

ON THE ALGEBRAIC STRUCTURE OF PRIMITIVE RECURSIVE FUNCTIONS

by ISTVÁN SZALKAI in Budapest (Hungary)¹⁾

§ 0. In this paper we consider functions f from \mathbb{N} to \mathbb{N} . By o , s , p , sg we mean the functions which are given by

$$o(n) = 0, \quad s(n) = n + 1, \quad p(n) = \begin{cases} 0 & \text{if } n = 0, \\ n - 1 & \text{if } n > 0, \end{cases} \quad sg(n) = \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \end{cases}$$

respectively. For any $c \in \mathbb{N}$ let \bar{c} be the function from \mathbb{N} to \mathbb{N} which is constant equal c and by $a(n)$ we mean the quadratic residuum of n , i.e. the distance between n and the greatest square number not greater than n . By \circ and $+$ we denote the operators of composition and addition of arithmetical functions respectively. For an arbitrary function $f: \mathbb{N} \rightarrow \mathbb{N}$ and a natural number m we denote by $f^{\square(m)}$ the iteration of f from place m , i.e. $f^{\square(m)}$ is inductively defined by

$$f^{\square(m)}(0) = m, \quad f^{\square(m)}(n + 1) = f(f^{\square(m)}(n)).$$

Instead of $\square(0)$ we write \square .

The first characterizations of the class PR of all primitive recursive functions of only one variable ([9]) and of the class R of all general recursive functions of only one variable ([6]) were rather complicated. Gradually the characterizations and the proofs were simplified. The strongest result for PR seems to be the following, proved by JULIA ROBINSON in [7]: PR can be generated from two suitable functions u, v by the help of the operators \circ and \square . However, there does not exist a single function which generates PR with these operators. This fact is my Theorem 3, a special case of my Theorem 2 or Theorem 2A. In [7] J. ROBINSON proves a similar result: There is no single function from which PR can be obtained by \circ and $\square(m)$, where various values of m may be used. Her result is another generalization of my Theorem 3, but my proof seems easier to understand.

Similar results were proved by J. ROBINSON for R in [6] and [8] (some results of [6] can also be found in [4]). Namely she proves in [6] that there are two suitable complicated functions which generate R by the help of the operators \circ and $^{-1}$ (where $f^{-1}(x) = \min\{y: f(y) = x\}$ for a surjective function f). For proving this fact she uses a certain operation $*$ "mirror", but my Theorem 1 says that her method is not applicable in the general case P , because this operation is an endomorphism on $\langle \text{PR}, \circ, \square \rangle$. In [8] she examines finally the so-called generalized recursion scheme and proves that every general recursive function of one variable can be obtained from o and s by repeated compositions and general recursions from previously defined functions. If we allow only one of the operators \circ and \square , it is easy to see that we need infinitely many initial functions but till now I have not found a really good set of such initial functions.

¹⁾ The author thanks EMIL W. KISS for his useful remarks.

§ 1. In this section we are dealing with the endomorphisms of the structure $\langle \text{PR}, \circ, \square \rangle$. For every f we have $f^{\square} = \mathbf{o}$, therefore \mathbf{o} is the only fixed point of \square . We denote by $\text{End}(\mathfrak{A})$ the set of all endomorphisms of an algebraic structure \mathfrak{A} . It is obvious that \mathbf{o} is the null-element of PR, i.e. $\mathbf{o} \circ \mathbf{o} = \mathbf{o}$ and $\mathbf{o}^{\square} = \mathbf{o}$. So we get that \mathbf{Id} and \mathbf{O} are elements of $\text{End}(\langle \text{PR}, \circ, \square \rangle)$, where $\mathbf{Id}(f) = f$ and $\mathbf{O}(f) = \mathbf{o}$ for every element f of PR. In Theorem 1 we prove that $\text{End}(\langle \text{PR}, \circ, \square \rangle) = \{\mathbf{Id}, \mathbf{O}\}$. It is easy to see that for $c \in \mathbf{N}$, $c \neq 0$, if $L(f) = \bar{c}$ for every $f \in \text{PR}$, then $L \in \text{End}(\langle \text{PR}, \circ \rangle)$ and $L \notin \text{End}(\langle \text{PR}, \square \rangle)$. Conversely $L_{sg}, \square \in \text{End}(\langle \text{PR}, \square \rangle) - \text{End}(\langle \text{PR}, \circ \rangle)$, where $\square(f) = f^{\square}$ and $L_{sg}(f) = sg \circ f \circ sg$.

