilsemigroup.*

(c) For any $a \in T(S)$ and $i, j \in \mathbb{N}$, if $a^i \neq 0$, $a^j \neq 0$ and $i \neq j$, then

$$a^i U(S) \cap a^j U(S) = \emptyset.$$

Proof (a) If $f : U(S) \to U(S)$ is an endomorphism of the group $U(S)$, then the map $\widehat{f} : S \to S$ defined by

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

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 $U(S)$. Thus every endomorphism of the group $U(S)$ is a power function, so Lemma 2.1 implies that $U(S)$ is a finite cyclic group.

(b) The function $f : S \to S$ defined by

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

is easily seen to be an endomorphism of S preserving 0 and 1, and thus there exists $m \in \mathbb{N}$ such that for any $a \in T(S)$ we have $a^m = f(a) = 0$, i.e., (b) holds.

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

To prove the main result of this section, we will need the following lemma.

Lemma 3.1 *Let S be a nontrivial commutative monoid with* 0. *Denote* $U = U(S)$ *and* $T = T(S)$. *If every endomorphism of S preserving* 0 *and* 1 *is a power function and* $T \neq T^2$, *then* $T \setminus T^2 = aU$ *for some* $a \in T$.

Proof Assume that $T \neq T^2$. By Proposition 3.2(b) there exists $n \in \mathbb{N}$ such that $t^n = 0$ for any $t \in T$. Hence there exists a smallest $k \in \mathbb{N}$ such that $a^k \neq 0$ and $a^{k+1} = 0$ for some $a \in T \setminus T^2$. We denote $C = T \setminus aU$ and define $g : S \to S$ as follows:

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

Since the sets U, aU and C are pairwise disjoint and $S = U \cup aU \cup C$, 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

$$T^2 \subseteq C. \tag{3.1}$$

Indeed, if $T^2 \nsubseteq C = T \backslash aU$, 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 (3.1). Note that (3.1) 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 by (3.1), $xy \in C$ 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 $g(xy) = 0 = 1 \cdot 0 = g(x)g(y)$.

We have shown that g is an endomorphism of S preserving 0 and 1, and thus there exists $m \in \mathbb{N}$ with $g(x) = x^m$ for every $x \in S$. In particular, $a^k = g(a) = a^m$, and since $a^k \neq 0$, Proposition 3.2(c) implies that $k = m$. Hence it follows from the definition of g that $x^k = 0$ for every $x \in C$, and we conclude from our choice of k that $C \subseteq T^2$. Combining this with (3.1), we obtain $T^2 = C = T \backslash aU$ and thus $T \backslash T^2 = aU$.   □

The following theorem solves the Lesokhin–Oman problem for the class of commutative atomic monoids with 0.

Theorem 3.1 *Let S be a nontrivial commutative monoid with 0. If S is atomic, then the following conditions are equivalent.*

  (i) *Every endomorphism of S preserving 0 and 1 is a power function.*
  (ii) *Either S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined.*

Proof Denote $U = U(S)$ and $T = T(S)$.

(i) $\Rightarrow$ (ii): Assume (i). By Proposition 3.2, U is a finite cyclic group and T is a nilsemigroup. Hence, if $T = \{0\}$, then S is a finite cyclic group with zero adjoined. We are left with the case where $T \neq \{0\}$. Then, since S is atomic, there exist atoms of S, i.e., $T \neq T^2$. Hence by Lemma 3.1, for some $a \in T$ we have that $T \backslash T^2 = aU$. Since T is a nilsemigroup and $a \notin T^2$, there exists $k \in \mathbb{N}$ such that $a^k \neq 0$ and $a^{k+1} = 0$. Since S is atomic and the set of atoms of S is equal to $T \backslash T^2 = aU$, we deduce that

$$T = aU \cup a^2 U \cup \cdots \cup a^k U \cup a^{k+1} U.$$

Let $h : S \to S$ be defined as follows:

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

Proposition 3.2(c) implies that the sets $U, aU, a^2 U, \ldots, a^k U, a^{k+1} U$ are pairwise disjoint and thus h is well-defined. Since obviously h is an endomorphism of S preserving 0 and 1, there exists $m \in \mathbb{N}$ such that $h(x) = x^m$ for every $x \in S$. In particular,

$a^m = h(a) = a$, so we obtain from Proposition 3.2(c) that $m = 1$. Hence it follows from the definition of h that $U = \{1\}$, and thus

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

where $a^{k+1} = 0$. Thus S is a cyclic nilsemigroup with identity adjoined.
(ii) $\Rightarrow$ (i): This implication follows from Proposition 3.1. $\square$

The following theorem solves the Lesokhin–Oman problem in the class of commutative ACCP-monoids with 0.

