ACZÉLIAN n-ARY SEMIGROUPS

MIGUEL COUCEIRO AND JEAN-LUC MARICHAL

Abstract. We show that the real continuous, symmetric, and cancellative n-ary semigroups are topologically order-isomorphic to additive real n-ary semigroups. The binary case ($n = 2$) was originally proved by Aczél [1]; there symmetry was redundant.

1. Introduction

Let I be a nontrivial real interval (i.e., nonempty and not a singleton) and let $n \geqslant 2$ be an integer. Recall that an n-ary function $f\colon I^n \to I$ is said to be *associative* if it solves the following system of $n-1$ functional equations:

$$\begin{aligned} & f\big(x_1,\ldots,f(x_i,\ldots,x_{i+n-1}),x_{i+n},\ldots,x_{2n-1}\big) \\ & \quad = \quad f\big(x_1,\ldots,x_i,f(x_{i+1},\ldots,x_{i+n}),\ldots,x_{2n-1}\big), \quad i=1,\ldots,n-1. \end{aligned}$$

The pair (I,f) is then called an n-ary semigroup (see Dörnte [5] and Post [8]).

We say that a function $f\colon I^n \to I$ is *cancellative* if it is one-to-one in each variable; that is, for every $k \in [n] = \{1,\ldots,n\}$ and every $\mathbf{x} = (x_1,\ldots,x_n) \in I^n$ and $\mathbf{x}' = (x'_1,\ldots,x'_n) \in I^n$,

$$\big(x_i = x'_i \;\text{ for all } i \in [n] \smallsetminus \{k\} \quad \text{and} \quad f(\mathbf{x}) = f(\mathbf{x}')\big) \quad \Rightarrow \quad x_k = x'_k\,.$$

In this paper we present a complete description of those associative functions $f\colon I^n \to I$ which are continuous, symmetric, and cancellative. Our main result can be stated as follows.

Main Theorem. *A function $f\colon I^n \to I$ is continuous, symmetric, cancellative, and associative if and only if there exists a continuous and strictly monotonic function $\varphi\colon I \to J$ such that*

$$f(\mathbf{x}) = \varphi^{-1}\left(\sum_{i=1}^{n}\varphi(x_i)\right), \tag{1}$$

where J is a real interval of one of the forms $]-\infty,b[$, $]-\infty,b]$, $]a,\infty[$, $[a,\infty[$ or $\mathbb{R} = \,]-\infty,\infty[$ ($b \leqslant 0 \leqslant a$). In this case I is necessarily open at least on one end. Moreover, φ can be chosen to be strictly increasing. In other words, the n-ary semigroup (I,f) is topologically order-isomorphic to the n-ary semigroup $(J,+)$.

The binary case ($n = 2$) of the Main Theorem, for which symmetry is not needed, was first stated and proved by J. Aczél [1]. A shorter, more technical proof of Aczél's result was then provided by Craigen and Páles [4] (see also [2] for a recent survey). The corresponding binary semigroups are called *Aczélian* (see Ling [6, Section 3.2]).

Date: July 25, 2011.
2010 *Mathematics Subject Classification.* Primary 20N15, 39B22; Secondary 20M14.
Key words and phrases. n-ary semigroup, Aczélian semigroup, cancellativity, continuity.

We say that an n-ary semigroup is *Aczélian* if it satisfies the assumptions of the Main Theorem. Thus the Main Theorem provides an explicit description of the class of Aczélian n-ary semigroups. Although this result is not a trivial derivation of the binary case, we prove it by following more or less the same steps as in [4].

The following example shows that the symmetry assumption is necessary for every odd integer $n \geqslant 3$.

Example 1.1. Let $n \geqslant 3$ be an odd integer. The function $f\colon \mathbb{R}^n \to \mathbb{R}$, defined by

$$f(\mathbf{x}) = \sum_{i=1}^{n} (-1)^{i-1} x_i \, ,$$

is continuous, cancellative, and associative. However, it cannot be of the form (1) with a continuous and strictly monotonic function φ. Indeed, if the latter would be the case, then by identifying the variables, we would have $f(x^n) = x$ and hence $\varphi(x) = \varphi(f(x^n)) = n\,\varphi(x)$, a contradiction.

