Reprint from
aequationes mathematicae
Vol. 8, fasc. 3, 1972 BIRKHÄUSER VERLAG BASEL pages 238–241

On Functions Defined by Iterations of Each Other[1])

J. D. BECKER and E. T. ORDMAN (Cambridge, Massachusetts, U.S.A. and Lexington, Kentucky, U.S.A.)

1. Introduction

Let f and g be functions from and into the nonnegative integers, and let iteration of a function be denoted by superscripting (so that $f^2(n)=ff(n)=f(f(n))$). We shall prove

THEOREM. *The pairs* (f, g) *of functions satisfying*

$$f^{m+1}(n)=g^{n+1}(m), \quad 0 \leqq m, n < \infty \tag{1}$$

are precisely those given by

$$f(n)=g(n)=\begin{cases} n+1 & \text{for} \quad n<k \\ a & \text{for} \quad n=k \\ a_i & \text{for} \quad n>k,\ n \equiv i \pmod{p} \end{cases} \tag{2}$$

where $-1 \leqq k \leqq \infty$ *and (if* $k<\infty$*)* p, a, a_i *are integers satisfying* $1 \leqq p < \infty$, $1 \leqq i \leqq p$, $a, a_i > k$, $a \equiv k+1 \pmod{p}$ *and* $a_i \equiv i+1 \pmod{p}$.

From this it follows that

COROLLARY. *The function f satisfies*

$$f(n)=f^{n+1}(0), \quad n \geqslant 0 \tag{3}$$

if and only if f satisfies (2).

Proof of Corollary. If f is as in (2), the pair (f, f) satisfies (1) by the theorem and (3) is the special case $m=0$. Conversely, if f satisfies (3), we can define $g=f$ to give $f^{m+1}(n)=f^m f(n)=f^m f^{n+1}(0)=g^n g^{m+1}(0)=g^n g(m)=g^{n+1}(m)$. Then, since (f, g) satisfies (1), f must be as in (2).

The problem and many of the proofs may be pictured in terms of an array $\{a_{m,n}\}$ of integers with $a_{m,n}=f^{m+1}(n)=g^{n+1}(m)$. The crucial fact in this interpretation is that a number such as $f^3(0)=f^2 f(0)=ff^2(0)$ appears in each of the positions $a_{2,0}$, $a_{1,f(0)}$, and $a_{0,f^2(0)}$.

In figures 1, 2, and 3, $f(n)$ is directly to the right of, and $g(n)$ directly above, each occurrence of n.

[1]) This work was done at the National Bureau of Standards, Washington, D.C.

Received March 29, 1971

	0	1	2	3	4	5	6...
6							
5							
4	5						
3	4	5					
2	3	4	5				
1	2	3	4	5			
0	1	2	3	4	5	6	7...

$k=\infty$, p undefined

Figure 1

	0	1	2	3	4	5	6	7...
6	7							
5	6	7						
4	5	6	7					
3	0	5	6	7				
2	7	0	5	6	7			
1	6	7	0	5	6	7		
0	5	6	7	0	5	6	7	0...

$k=-1, p=4$

Figure 2

	0	1	2	3	4	5	6	7...
6	5							
5	4	5						
4	5	4	5					
3	8	5	4	5				
2	3	8	5	4	5			
1	2	3	8	5	4	5		
0	1	2	3	8	5	4	5	4...

$k=3, p=2$

Figure 3

2. Proof that (2) implies (1)

Let $a_{m,n}$ be given by

$$a_{m,n}=\begin{cases} m+n+1 & \text{for} \quad m+n<k \\ a & \text{for} \quad m+n=k \\ a_i & \text{for} \quad m+n>k,\ m+n\equiv i \pmod p \end{cases} \tag{4}$$

where the parameters are defined since f and g satisfy (2). We shall show that $f^{m+1}(n)=a_{m,n}$; $g=f$ by hypothesis and clearly $a_{m,n}=a_{n,m}$, so it will follow that $f^{m+1}(n)=a_{n,m}=f^{n+1}(m)=g^{n+1}(m)$ completing the proof.

Formulae (2) and (4) make clear that $a_{0,n}=f(n)$; we shall prove $a_{m,n}=f^{m+1}(n)$ by induction on m, by showing that for all $m, n, f(a_{m,n})=a_{m+1,n}$. There are four cases, for $m+n$ respectively less than $k-1$, equal to $k-1$, equal to k, and greater than k. All are elementary; we illustrate with $m+n=k$. In this case $a_{m,n}=a$, so $f(a_{m,n})=f(a)$ $=a_i$ where $i\equiv a\equiv k+1 \pmod p$. However, $a_{m+1,n}=a_i$ where $i\equiv(m+1)+n=k+1 \pmod p$, so $f(a_{m,n})=a_{m+1,n}$.

3. Proof that (1) implies (2)

LEMMA 1. $g^m f^r(n)=f^r(m+n)$

Proof. Using (1) twice, $g^m f^r(n)=g^m g^{n+1}(r-1)=g^{m+n+1}(r-1)=f^r(m+n)$.