Theorem 3.2 *Let S be a nontrivial commutative ACCP-monoid with 0. Then the following conditions are equivalent.*

 (i) Every endomorphism of S preserving 0 and 1 is a power function.
 (ii) Either S is a finite cyclic group with zero adjoined or S is a cyclic nilsemigroup with identity adjoined.

Proof Assume (i). Since S is an ACCP-monoid, $T(S)$ is an ACCP-semigroup, which furthermore, by Proposition 3.2(b), is a nilsemigroup. Hence by Proposition 2.2, $T(S)$ is a 0-atomic semigroup, i.e., S is an atomic monoid. Thus (ii) follows by Theorem 3.1, which completes the proof of the implication (i) $\Rightarrow$ (ii). The opposite implication follows from Proposition 3.1. $\square$

Since all finitely generated commutative semigroups are ACCP-semigroups (see, [7, Corollary 1.4]), the following result is an immediate consequence of Theorem 3.2.

Corollary 3.1 *Let S be a nontrivial finitely generated commutative monoid with 0. Then every endomorphism of S preserving 0 and 1 is 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.*

Corollary 3.1 applies, in particular, to finite commutative semigroups with $1 \neq 0$, giving Theorem 1.2 (which is one of the main results of [11]).

4 Commutative semigroups without idempotents whose endomorphisms are power functions

In this section we focus on the class of finitely generated commutative semigroups without idempotents whose endomorphisms are power functions. The following result shows that every subsemigroup of an infinite cyclic semigroup belongs to this class of semigroups.

Theorem 4.1 *If S is a subsemigroup of an infinite cyclic semigroup, then every endomorphism of S is a power function, S is a finitely generated commutative semigroup and S has no idempotents.*

Proof Since every infinite cyclic semigroup is isomorphic to the additive semigroup of positive integers $\mathbb{N}$, without loss of generality we can assume that S is a subsemigroup of $\mathbb{N}$ (consequently, in the rest of the proof S is written additively). Clearly S is a semigroup without idempotents (i.e., without an element e such that $2e = e$). Furthermore, it is well known that all subsemigroups of $\mathbb{N}$ are finitely generated (see, e.g., [8, Corollary 3.1.1]). Hence there exist $a_1, a_2, \ldots, a_j \in \mathbb{N}$ such that $S = \langle a_1, a_2, \ldots, a_j \rangle$.

It remains to show that every endomorphism f of S is a power function (i.e., there exists $m \in \mathbb{N}$ such that $f(x) = mx$ for any $x \in S$). By Lemma 2.2 the case $j = 1$ is obvious, so we assume that $j > 1$. Let $f : S \to S$ be an endomorphism of the semigroup $S = \langle a_1, a_2, \ldots, a_j \rangle$. Set $d = gcd\{a_1, a_2, \ldots, a_j\}$ and put

$$\widehat{S} = \left\langle \frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_j}{d} \right\rangle.$$

Since $gcd\{\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_j}{d}\} = 1$, it follows from [8, Lemma 3.1] that there exists $k \in \mathbb{N}$ such that $n \in \widehat{S}$ for any integer $n \geq k$. Hence

$$nd \in S \text{ for any } n \geq k.$$

In particular, $kd \in S$ and $(k+1)d \in S$, and thus

$$f(kd), \, f((k+1)d) \in S = \langle a_1, a_2, \ldots, a_j \rangle.$$

Since $d = gcd\{a_1, a_2, \ldots, a_j\}$, d divides any integral combination of $a_1, a_2, \ldots, a_j$ and thus there exist $u, v \in \mathbb{N}$ such that $f(kd) = ud$ and $f((k+1)d) = vd$. Since

$$(k+1)ud = (k+1)f(kd) = f((k+1)kd) = f(k(k+1)d) = kf((k+1)d) = kvd,$$

it follows that $(k+1)u = kv$. Hence k divides $(k+1)u$ and thus k divides u. Therefore $u = mk$ for some $m \in \mathbb{N}$. Thus for any $i \in \{1, 2, \ldots, j\}$ we have

$$kdf(a_i) = f(a_i kd) = a_i f(kd) = a_i ud = a_i mkd.$$

Hence $f(a_i) = ma_i$ for any generator a_i of S, which implies that $f(x) = mx$ for any $x \in S$. □

We do not know whether the implication in Theorem 4.1 is in fact an equivalence. As we will show in Theorem 4.2, it is so for commutative 2-generated semigroups without idempotent. In the proof of this theorem we will need the following lemma and its corollary.