This paper is organized as follows. In Section 2 we show how n-ary associative functions can be extended to associative functions of certain higher arities. In Section 3 we provide the proof of the Main Theorem.

To avoid cumbersome notation, we henceforth regard tuples $\mathbf{x}$ in I^n as n-strings over I and we write $|\mathbf{x}| = n$. The 0-string or *empty* string is denoted by ε so that $I^0 = \{\varepsilon\}$. We denote by I^* the set of all strings over I, that is, $I^* = \bigcup_{n \in \mathbb{N}} I^n$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$. Moreover, we consider I^* endowed with concatenation for which we adopt the juxtaposition notation. For instance, if $\mathbf{x} \in I^n$, $y \in I$, and $\mathbf{z} \in I^m$, then $\mathbf{x}y\mathbf{z} \in I^{n+1+m}$.[1] Furthermore, for $x \in I$, we use the short-hand notation $x^m = x \cdots x \in I^m$. Given a function $g\colon I^* \to I$, we denote by g_m the restriction of g to I^m, i.e. $g_m := g|_{I^m}$. We convey that g_0 is defined by $g_0(\varepsilon) = \varepsilon$.

2. Associative extensions

Recall that a binary function $f\colon I^2 \to I$ is said to be *associative* if

$$f(f(xy)z) = f(xf(yz)) \qquad \text{for all } x, y, z \in I.$$

Using an infix notation, we can also write this property as

$$(x \diamond y) \diamond z = x \diamond (y \diamond z) \qquad \text{for all } x, y, z \in I.$$

Since associativity expresses that the order in which variables are bracketed is not relevant, it can be easily extended to functions $g\colon I^* \to I$ by defining

$$g_m(x_1 \cdots x_m) = x_1 \diamond \cdots \diamond x_m$$

for every integer $m \geqslant 2$. The latter definition can be reformulated in prefix notation as $g_2 = f$ and

$$g_m(x_1 \cdots x_m) = g_2(g_2(\cdots g_2(g_2(g_2(x_1 x_2) x_3) x_4) \cdots) x_m) \tag{2}$$

for every $m > 2$.[2]

---

[1] Using this convenient notation, we immediately see that a function $f\colon I^n \to I$ is associative if and only if we have $f(\mathbf{x}\, f(\mathbf{y})\mathbf{z}) = f(\mathbf{x}'\, f(\mathbf{y}')\mathbf{z}')$ for every $\mathbf{xyz}, \mathbf{x}'\mathbf{y}'\mathbf{z}' \in I^{2n-1}$ such that $\mathbf{y}, \mathbf{y}' \in I^n$ and $\mathbf{xyz} = \mathbf{x}'\mathbf{y}'\mathbf{z}'$. Similarly, f is cancellative if and only if, for every $\mathbf{xz} \in I^{n-1}$ and every $y, y' \in I$, the equality $f(\mathbf{x}y\mathbf{z}) = f(\mathbf{x}y'\mathbf{z})$ implies $y = y'$.

[2] Or equivalently, $g_2 = f$ and $g_m(x_1 \cdots x_m) = g_2(g_{m-1}(x_1 \cdots x_{m-1}) x_m)$ for every $m > 2$.

Note that the unary function g_1 is not involved in this construction and so it could be chosen arbitrarily. However, as we will see in Proposition 2.2, it is convenient to ask g_1 to satisfy the following condition:

$$g_1 \circ g = g \quad \text{and} \quad g(\mathbf{x}\, g_1(y)\mathbf{z}) = g(\mathbf{x}y\mathbf{z}) \quad \text{for all } \mathbf{x}y\mathbf{z} \in I^*. \tag{3}$$

Definition 2.1. A function $g{:}\, I^* \to I$ is said to be *associative* if

(i) g_2 is associative,
(ii) condition (2) holds for every $m > 2$ and every $x_1, \ldots, x_m \in I$, and
(iii) condition (3) holds.

By definition, an associative function $g{:}\, I^* \to I$ can always be constructed from a binary associative function $f{:}\, I^2 \to I$ by defining $g_2 = f$, using (2), and choosing a unary function g_1 satisfying (3) (e.g., the identity function).[3] Such a function g, which is completely determined by g_1 and $g_2 = f$, will be called an *associative extension* of f.