Lemma 1. *Let $u, v \in \text{PR}$ be arbitrary functions such that $v \circ u \neq \text{id}$ and u is not constant. Let $L(f) = u \circ f \circ v$ for every $f \in \text{PR}$. Then $L \notin \text{End}(\langle \text{PR}, \circ \rangle)$.*

Proof. Let x_1, x_2, y and z natural numbers such that $v \circ u(z) = y \neq z$ and $u(x_1) \neq u(x_2)$. Furthermore let $f, g \in \text{PR}$ such that $g(v(0)) = z$ and $f(z) = x_1, f(y) = x_2$. Then

$$\begin{aligned} L(f \circ g)(0) &= (u \circ f \circ g \circ v)(0) = u(x_1) \\ &\neq u(x_2) = (u \circ f \circ v \circ u \circ g \circ v)(0) = [L(f) \circ L(g)](0). \quad \square \end{aligned}$$

In consideration of this lemma the question arises whether there are functions u and v such that $f^{\square} = u \circ f \circ v$ for every $f \in \text{PR}$. It is clear that the answer is no: By the definition of \square we might have $0 = f^{\square}(0) = u(f(v(0)))$ for every $f \in \text{PR}$. For every natural number n there exists a primitive recursive function f such that $f(v(0)) = n$ and so $0 = f^{\square}(0) = u(f(v(0))) = u(n)$, i.e. $u(n) = 0$ for every n , which leads to $f^{\square}(m) = u(f(v(m)))$ for every $f \in \text{PR}$ and $m \in \mathbf{N}$. This is impossible.

Lemma 2. *Let f^{-1} be usual inverse function of f with respect to the operation \circ , i.e. $f^{-1} \circ f = f \circ f^{-1} = \text{id}$. Let $f \in \text{PR}$ and $f(0) = 0$. Assume that f^{-1} exists and $f^{-1} \in \text{PR}$. Then there exists exactly one $g \in \text{PR}$ such that $f = g^{\square}$.*

Proof. If $f = g^{\square}$, then $f(0) = 0$ and $f(n+1) = g^{\square}(n+1) = g(g^{\square}(n)) = g(f(n))$, i.e. $f \circ s = g \circ f$ and $g = f \circ s \circ f^{-1}$, i.e. there is only one possible g and this g is suitable. \square

Corollary. $\text{id} = f^{\square}$ iff $f = s$.

Theorem 1. *There are only two endomorphisms on $\langle \text{PR}, \circ, \square \rangle$, namely \mathbf{O} and \mathbf{Id} .*

Proof. There are two cases:

Case (a): $L(\text{id}) = \text{id}$ where L is the considered endomorphism on $\langle \text{PR}, \circ, \square \rangle$. Then $\text{id} = L(\text{id}) = L(s^{\square}) = L(s)^{\square}$ and so $L(s) = s$, using the corollary of Lemma 2. For every $c \in \mathbf{N}$ and each $f: \mathbf{N} \rightarrow \mathbf{N}$ let $f^0 = \text{id}$ and $f^c = \underbrace{f \circ f \circ \dots \circ f}_{c \text{ times}}$ for $c \neq 0$. Then for each constant function \bar{c} we have $\bar{c} = s^c \circ \mathbf{o}$ and