Lemma 4.1 *Let S be a commutative semigroup. If there exist $x, y \in S$ and $i, j \in \mathbb{N}$ such that $x^i = x^j y$ and $i < j$, then S has an idempotent.*

Proof Assume $x^i = x^j y$ with $i < j$. Then $x^i = x^i(x^{j-i}y)$ and thus $x^i = x^i(x^{j-i}y)^i$. Obviously $(x^{j-i}y)^i = x^i t$ for some $t \in S$. Hence $x^i = x^i x^i t$ and consequently $x^i t = (x^i t)^2$ is an idempotent of S. □

Corollary 4.1 *If S is a commutative semigroup without idempotents, $x \in S$ and $x^i \in x^j S$ for some $i, j \in \mathbb{N}$, then $i \geq j$.*

The following theorem solves the Lesokhin–Oman problem for 2-generated commutative semigroups without idempotents.

Theorem 4.2 *Let S be a commutative semigroup generated by two elements $a, b \in S$. Then the following conditions are equivalent.*

  (i) *Every endomorphism of S is a power function and S has no idempotents.*
 (ii) *The element a has infinite order and there exist relatively prime positive integers m, n such that $a^m = b^n$.*
(iii) *S is a subsemigroup of an infinite cyclic semigroup.*

Proof (i) $\Rightarrow$ (ii) Assume (i). It is clear that a has infinite order.

Suppose that a and b are free generators of S. Then every element $x \in S$ can be uniquely written in the form $x = a^\alpha b^\beta$, where $\alpha, \beta \in \mathbb{N} \cup \{0\}$ and $\alpha + \beta > 0$ (as usually, by $a^\alpha b^\beta$ with $\alpha = 0$ (resp. $\beta = 0$) we mean b^β (resp. a^α)). By defining $f(x) = f(a^\alpha b^\beta) = b^{\alpha+\beta}$, we obtain an endomorphism of S. Since every endomorphism of S is a power function, there exists $m \in \mathbb{N}$ such that $f(x) = x^m$ for any $x \in S$. Thus $a^m = f(a) = b$, which contradicts that a, b are free generators of S.

By the above, the generators a, b of S are not free generators and thus there exist $s, t, u, v \in \mathbb{N}$ such that

$$a^s b^t = a^u b^v \text{ and } (s, t) \neq (u, v). \tag{4.1}$$

We claim that

$$(ab)^i = (ab)^j b^k \text{ for some } i, j, k \in \mathbb{N} \text{ such that } j \leq i \leq j + k. \tag{4.2}$$

To prove the claim, note first that (4.1) implies that

$$(ab)^{s+t} = a^{u+t} b^{v+s}. \tag{4.3}$$

If $u + t = v + s$, then (4.3) yields $(ab)^{s+t} = (ab)^{u+t}$, and since S contains no idempotents, $s+t = u+t$ follows. Hence $s = u$, and consequently $t = v$, contradicting that $(s, t) \neq (u, v)$. Thus $u + t \neq v + s$. If $u + t < v + s$, then (4.3) implies $(ab)^{s+t} = (ab)^{u+t} b^{v+s-(u+t)}$, so for $i = s+t$, $j = u+t$ and $k = v+s-(u+t)$ we have $i, j, k \in \mathbb{N}$ and $(ab)^i = (ab)^j b^k$. If $u+t > v+s$, then by multiplying both sides of (4.3) by $b^{u+t-(v+s)}$, we obtain $(ab)^{u+t} = (ab)^{s+t} b^{u+t-(v+s)}$ and thus for $i = u+t$, $j = s+t$ and $k = u+t - (v+s)$ we have $i, j, k \in \mathbb{N}$ and $(ab)^i = (ab)^j b^k$.