The following proposition provides concise reformulations of associativity of functions $g{:}\, I^* \to I$ and justifies condition (3). We will prove a more general statement in Proposition 2.5. The equivalence of assertions (ii)–(iv) was proved in [3].

Proposition 2.2. *Let $g{:}\, I^* \to I$ be a function. The following assertions are equivalent.*

(i) *g is associative.*
(ii) $g(\mathbf{x}\, g(\mathbf{y})\mathbf{z}) = g(\mathbf{x}'g(\mathbf{y}')\mathbf{z}')$ *for every* $\mathbf{x}\mathbf{y}\mathbf{z}, \mathbf{x}'\mathbf{y}'\mathbf{z}' \in I^*$ *such that* $\mathbf{x}\mathbf{y}\mathbf{z} = \mathbf{x}'\mathbf{y}'\mathbf{z}'$.
(iii) $g(\mathbf{x}\, g(\mathbf{y})\mathbf{z}) = g(\mathbf{x}\mathbf{y}\mathbf{z})$ *for every* $\mathbf{x}\mathbf{y}\mathbf{z} \in I^*$.
(iv) $g(g(\mathbf{x})g(\mathbf{y})) = g(\mathbf{x}\mathbf{y})$ *for every* $\mathbf{x}\mathbf{y} \in I^*$.

For any integer $n \geqslant 2$, define the sets

$$A_n = \{m \in \mathbb{N} : m \equiv 1 \pmod{n-1}\} \qquad \text{and} \qquad I^{(n)} = \bigcup_{m \in A_n} I^m = I \times (I^{n-1})^*.$$

Just as associativity for binary functions can be extended to functions $g{:}\, I^* \to I$, one can also extend the associativity of n-ary functions to functions $g{:}\, I^{(n)} \to I$ as follows.[4] Given an associative function $f{:}\, I^n \to I$, we define $g{:}\, I^{(n)} \to I$ as $g_n = f$ and

$$g_m(x_1 \cdots x_m) = g_n(g_n(\cdots g_n(g_n(x_1 \cdots x_n)x_{n+1} \cdots x_{2n-1}) \cdots)x_{m-n+2} \cdots x_m) \tag{4}$$

for every $m \in A_n$ and $m > n$.[5]

Once again, the unary function g_1 can be chosen arbitrarily. However, we ask g_1 to satisfy the following condition:

$$g_1 \circ g = g \quad \text{and} \quad g(\mathbf{x}\, g_1(y)\mathbf{z}) = g(\mathbf{x}y\mathbf{z}) \quad \text{for all } \mathbf{x}y\mathbf{z} \in I^{(n)}. \tag{5}$$

Definition 2.3. A function $g{:}\, I^{(n)} \to I$ is said to be *n-associative* if

(i) g_n is associative,
(ii) condition (4) holds for every $m \in A_n$, $m > n$, and every $x_1, \ldots, x_m \in I$, and
(iii) condition (5) holds.

[3] Note that g_1 necessarily solves the idempotency equation $g_1 \circ g_1 = g_1$.

[4] This construction is inspired from Dörnte [5] and Post [8].

[5] Or equivalently, $g_n = f$ and $g_m(x_1 \cdots x_m) = g_n(g_{m-n+1}(x_1 \cdots x_{m-n+1})x_{m-n} \cdots x_m)$ for every $m \in A_n$ and $m > n$.

By definition, an n-associative function $g\colon I^{(n)} \to I$ can always be constructed from an n-ary associative function $f\colon I^n \to I$ by defining $g_n = f$, using (4), and choosing a unary function g_1 satisfying (5) (e.g., the identity function). Such a function g, which is completely determined by g_1 and $g_n = f$, will be called an *n-associative extension* of f.

Example 2.4. From the ternary associative function $f\colon \mathbb{R}^3 \to \mathbb{R}$, defined by $f(x_1x_2x_3) = x_1 - x_2 + x_3$, we can construct the 3-associative extension $g\colon \mathbb{R}^{(3)} \to \mathbb{R}$ as

$$g_m(x_1\cdots x_m) = \sum_{i=1}^{m}(-1)^{i-1}x_i \qquad (m \geqslant 3,\ \text{odd}),$$

for which (5) provides the unique solution $g_1 = \mathrm{id}$.