$$L(\bar{c}) = L(s^c \circ \mathbf{o}) = L(s^c \circ \text{id}^{\square}) = L(s)^c \circ L(\text{id})^{\square} = s^c \circ \mathbf{o} = \bar{c},$$

i.e. $L(\bar{c}) = \bar{c}$. Furthermore for every $f \in \text{PR}$ and $c \in \mathbf{N}$ we have

$$(f(c))^{-} = L((f(c))^{-}) = L(f \circ \bar{c}) = L(f) \circ \bar{c} = (L(f)(c))^{-},$$

i.e. $f(c) = L(f)(c)$, which implies $f = L(f)$, i.e. $L = \mathbf{Id}$.

Case (b): $L(\text{id}) \neq \text{id}$. For short we set $L(f) = f'$ for every $f \in \text{PR}$, and $N' = \bigcup \{\text{rg}(f') \mid f \in \text{PR}\}$, where $\text{rg}(f')$ denotes the range of f' . Firstly we examine whether N' equals to \mathbf{N} or not. For every $f \in \text{PR}$ we have $\text{id} \circ f = f$ and so $\text{id}' \circ f' = f'$,

i.e. $id'(f'(c)) = f'(c)$ for every $c \in \mathbf{N}$ and for each $f \in \text{PR}$. In other words: $id'|_{N'} = id|_{N'}$, and therefore $\text{rg}(id') = N'$. From this follows $N' \neq \mathbf{N}$.

Now we remark the following simple fact: $f'|_{N'} = g'|_{N'}$ implies $f' = g'$, for every function f and g . (Since for every $y \in \mathbf{N}$: $f'(y) = (f' \circ id')(y) = f'(id'(y)) = g'(id'(y)) = (g' \circ id')(y) = g'(y)$.)

Obviously $\mathbf{o}' = (id^{\square})' = (id')^{\square} = \mathbf{o}$. Furthermore for every $a \in \mathbf{N}$ we have:

$$\tilde{a}' = (s^a \circ \mathbf{o})' = s'^a \circ \mathbf{o} = (s'^{\square}(a))' = s'^{\square} \circ \tilde{a} = id' \circ \tilde{a},$$

i.e.

$$(1) \quad id' \circ \tilde{a}' = id' \circ \tilde{a}, \quad \text{for every } a \in \mathbf{N}.$$

Therefore $id'' \circ \tilde{a} = id'' \circ \tilde{a}' = (id' \circ \tilde{a})' = \tilde{a}' = \tilde{a}$ if $a \in N'$, and so $id''|_{N'} = id|_{N'} = id'|_{N'}$ and $id'' = id'$ from the previous remark. Furthermore for every $f \in \text{PR}$ and $y \in \mathbf{N}$ we have $(id' \circ f \circ id')(y) \in N'$ and $f' = id' \circ f \circ id'$ and therefore

$$\begin{aligned} ((id' \circ f \circ id')(y))' &= [((id' \circ f \circ id')(y))'] = [id' \circ f \circ id' \circ \tilde{y}] \\ &= id'' \circ f' \circ id'' \circ \tilde{y}' = id' \circ f' \circ id' \circ \tilde{y}', \end{aligned}$$

and using (1) we get

$$id' \circ f' \circ id' \circ \tilde{y} = f' \circ y = (f'(y))',$$

i.e. $id' \circ f' \circ id' = f'$. We know that $\text{rg}(id') = N' \neq \mathbf{N}$, and so $id' \circ id' \neq id$. Moreover $id'(0) = s'^{\square}(0) = 0$, i.e. $0 \in \text{rg}(id')$. If id' is a constant function then $id' = \mathbf{o}$ and $L = \mathbf{O}$. Now suppose that id' were not constant. Then we could apply Lemma 1 choosing $u = v = id'$, and by this Lemma we obtain a contradiction. \square

The following corollary shows the importance of this theorem.