We already know that there exist $i, j, k \in \mathbb{N}$ such that $(ab)^i = (ab)^j b^k$. Then also $(ab)^{j+k} = (ab)^i a^k$, and thus Corollary 4.1 implies that $j \leq i \leq j + k$, which completes the proof of (4.2).

Let $i, j, k \in \mathbb{N}$ be as in (4.2). We claim that for any $\alpha, \beta, \gamma, \delta \in \mathbb{N} \cup \{0\}$ such that $\alpha + \beta > 0$ and $\gamma + \delta > 0$,

$$\text{if } a^\alpha b^\beta = a^\gamma b^\delta, \text{ then } \alpha(j + k - i) + \beta(i - j) = \gamma(j + k - i) + \delta(i - j). \tag{4.4}$$

To prove (4.4), note first that without loss of generality we can assume that all the exponents $\alpha, \beta, \gamma, \delta$ are positive (it suffices to increase each of the exponents by 1, i.e., replace α with $\alpha + 1$, β with $\beta + 1$, etc.) Now, since $a^\alpha b^\beta = a^\gamma b^\delta$, it follows that $(ab)^{\alpha+\beta} = a^{\gamma+\beta} b^{\delta+\alpha}$ and thus, by using also the equation (4.2), we obtain that

$$
\begin{aligned}
(ab)^{k(\alpha+\beta)+j(\delta+\alpha)+i(\gamma+\beta)} &= \left((ab)^{\alpha+\beta}\right)^k \left((ab)^i\right)^{\gamma+\beta}(ab)^{j(\delta+\alpha)} \\
&= \left(a^{\gamma+\beta}b^{\delta+\alpha}\right)^k \left((ab)^j b^k\right)^{\gamma+\beta}(ab)^{j(\delta+\alpha)} = \left((ab)^{\gamma+\beta}\right)^k \left((ab)^j\right)^{\gamma+\beta}\left((ab)^j b^k\right)^{\delta+\alpha} \\
&= \left((ab)^{\gamma+\beta}\right)^k \left((ab)^j\right)^{\gamma+\beta}\left((ab)^i\right)^{\delta+\alpha} = (ab)^{k(\gamma+\beta)+j(\gamma+\beta)+i(\delta+\alpha)}.
\end{aligned}
$$

Since S has no idempotent, it follows that

$$
k(\alpha + \beta) + j(\delta + \alpha) + i(\gamma + \beta) = k(\gamma + \beta) + j(\gamma + \beta) + i(\delta + \alpha).
$$

Hence $\alpha(j + k - i) + \beta(i - j) = \gamma(j + k - i) + \delta(i - j)$, which proves (4.4).

It is clear that in (4.2) at least one of the inequalities $j \le i \le j + k$ is strict. Below we show that in fact both of them are strict. We separately exclude the cases when $j = i$ and when $i = j + k$.

Case 1. Suppose, for contradiction, that $j = i$. Then

$$
(ab)^i = (ab)^i b^k. \tag{4.5}
$$

For any $w \in \mathbb{N}$ we show that by setting

$$
g(a^\alpha b^\beta) = (ab)^{i\alpha} b^{kw(\alpha+\beta)} \text{ for any } \alpha, \beta \in \mathbb{N} \cup \{0\} \text{ with } \alpha + \beta > 0
$$

we obtain an endomorphism of S. To show that g is well-defined, assume that $a^\alpha b^\beta = a^\gamma b^\delta$, where $\alpha, \beta, \gamma, \delta \in \mathbb{N} \cup \{0\}$, and both $\alpha + \beta$ and $\gamma + \delta$ are positive. Then (4.4) implies $\alpha k = \gamma k$ and thus $\alpha = \gamma$. If $\alpha = 0$, we get $b^\beta = b^\delta$, hence $\beta = \delta$, and thus

$$
(ab)^{i\alpha} b^{kw(\alpha+\beta)} = (ab)^{i\gamma} b^{kw(\gamma+\delta)}.
$$

If $\alpha \ne 0$, then using (4.5) we obtain that

$$
(ab)^{i\alpha} = (ab)^{i\alpha-i}(ab)^i = (ab)^{i\alpha-i}(ab)^i b^k = (ab)^{i\alpha} b^k,
$$

hence $(ab)^{i\alpha} = (ab)^{i\alpha} b^{kl}$ for any $l \in \mathbb{N}$, and since $\alpha = \gamma$, also in this case we have that

$$
(ab)^{i\alpha} b^{kw(\alpha+\beta)} = (ab)^{i\gamma} b^{kw(\gamma+\delta)}.
$$