The following proposition generalizes Proposition 2.2 and provides concise reformulations of n-associativity of functions $g\colon I^{(n)} \to I$ and justifies condition (5).

Proposition 2.5. *Let $g\colon I^{(n)} \to I$ be a function. The following assertions are equivalent.*

- (*i*) *g is n-associative.*
- (*ii*) *$g_1 \circ g = g$ and $g(\mathbf{x}\,g(\mathbf{y})\mathbf{z}) = g(\mathbf{x}'g(\mathbf{y}')\mathbf{z}')$ for every $\mathbf{xyz}, \mathbf{x}'\mathbf{y}'\mathbf{z}' \in I^{(n)}$ such that $\mathbf{y}, \mathbf{y}' \in I^{(n)}$ and $\mathbf{xyz} = \mathbf{x}'\mathbf{y}'\mathbf{z}'$.*
- (*iii*) *$g(\mathbf{x}\,g(\mathbf{y})\mathbf{z}) = g(\mathbf{xyz})$ for every $\mathbf{xyz} \in I^{(n)}$ such that $\mathbf{y} \in I^{(n)}$.*
- (*iv*) *$g_1 \circ g = g$ and $g(g(\mathbf{x}_1)\cdots g(\mathbf{x}_n)) = g(\mathbf{x}_1\cdots \mathbf{x}_n)$ for every $\mathbf{x}_1, \ldots, \mathbf{x}_n \in I^{(n)}$.*

Proof. Implications $(iii) \Rightarrow (i)$, $(iii) \Rightarrow (ii)$, and $(iii) \Rightarrow (iv)$ are easy to verify.

To prove $(ii) \Rightarrow (iii)$ simply take $\mathbf{y}' = \mathbf{xyz}$ (i.e., $\mathbf{x}'\mathbf{z}' = \varepsilon$).

Let us now prove that $(iv) \Rightarrow (iii)$. Let $\mathbf{xyz} \in I^{(n)}$ such that $\mathbf{y} \in I^{(n)}$. We write $\mathbf{x}\,g(\mathbf{y})\mathbf{z} = t_1\cdots t_m$, with $t_k = g(\mathbf{y})$. By (iv) we have

$$g(\mathbf{x}\,g(\mathbf{y})\mathbf{z}) = g(t_1\cdots t_m) = g\big(g(t_1)\cdots g(t_{n-1})g(t_n\cdots t_m)\big).$$

If $k \leqslant n-1$, then

$$\begin{aligned} g(\mathbf{x}\,g(\mathbf{y})\mathbf{z}) &= g\big(g(t_1)\cdots g(t_k)\cdots g(t_{n-1})g(t_n\cdots t_m)\big) \\ &= g\big(g(t_1)\cdots g(\mathbf{y})\cdots g(t_{n-1})g(t_n\cdots t_m)\big) = g(\mathbf{xyz}). \end{aligned}$$

If $k \geqslant n$, we proceed similarly with $g(t_n\cdots t_m)$, unless $n = m$ in which case the result follows immediately.

Let us establish that $(i) \Rightarrow (iii)$. We only need to prove that $g(\mathbf{x}\,g(\mathbf{y})\mathbf{z}) = g(\mathbf{xyz})$ for every $\mathbf{xyz} \in I^{(n)}$ such that $|\mathbf{y}| \geqslant 2$ and $|\mathbf{xz}| \geqslant 1$. Using (4) twice and the associativity of g_n, we can rewrite the function $\mathbf{xyz} \mapsto g(\mathbf{x}\,g(\mathbf{y})\mathbf{z})$ in terms of nested g_n's only. Then, using the associativity of g_n again, we can move all the g_n's to the left to obtain the right-hand side of (4), which reduces to $g(\mathbf{xyz})$.