Corollary. *Let $g_1, \dots, g_k \in \text{PR}$ and $\omega_1, \dots, \omega_r$ be operators on PR. Suppose that there is a finite procedure to calculate f^{\square} and $f \circ g$ from the functions $f, g \in \text{PR}$ and g_1, \dots, g_k by the help of the above operators. If $L \in \text{End}(\langle \text{PR}, \omega_1, \dots, \omega_r \rangle)$ and $L(g_i) = g_i$ for $i = 1, 2, \dots, k$, then $L \in \text{End}(\langle \text{PR}, \circ, \square \rangle)$ and so $L = Id$.*

The corollary says that the theorem is true in many usual structures of primitive recursive functions. For example:

(a) Let $\omega_1 = \circ$ and $\omega_2 = \square(m)$, where m is a fixed natural number. For every function f we have $f^{\square} = p^m \circ (s^m \circ f \circ p^m)^{\square(m)}$. So we can put $g_1 = p$ and $g_2 = s$. By our corollary, if $L \in \text{End}(\langle \text{PR}, \circ, \square(m) \rangle)$ and $L(s) = s$, $L(p) = p$ then $L = Id$.

(b) At this point let f^{-1} be defined only for surjective functions as $f^{-1}(x) = \min\{y: f(y) = x\}$ for every x . J. ROBINSON showed in [2] how to calculate f^{\square} from the functions f, s and q by the help of the operators $\circ, -1$, and $+$. (The proof can be found in [9], Theorems 3.49 and 3.50 in Part I, too.) She also showed how to calculate f^{\square} from the function f and two certain complicated functions u and v (which are independent of f) by the help of the operators \circ and -1 . So we got the following statements:

If $L \in \text{End}(\langle \text{PR}, \circ, +, -1 \rangle)$ and $L(s) = s$, $L(q) = q$, then $L = Id$.

If $L \in \text{End}(\langle \text{PR}, \circ, -1 \rangle)$ and $L(u) = u$ and $L(v) = v$, then $L = Id$.

The proof of Theorem 1 shows that we used a few properties of our structure $\langle \text{PR}, \circ, \square \rangle$ only. This implies the following generalizations:

Theorem 1A. Let $\langle P, \circ, \square \rangle$ be an arbitrary algebraic structure on which the following axioms hold:

(a) $\langle P, \circ \rangle$ is a semigroup with unit element id .

(b) There exists exactly one s in P such that $s^\square = id$. We denote by PS the set of the left-hand singular elements of $\langle P, \circ \rangle$, i.e. for every $c \in PS$ and $f \in P$ let $c \circ f = c$.

(c) $(\forall f, g \in P) ((\forall c \in PS) f \circ c = g \circ c) \Rightarrow f = g$.

(d) $(\exists c_0 \in PS) (\forall f \in P) f^{\square\square} = c_0$.

(e) $(\forall c \in PS) (\exists k_c \in \mathbf{N}) c = \underbrace{s \circ s \circ \dots \circ s}_{k_c \text{ times}} \circ c_0$.

If $L \in \text{End}(\langle P, \circ, \square \rangle)$ and $L(id) = id$ then $L = Id$.

Theorem 1B. Let $\langle P, \circ, \square \rangle$ be an arbitrary algebraic structure. Suppose that all the above axioms (a)–(e) and the following axiom hold:

(f) $(\forall x_1, x_2, y, z \in PS) (\exists f \in P) (f \circ z = x_1 \ \& \ f \circ y = x_2)$.

Then there are only two endomorphisms on $\langle P, \circ, \square \rangle$, namely Id and O .

§ 2. In this section we examine the generations of PR. Except from Theorem 3, we consider arbitrary functions $f: \mathbf{N} \rightarrow \mathbf{N}$.

Lemma 3. Let f be an arbitrary function. If f^\square is not injective, then $\text{rg}(f^\square)$ is a finite set.