Hence g is well-defined. It is easy to see that g is an endomorphism of S. Since every endomorphism of S is a power function, there exists $m \in \mathbb{N}$ such that $g(x) = x^m$ for any $x \in S$. Since $b^m = g(b) = b^{kw}$, it follows that $m = kw$, which together with (4.5) implies that $a^{kw} = a^m = g(a) = (ab)^i b^{kw} = (ab)^i$. Hence $a^{kw} = (ab)^i$ for

any $w \in \mathbb{N}$. In particular, $a^k = a^{2k} = (a^k)^2$, which is a contradiction, since S has no idempotent.

Case 2. Suppose $i = j + k$. Then $(ab)^i = (ab)^{j+k} = ((ab)^j b^k) a^k = (ab)^i a^k$, and we are in conditions of Case 1, with a and b interchanged. The same argument as in Case 1 shows that also Case 2 is impossible.

We have proved that $j < i$ and $i < j + k$. Now (4.4) shows that by setting

$$f(a^\alpha b^\beta) = b^{\alpha(j+k-i)+\beta(i-j)} \text{ for any } \alpha, \beta \in \mathbb{N} \cup \{0\} \text{ with } \alpha + \beta > 0$$

we obtain a well-defined map $f : S \to S$. It is easy to verify that f is an endomorphism of S, and since every endomorphism of S is a power function, there exists $m \in \mathbb{N}$ such that $f(x) = x^m$ for any $x \in S$. Hence

$$a^m = f(a) = b^{j+k-i}.$$

Thus there exist $m, n \in \mathbb{N}$ such that $a^m = b^n$. To complete the prove of (i) $\Rightarrow$ (ii), it suffices to show that m, n can be chosen to be relatively prime. Let $d = gcd\{m, n\}$. Then $m = dm_1$ and $n = dn_1$ for some relatively prime $m_1, n_1 \in \mathbb{N}$, and thus it suffices to show that $a^{m_1} = b^{n_1}$.

Since $a^m = b^n$, for any $\alpha, \beta, \gamma, \delta \in \mathbb{N} \cup \{0\}$ with $\alpha + \beta > 0$ and $\gamma + \delta > 0$ we have that if $a^\alpha b^\beta = a^\gamma b^\delta$, then

$$a^{n\alpha+m\beta} = a^{n\alpha}(a^m)^\beta = a^{n\alpha}(b^n)^\beta = (a^\alpha b^\beta)^n$$
$$= (a^\gamma b^\delta)^n = a^{n\gamma}(b^n)^\delta = a^{n\gamma}(a^m)^\delta = a^{n\gamma+m\delta},$$

and $n\alpha + m\beta = n\gamma + m\delta$ follows. Hence also $n_1\alpha + m_1\beta = n_1\gamma + m_1\delta$ and thus the map $h : S \to S$ given by

$$h(a^\alpha b^\beta) = b^{n_1\alpha+m_1\beta} \text{ for any } \alpha, \beta \in \mathbb{N} \cup \{0\} \text{ with } \alpha + \beta > 0$$

is well-defined. It is easy to see that h is an endomorphism of S. Since every endomorphism of S is a power function, there exists $l \in \mathbb{N}$ such that $h(x) = x^l$ for any $x \in S$. Since $b^l = h(b) = b^{m_1}$, we obtain $l = m_1$. Hence $a^{m_1} = a^l = h(a) = b^{n_1}$, as desired.

(ii) $\Rightarrow$ (iii) Assume (ii). To prove (iii) it suffices to show that S is isomorphic to a subsemigroup of the additive semigroup of positive integers $\mathbb{N}$. Note first that the same argument as in the last part of the proof of (i) $\Rightarrow$ (ii) shows that for any $\alpha, \beta, \gamma, \delta \in \mathbb{N} \cup \{0\}$ with $\alpha + \beta > 0$ and $\gamma + \delta > 0$, if $a^\alpha b^\beta = a^\gamma b^\delta$, then $n\alpha + m\beta = n\gamma + m\delta$. Hence the map $f : S \to \mathbb{N}$ given by

$$f(a^\alpha b^\beta) = n\alpha + m\beta \text{ for any } \alpha, \beta \in \mathbb{N} \cup \{0\} \text{ with } \alpha + \beta > 0,$$

is well-defined. Obviously, f is a semigroup homomorphism from S to the additive semigroup $\mathbb{N}$.