LEMMA 2. *There are integers k, $-1\leqq k\leqq\infty$, and (if $k<\infty$) p, $1\leqq p<\infty$, such that the values $f(0),\ldots,f(k)$ are assumed by f only at the points $0,\ldots,k$ respectively, and such that for all $r>0, f(k+r)=f(k+r+p)$, while the values $f(k+1),\ldots,f(k+p)$ are distinct.*

Proof. If f is one-one, then $k=\infty$. If not, let k be the least integer such that $f(k+1)$ is the image of more than one point, and let $p>0$ be the least integer for which $f(k+1+p)=f(k+1)$. Then, using Lemma 1 twice, $f(k+r)=g^{r-1}f(k+1)=g^{r-1}f(k+1+p)=f(k+r+p)$ for all $r>0$. To show that $f(k+1),\ldots,f(k+p)$ are distinct, suppose that $k+1\leqq m<n\leqq k+p$ and $f(m)=f(n)$. Again, using Lemma 1 twice,

$f(k+1)=f(k+1+p)=g^{k+1+p-n}f(n)=g^{k+1+p-n}f(m)=f(k+1+(p+m-n))$; but, since $p+m-n<p$, this contradicts the choice of p as the least period.

That is, f is one-one on the segment $\{0,\dots,k\}$ and periodic with period p thereafter; the cases where the segment is null or infinite correspond to $k=-1$ and $k=\infty$ respectively. To establish (2) it now suffices to show that $f(n)=n+1$ for $n<k$; that $f(n)\equiv n+1 \pmod{p}$ and $f(n)>k$ for $n\geqslant k$; and that $g(n)=f(n)$ for all n.

LEMMA 3. *If $f(m)=f(n)$, then $m\equiv n \pmod{p}$. If in addition $m\leqq k$ or $n\leqq k$, then $m=n$.*

Proof. If m and n are each greater than k, they must differ by a multiple of the period since the values in the period are distinct. If $m\leqq k$, $f(m)$ is a value assumed only at the point m, so $n=m$.

LEMMA 4. *$f^{n+1}(0)=f(nf(0))$.*

Proof. This is clearly true for $n=0$; suppose it is true for some m. Then by Lemma 1,

$$f^{(m+1)+1}(0)=f^{m+1}(f(0))=g^{f(0)}f^{m+1}(0)$$
$$=g^{f(0)}f(mf(0))=f(mf(0)+f(0))=f((m+1)f(0)),$$

completing the induction.

PROPOSITION 1. *If $k\neq\infty$ then $f(n)\equiv n+1 \pmod{p}$.*

Proof. By Lemma 1, formula (1), and Lemma 4, $f(n+1)=gf(n)=f^{f(n)+1}(0)=f(f(n)\cdot f(0))$; by Lemma 3,

$$n+1\equiv f(n)\cdot f(0) \pmod{p}. \tag{5}$$

Lemma 1 also yields $ff(n)=g^n ff(0)=f(f(0)+n)$, so by Lemma 3,

$$f(n)\equiv f(0)+n \pmod{p}. \tag{6}$$

Combining these, $f(n)-f(0)+1\equiv n+1\equiv f(n)\cdot f(0) \pmod{p}$; rearranging, $f(n)+1\equiv \equiv f(0)\cdot(f(n)+1) \pmod{p}$. By (6), there is an n such that $f(n)+1$ is relatively prime to p; thus we may divide by $f(n)+1$ to get $f(0)\equiv 1 \pmod{p}$ and $f(n)\equiv n+1 \pmod{p}$ for all n.

PROPOSITION 2. *If $n<k$, then $f(n)=n+1$.*

Proof. Where $n<k$ (including the case $k=\infty$) the proof of Proposition 1 holds with congruences replaced by equality. (5) holds since $n<k$ implies $n+1\leqq k$; then (5) implies $f(n)\leqslant k$ so (6) holds, by Lemma 3. In this case (5) implies $f(0)=1$ immediately, since $f(0)$ is nonnegative by hypothesis.

PROPOSITION 3. *$f(n)>k$ for $n\geqslant k$.*

Proof. If $k\geqslant 0$, f never assumes the value 0. If it did, $f(r)=0$ would imply $f(r+1)=gf(r)=g(0)=f(0)$ would be the image of more than one point, and k would equal -1. If $k>0$, f assumes the values $1, 2, \ldots, k$ at $0, 1, \ldots, k-1$ and only there. Thus at all other points, $f(n)>k$.

PROPOSITION 4. *$g(n)=f(n)$ for all n.*

Proof. Since (f, g) satisfies (1), $g(n)=f^{n+1}(0)$. But we have shown that f satisfies (2), so (f, f) satisfies (1) and thus $f^{n+1}(0)=f(n)$. Thus $g(n)=f(n)$ and the proof that (1) implies (2) is complete.

Stanford University and
University of Kentucky