Proof. By the definition of f^\square from $f^\square(n) = f^\square(m)$ for any $m > n$ it follows that $\text{rg}(f^\square) = \{f^\square(0), \dots, f^\square(m-1)\}$. \square

Note that in the case above f^\square is a periodic function and its period is $m-n$. L. Lovász asked whether for every periodic function f there is a function g such that $f = g^\square$. The answer is the following: Let the sequence $f(i)$ be periodic with the period $m-n$, then there exists such a g iff $f(0) = 0$ and the numbers $f(0), f(1), \dots, f(m-1)$ are all distinct.

Lemma 4. If f is not injective, then f^\square is not surjective.

Proof. Let $i = f(k_1) = f(k_2)$, where $k_1 \neq k_2$. If f^\square is surjective, then there exist natural numbers h_1, h_2 such that $k_1 = f^\square(h_1)$ and $k_2 = f^\square(h_2)$. Then $i = f(k_1) = f(f^\square(h_1)) = f^\square(h_1 + 1)$ and in similar way we get $i = f^\square(h_2 + 1)$. We know that $h_1 + 1 \neq h_2 + 1$ and because of Lemma 3, f^\square is not surjective. This contradiction proves the lemma. \square

From this point on for an arbitrary function a we denote by $\langle a \rangle$ the closure of $\{a\}$ with respect to the operators \circ and \square .

Lemma 5. If a is an arbitrary injective function, then for every member f of $\langle a \rangle$ either f is injective or $\text{rg}(f)$ is finite.

Proof. The order of an element f in $\langle a \rangle$ is defined as the minimal number of operations \circ and \square which are necessary to generate f from a . Now the lemma is proved by induction on the order of f . As the assertion is true for a , the lemma holds for order 0. Assume the assertion is true for order $k \leq n$, and let $\text{ord}(f) = n + 1$.

Case 1: $f = g^\square$ and $\text{ord}(g) = n$. If $\text{rg}(g)$ is finite, then $\text{rg}(g^\square)$ is also finite. If g is injective and g^\square is not injective, then by Lemma 3 $\text{rg}(g^\square)$ is finite.

Case 2: $f = g \circ h$ and $\text{ord}(g), \text{ord}(h) \leq n$. If g and h are injective, then $g \circ h$ is injective. If $\text{rg}(g)$ or $\text{rg}(h)$ is finite, then $\text{rg}(g \circ h)$ is finite. \square

Lemma 6. *For every element f of $\langle a \rangle$ either there exists a suitable natural number k such that $f = a^k$ or $(\text{rg}(f) \subseteq \text{rg}(a^\square))$.*

Proof. For every natural number m and each function f we have $f^m \circ f^\square = f^\square \circ s^m$ and $(f^m)^\square = f^\square \circ (s^m)^\square$. Taking these identities into account we get the following scheme for the construction of $\langle a \rangle$ on the strength of the definition of the order of the elements in $\langle a \rangle$:

$$a, a^2, a^\square, a^3, (a^2)^\square = a^\square \circ (s^2)^\square, a^{\square\square} = o,$$

$$a^4, (a^3)^\square = a^\square \circ (s^3)^\square, a^\square \circ a^\square, \dots$$

...

$$a^m, (a^m)^\square = a^\square \circ (s^m)^\square, (a^\square)^m = a^\square \circ (a^\square)^{m-1}, a^m \circ a^\square = a^\square \circ s^m, a^\square \circ a^m.$$

A short look of this scheme yields the proof. \square

Theorem 2. *Let a be an arbitrary function from \mathbb{N} to \mathbb{N} . Then either there exists no bijection in $\langle a \rangle$ or for every member f of $\langle a \rangle$ it holds that f is injective or $\text{rg}(f)$ is finite.*