To illustrate, consider the following example with $n = 3$:

$$\begin{aligned} g(x_1x_2x_3\,g(x_4x_5x_6x_7x_8)x_9) &= g(x_1\,g(x_2x_3\,g(x_4\,g(x_5x_6x_7)x_8))x_9) \\ &= g(g(g(g(x_1x_2x_3)x_4x_5)x_6x_7)x_8x_9) \\ &= g(x_1x_2x_3x_4x_5x_6x_7x_8x_9). \quad \square \end{aligned}$$

Remark 1. Proposition 2.2 follows from Proposition 2.5. Note that the condition $g_1 \circ g = g$ is not needed in assertions (ii) and (iv) of Proposition 2.2 since I^* is used instead of $I^{(n)}$, thus allowing the use of the empty string ε.

3. Proof of the Main Theorem

It is easy to show that the condition in the Main Theorem is sufficient. To show that the condition is necessary, let I be a nontrivial real interval, let $f\colon I^n \to I$ be a continuous, symmetric, cancellative, and associative function, and let $g\colon I^{(n)} \to I$ be the unique n-associative extension of f such that $g_1 = \mathrm{id}$ (see the observation following Definition 2.3).

Claim 1. f is strictly increasing in each variable.

Proof. Since f is continuous and cancellative, it must be strictly monotonic in each variable. Suppose it is strictly decreasing in the first variable. Then, by associativity, for every $\mathbf{y} \in I^{n-1}$, $u \in I$, and $\mathbf{v} \in I^{n-2}$, the unary function $x \mapsto f(f(x\mathbf{y})u\mathbf{v}) = f(x\,f(\mathbf{y}u)\mathbf{v})$ is both strictly increasing and strictly decreasing, which leads to a contradiction. Thus f must be strictly increasing in the first variable and hence in every variable by symmetry. □

An element $e \in I$ is said to be an *idempotent* for f if $f(e^n) = e$. For instance, any real number is an idempotent for the function defined in Example 1.1.

Claim 2. There cannot be two distinct idempotents for f.

Proof. Otherwise, if d and e were distinct idempotents, we would have

$$f(d\,e^{n-1}) = f(f(d^n)\,e^{n-1}) = f(d\,f(d^{n-1}e)\,e^{n-2})$$

and hence (by cancellation), $e = f(d^{n-1}e) = f(e\,d^{n-1})$. Similarly, $d = f(e^{n-1}d) = f(d\,e^{n-1})$. Now, if $e < d$, then $d = f(d\,e^{n-1}) < f(d^{n-1}e) = e$ (by Claim 1), a contradiction. We arrive at a similar contradiction if $d < e$. □

Because of Claim 2, there is a $c \in I$ such that either $c < f(c^n)$ or $c > f(c^n)$. We assume w.l.o.g. that the former holds and fix such a c. The latter case can be dealt with similarly.

Claim 3. For all fixed $x \in I$, we have $x < f(x\,c^{n-1})$. Thus the sequence $x_m = f(x_{m-1}c^{n-1})$ strictly increases, and $\lim x_m \notin I$ (hence $\lim x_m = \sup I$ and I is open from above).

Proof. Since $c < f(c^n)$, we have $f(c\,x^{n-1}) < f(f(c^n)\,x^{n-1}) = f(c\,f(c^{n-1}x)\,x^{n-2})$ and hence (by strict monotonicity) $x < f(c^{n-1}x) = f(x\,c^{n-1})$. Thus $x_m = f(x_{m-1}c^{n-1}) > x_{m-1}$. If $\lim x_m = x'$ and $x' \in I$, continuity gives the following:

$$x' = \lim x_m = \lim f(x_{m-1}c^{n-1}) = f(\lim x_{m-1}c^{n-1}) = f(x'c^{n-1}),$$

a contradiction. Thus $x' \notin I$, so $\lim x_m = \sup I$. □

Hereinafter we work on the extended real line so that suprema of arbitrary sets exist and all monotone sequences converge.

Claim 4. Let $x \in I$ and let $j,k,p,q \in \mathbb{N}$ such that $j+1,k,p,q+1 \in A_n$. Then we have

$$g(c^p) > g(x\,c^q) \quad\Leftrightarrow\quad g(c^{kp}) > g(x^k c^{kq}) \quad\Leftrightarrow\quad g(c^{p+j}) > g(x\,c^{q+j}).$$

The same equivalence holds if "$<$" or "$=$" replaces "$>$".