We show that f is injective. Assume $f(a^\alpha b^\beta) = f(a^\gamma b^\delta)$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{N} \cup \{0\}$ with $\alpha + \beta > 0$ and $\gamma + \delta > 0$. Then $n\alpha + m\beta = n\gamma + m\delta$. Since

$n(\alpha - \gamma) = m(\delta - \beta)$ and m, n are relatively prime, it follows that $\alpha = \gamma + lm$ and $\delta = \beta + ln$ for some integer l. Without loss of generality we can assume that $l \in \mathbb{N} \cup \{0\}$ (i.e., $\alpha \geq \gamma$). Hence

$$a^\alpha b^\beta = a^{\gamma + lm} b^\beta = a^\gamma (a^m)^l b^\beta = a^\gamma (b^n)^l b^\beta = a^\gamma b^{\beta + nl} = a^\gamma b^\delta,$$

which proves that f is an injection. Hence S is isomorphic to the subsemigroup $f(S) = \langle m, n \rangle$ of $\mathbb{N}$.

(iii) $\Rightarrow$ (i) is an immediate consequence of Theorem 4.1. $\square$

As the author was informed by M. Volkov, recently A.A. Borisov announced a solution of the Lesokhin–Oman problem for finitely generated cancellative commutative semigroups without idempotents.

References

1. Borisov, A.A.: On endomorphisms of finite commutative semigroups (Russian), Modern Algebra (Russian), Mezhvuz. Sb. Nauchn. Tr., No. 2(22), 14-17, Rostov-on-Don (1997)
2. Bourlès, H.: Fundamentals of Advanced Mathematics. 1. Categories, Algebraic Structures, Linear and Homological Algebra. ISTE Press, London (2017)
3. Clifford, A.H., Preston, G.B.: The Algebraic Theory of Semigroups. Vol. I. Mathematical Surveys, No. 7 American Mathematical Society, Providence, RI (1961)
4. Fuchs, L.: Abelian Groups. Publishing House of the Hungarian Academy of Sciences, Budapest (1958)
5. Geroldinger, A., Halter-Koch, F.: Non-unique Factorizations. Algebraic, Combinatorial and Analytic Theory. Pure and Applied Mathematics, vol. 278. CRC, Boca Raton, FL (2006)
6. Göbel, R., Shelah, S., Strüngmann, L.: Generalized E-rings. Rings, Modules, algebras, and Abelian Groups, 291–306, Lecture Notes in Pure and Appl. Math., vol. 236, Marcel Dekker, New York (2004)
7. Grillet, P.A.: Commutative Semigroups. Advances in Mathematics, vol. 2. Kluwer Academic Publishers, Dordrecht (2001)
8. Higgins, J.C.: Representing N-semigroups. Bull. Aust. Math. Soc. **1**, 115–125 (1969)
9. Krylov, P.A., Tuganbaev, A.A., Tsarev, A.V.: E-groups and E-rings (Russian). Itogi Nauki i Tekhniki. Ser. Sovrem. Mat. Pril. Temat. Obz. **159**, 111–132 (2019)
10. Kuptsov, A.I.: A property of the semigroup of endomorphisms of commutative regular semigroups (Russian), Semigroup Varieties and Semigroups of Endomorphisms (Russian), 80. Leningrad. Gos. Ped. Inst, Leningrad (1979)
11. Mazurek, R.: Semigroups whose endomorphisms are power functions. Semigroup Forum **88**(1), 67–75 (2014)
12. Oman, G.: Rings whose multiplicative endomorphisms are power functions. Semigroup Forum **86**(2), 272–278 (2013)

13. Schultz, P.: The endomorphism ring of the additive group of a ring. J. Aust. Math. Soc. **15**, 60–69 (1973)
14. Shevrin, L. N. (ed.): The Sverdlovsk Tetrad (Unsolved Problems of Semigroup Theory). Ural State University, Sverdlovsk (1969). English translation: Semigroup Forum **4**, 274–280, 373 (1972)
15. Vinsonhaler, C.: E-Rings and Related Structures, Non-Noetherian Commutative Ring Theory, 387–402, Math. Appl., vol. 520, Kluwer Academic Publishers, Dordrecht (2000)

Springer