Proof. If a is injective, the assertion follows by Lemma 5. If a is not injective, then a^m is not injective, too. In this case we prove that there is no bijective function in $\langle a \rangle$. Assume on the contrary that there exists a bijective member f in $\langle a \rangle$. Then $f \neq a^m$ because f is injective. But f is surjective and by Lemma 6 then a^\square must be a surjective function. By Lemma 4 this is a contradiction which proves the theorem. \square

Theorem 3. *There is no primitive recursive function which generates all monoton increasing primitive recursive functions. In particular, there is no primitive recursive function a such that $\langle a \rangle = \text{PR}$.*

Proof. Because of Theorem 2 id and p can not be at the same time in $\langle a \rangle$. \square

We now give a more general algebraic form of Theorem 2 similar to Theorem 1 A. Let (g) be the following axiom:

(g) $PS = \{c_0, c_1, \dots\}$ (i.e. PS is countable) and, for every $f \in P$ and each natural number i , $f^\square \circ c_0 = c_0$ and $f^\square \circ c_{i+1} = f^\square \circ f \circ c_i$ hold.

Really it is a very strong axiom: From (c) and (g) one can easily prove the axioms (d), (e) and half of (b). If we identify the elements f of P with functions f mapping from PS to PS with $f(c) = f \circ c$, then we can easily prove Lemma 3 – Lemma 6 and so we get

Theorem 2 A. *Let $\langle P, \circ, \square \rangle$ an arbitrary algebraic structure on which axiom (g) holds. Then for every element a of P either there exists no bijection in $\langle a \rangle$ or for every $f \in \langle a \rangle$ it holds that f is injective or $\text{rg}(f)$ is finite.*

Note that we can show by the help of Theorem 2 that several subspaces of $\langle \mathbb{N}^{\mathbb{N}}, \circ, \square \rangle$ can not be generated from only one function, e.g. $\{f: f(0) = 0 \text{ and } f \text{ is strictly monoton}\} \cup \{o\}$, etc. Till now I have not found a monotone increasing primitive recursive function which is not in $\langle s \rangle$. This is not an important question but I am interested in it. The results of this paper seem to be the first ones concerning the algebraic properties of $\langle \text{PR}, \circ, \square \rangle$. I think it is interesting and useful to investigate

similar problems, for example to study other properties of the operators \circ and \square , to investigate other operators on PR (e.g. $\Sigma(f)(n) = f(0) + \dots + f(n)$ or f^{-1}) or to raise usual or unusual algebraic questions about $\langle \text{PR}, \circ, \square \rangle$.

References

- [1] GLADSTONE, M. D., A reduction of the recursion scheme. *J. Symb. Logic* **32** (1967), 505–508.
- [2] GLADSTONE, M. D., Simplification of the recursion scheme. *J. Symb. Logic* **36** (1971), 653–665.
- [3] MAZUR, S., and R. M. ROBINSON, Problem 143. In: *The Scottish Problem Book* (R. MAULDIN, ed.), Birkhäuser-Verlag, Basel 1981.
- [4] MONK, J. D., *Mathematical Logic*. Springer-Verlag, Berlin–Heidelberg–New York 1976.
- [5] PÉTER, R., *Recursive Functions*. Akadémia, Budapest 1967.
- [6] ROBINSON, J., General recursive functions. *Proc. Amer. Math. Soc.* **1** (1950), 703–718.
- [7] ROBINSON, J., A note on primitive recursive functions. *Proc. Amer. Math. Soc.* **6** (1955), 667–670.
- [8] ROBINSON, J., Recursive functions of one variable. *Proc. Amer. Math. Soc.* **19** (1968), 815–820.
- [9] ROBINSON, R. M., Primitive recursive functions. *Bull. Amer. Math. Soc.* **53** (1947), 925–942.
- [10] ROBINSON, R. M., Primitive recursive functions II. *Proc. Amer. Math. Soc.* **6** (1955), 663–666.

István Szalkai
Hungary

(Eingegangen am 16. November 1983;
überarbeitete Fassung vom 4. April 1984)