Proof. Assume that $g(c^p) > g(x\,c^q)$. Then, by Proposition 2.5(iv), Claim 1, and symmetry, we have $g(c^{kp}) = g(g(c^p)^k) > g(g(x\,c^q)^k) = g(x^k c^{kq})$, which proves the first equivalence (since the same conclusion clearly holds if "$<$" or "$=$" replaces

"$>$"). For the second equivalence, assume again that $g(c^p) > g(x\,c^q)$. Then, as before, we have $g(c^{p+j}) = g(g(c^p)\,c^j) > g(g(x\,c^q)\,c^j) = g(x\,c^{q+j})$. □

Let x be any fixed element of I. Define S_x to be the subset of all rational numbers r for which there exist $k,p,q \in \mathbb{N}$ such that $k,p,q+1 \in A_n$, $g(c^p) > g(x^k c^q)$, and $r = (p-q)/k$. Now, if $r = (p-q)/k = (p'-q')/k'$, then we have $pk' + q'k = p'k + qk'$ and it follows from Claim 4 that

$$\begin{aligned} g(c^p) > g(x^k c^q) \quad &\Leftrightarrow \quad g(c^{pk'}) > g(x^{kk'}c^{qk'}) \\ &\Leftrightarrow \quad g(c^{pk'+q'k}) > g(x^{kk'}c^{qk'+q'k}) \\ &\Leftrightarrow \quad g(c^{p'k+qk'}) > g(x^{kk'}c^{q'k+qk'}) \\ &\Leftrightarrow \quad g(c^{p'k}) > g(x^{kk'}c^{q'k}) \\ &\Leftrightarrow \quad g(c^{p'}) > g(x^{k'}c^{q'}). \end{aligned}$$

Hence S_x is in fact the subset of rational numbers r for which every representation $r = (p-q)/k$ with $k,p,q+1 \in A_n$ satisfies $g(c^p) > g(x^k c^q)$.

Claim 5. The set $S = \{\frac{p-q}{k} : k,p,q+1 \in A_n\}$ is dense in $\mathbb{R}$.

Proof. For every $a,b \in \mathbb{N}$, the sequence

$$x_m = \frac{1 \pm a\,m\,(n-1)}{1 + b\,m\,(n-1)}$$

of S converges to $\pm a/b$. Thus S is dense in $\mathbb{Q}$ and hence (by transitivity) in $\mathbb{R}$. □

Claim 6. Any two numbers $r, r' \in S$ may be written $r = (p-q)/k$, $r' = (p'-q)/k$ for suitable $k,p,p',q+1 \in A_n$.

Proof. Let $r = (p-q)/k$ and $r' = (p'-q')/k'$, with $k,k',p,p',q+1,q'+1 \in A_n$. Assume w.l.o.g. that $r' > r$. Setting $\tilde{k} = k\,k'$, $\tilde{q} = |\tilde{k}\,r - 1|$, $\tilde{p} = \tilde{k}\,r + \tilde{q}$, and $\tilde{p}' = \tilde{k}\,r' + \tilde{q}$, we have $r = (\tilde{p}-\tilde{q})/\tilde{k}$, $r' = (\tilde{p}'-\tilde{q})/\tilde{k}$ with $\tilde{k},\tilde{p},\tilde{p}',\tilde{q}+1 \in A_n$. □

Claim 7. S_x is a nonempty, proper, and upper subset of S ("upper" means that if $r \in S_x$ and $r' \in S$, $r' > r$, then $r' \in S_x$).

Proof. To show that S_x is an upper subset, let $r = (p-q)/k \in S_x$ and $r' = (p'-q)/k > r$ (cf. Claim 6). Then $p' > p$ and, since $p,p' \in A_n$, we have $p' = p + j(n-1)$ for some integer $j \geqslant 1$. Using the definition of S_x and the first part of Claim 3, we obtain

$$\begin{aligned} g(x^k c^q) \;<\; g(c^p) \;&<\; g(g(c^p)\,c^{n-1}) \;=\; g(c^p c^{n-1}) \\ &<\; g(g(c^p c^{n-1})\,c^{n-1}) \;=\; g(c^p c^{2(n-1)}) \\ &<\; \cdots \\ &<\; g(c^p c^{j(n-1)}) \;=\; g(c^{p'}). \end{aligned}$$

Hence $r' \in S_x$. Now, by Claim 3, $\lim f(c^{m(n-1)+1}) = \sup I > g(x\,c^{n-1})$, and hence there is some $p \in A_n$ with $g(c^p) > g(x\,c^{n-1})$. Hence $r = (p-(n-1))/1 \in S_x$, and so S_x is nonempty. Similarly, since $\lim g(x\,c^{m(n-1)}) = \sup I$, there must a q such that $q+1 \in A_n$ and $g(c) < g(x\,c^q)$, and so $(1-q)/1 \notin S_x$. □

Now, by Claim 7, S_x is precisely the set of elements in S which are greater (and possibly equal to) $\inf S_x$. Using this fact, let $\varphi\colon I \to \mathbb{R}$ be the function given by

$$\varphi(x) := \inf S_x\,.$$

Claim 8. If $g(c^p) = g(x^k c^q)$, then $\varphi(x) = (p-q)/k$. In particular, $\varphi(c) = 1$.

Proof. Note that $g(c^p) = g(x^k c^q)$ implies $r = (p-q)/k \notin S_x$. Moreover, by Claim 7 it follows that if $r' = (p'-q)/k > r$ (resp. $r' < r$), then $g(c^{p'}) > g(c^p) = g(x^k c^q)$ (resp. $g(c^{p'}) < g(c^p) = g(x^k c^q)$), and hence $r' \in S_x$ (resp. $r' \notin S_x$). Thus $\inf S_x = (p-q)/k$ by Claim 5. For the last claim just note that $g(c^{q+1}) = g(c\,c^q)$. □

Claim 9. We have $\varphi(g(x_1\cdots x_n)) = \sum_{i=1}^n \varphi(x_i)$ for every $x_1,\ldots,x_n \in I$.

Proof. Let $r_i = (p_i - q)/k > \varphi(x_i)$ for all $i \in [n]$. Then $g(c^{p_i}) > g(x_i^k c^q)$, and by Proposition 2.5(iv), Claim 1, and symmetry, we have

$$g(c^{\sum_{i=1}^n p_i}) = g(g(c^{p_1})\cdots g(c^{p_n})) > g(g(x_1^k c^q)\cdots g(x_n^k c^q)) = g(g(x_1\cdots x_n)^k c^{nq}).$$

By Claim 8, $(\sum_{i=1}^n p_i - nq)/k \in S_{g(x_1\cdots x_n)}$. Thus $\sum_{i=1}^n r_i > \varphi(g(x_1\cdots x_n))$. Similarly, if $r_i \leqslant \varphi(x_i)$ for all $i \in [n]$, then $\sum_{i=1}^n r_i \leqslant \varphi(g(x_1\cdots x_n))$. The result then follows from Claim 5. □

Claim 10. φ is nondecreasing.

Proof. Suppose $y > x$ and $(p-q)/k \in S_y$. Then $g(c^p) > g(y^k c^q) > g(x^k c^q)$ and hence $S_y \subseteq S_x$ and so $\varphi(y) = \inf S_y \geqslant \inf S_x = \varphi(x)$. □

Claim 11. φ is continuous.

Proof. Since φ is nondecreasing, the only possible sort of discontinuity is a gap discontinuity. Hence, if φ is discontinuous, there must exist $x, y \in I$, say $x < y$, and an interval, and thus a rational $r \notin \varphi(I)$, such that $\varphi(x) < r < \varphi(y)$. Now if $r = (p-q)/k$, then $g(x^k c^q) < g(c^p) \leqslant g(y^k c^q)$. By continuity of g_{k+q}, there is $t \in \,]x,y]$ such that $g(c^p) = g(t^k c^q)$. By Claim 8 it then follows that $\varphi(t) = r$, which yields the desired contradiction. □

Claim 12. φ is strictly increasing.

Proof. For the sake of contradiction, suppose that there are $x, y \in I$ such that $x < y$ and $\varphi(x) = \varphi(y) = a$. Since φ is nondecreasing, there is an interval I' containing x and y, and such that $\varphi(z) = a$, for all $z \in I'$. Let I' be the largest interval having this property, and set $t = \sup I'$. If $t \notin I$, then for every $z > x$, $\varphi(z) = a$. Now $g(x\,c^{n-1}) > x$ (by Claim 3) and hence $a = \varphi(g(x\,c^{n-1})) = a + (n-1) > a$ (by Claim 9), a contradiction. Thus $t \in I$, and $\varphi(t) = a$ by Claim 11. We have $g(x\,t^{n-1}) < g(t^n)$ and, by Claim 3, there exists q such that $q+1 \in A_n$ and $g(t^n) < g(x\,c^{q(n-1)}) = g(x\,g(c^q)^{n-1})$ and $g(c^q) > t$. By continuity of g_n, there is $z \in I$ such that $t < z < g(c^q)$ (and so $z \notin I'$) and $g(x\,z^{n-1}) = g(t^n)$. Thus

$$a + (n-1)\,\varphi(z) = \varphi(x) + (n-1)\,\varphi(z) = \varphi(g(x\,z^{n-1})) = \varphi(g(t^n)) = n\,\varphi(t) = n\,a\,,$$

and we obtain $\varphi(z) = a$, so $z \in I'$, a contradiction. □

Thus φ is a continuous strictly increasing n-ary semigroup homomorphism and, by Claim 9, its range J is a connected real additive n-ary semigroup. Hence the only possibilities for J are $]-\infty,b[$, $]-\infty,b]$, $]a,\infty[$, $[a,\infty[$ or $]-\infty,\infty[$ $(b \leqslant 0 \leqslant a)$; see final comments in [4]. This completes the proof of the Main Theorem. □

Remark 2. The function φ is determined up to a multiplicative constant, that is, with φ all functions $\psi = r\,\varphi$ $(r \neq 0)$ belong to the same function f, and only these; see the "Uniqueness" section in [2].

Remark 3. An n-ary semigroup (I,f) is said to be *reducible to* (or *derived from*) a binary semigroup $(I,\diamond)$ if there is an associative extension $g\colon I^*\to I$ of $\diamond$ such that $g_n=f$; that is, $f(x_1\cdots x_n)=x_1\diamond\cdots\diamond x_n$ (see [5, 8]). The Main Theorem shows that every Aczélian n-ary semigroup is reducible. The n-ary semigroup given in Example 1.1 is not reducible (see [7]). Finding necessary and sufficient conditions for an n-ary semigroup to be reducible remains an interesting open problem (see [3]).

Acknowledgments

The authors wish to thank Judita Dascăl, Pierre Mathonet, and Michel Rigo for helpful comments and suggestions. This research is supported by the internal research project F1R-MTH-PUL-09MRDO of the University of Luxembourg.

References

[1] J. Aczél. Sur les opérations définies pour nombres réels. *Bull. Soc. Math. France*, 76:59–64, 1949.

[2] J. Aczél. The associativity equation re-revisited. In G. Erikson and Y. Zhai, editors, *Bayesian Inference and Maximum Entropy Methods in Science and Engineering*, pages 195-203. American Institute of Physics, Melville-New York, 2004.

[3] M. Couceiro and J.-L. Marichal. Associative polynomial functions over bounded distributive lattices. *Order*, 28(1):1–8, 2011.

[4] R. Craigen and Zs. Páles. The associativity equation revisited. *Aeq. Math.*, 37:306–312, 1989.

[5] W. Dörnte. Untersuchengen über einen verallgemeinerten Gruppenbegriff. *Math. Z.*, 29:1–19, 1928.

[6] C.H. Ling Representation of associative functions. *Publ. Math. Debrecen*, 12:189–212, 1965.

[7] J.-L. Marichal and P. Mathonet. A description of n-ary semigroups polynomial-derived from integral domains. *Semigroup Forum.* In press.

[8] E. L. Post. Polyadic groups, *Trans. Amer. Math. Soc.*, 48:208–350, 1940.

Mathematics Research Unit, FSTC, University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: miguel.couceiro[at]uni.lu

Mathematics Research Unit, FSTC, University of Luxembourg, 6, rue Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg

E-mail address: jean-luc.marichal[at]uni.lu