FUNDAMENTA
MATHEMATICAE
163 (2000)

A deceptive fact about functions

by

Wiesław Dziobiak (Mayagüez, PR),
Andrzej Ehrenfeucht (Boulder, CO),
Jacqueline B. Grace (New Paltz, NY) and
Donald Silberger (New Paltz, NY)

Abstract. The paper provides a proof of a combinatorial result which pertains to the characterization of the set of equations which are solvable in the composition monoid of all partial functions on an infinite set.

1. Introduction. The immediate objective of this paper is to prove the following

THEOREM 1. *Let m be a positive integer. Let there exist a* (*partial*) *function $f \subseteq X \times X$ such that $f^m\restriction Y$ is a bijection from Y onto X where $Y \subseteq X$ and $X \setminus Y$ is finite. Then m is a factor of the integer $|X \setminus Y|$.*

We have stated this theorem to several mathematicians, all of whom declared it to be trivial. Some of them gave us proofs. But all of those proofs revealed flaws. Two of us had similar experiences two decades ago with the theorem. In fact, one of us subsequently published a proof that was at least incomplete if not indeed downright wrong; see [2, Theorem 1]. What seems to happen to a reader confronting Theorem 1 is that its hypotheses may beguile into one or more false assumptions. At first sight, for instance, one might be tempted to surmise that the hypotheses of Theorem 1 necessitate that the set inclusion $Y \subseteq f[Y]$ holds. In fact, if it were indeed always the case that $Y \subseteq f[Y]$ then the proof of Theorem 1 would be short and straightforward. But, curiously, this inclusion may fail, as the following example shows.

Let $X = \omega$, $Y = X \setminus \{1, 3, 8, 10\}$, and let $f \subset X \times X$ be defined by $f(x) = x - 4$ for x even and $x \geq 4$, $f(x) = x$ for x odd and $x \geq 5$, $f(x) = x + 1$ for $x = 0, 1, 2$, and $f(3) = 0$. Then, for $m = 2$, $f^m\restriction Y$ is a bijection from Y onto X and $Y \not\subseteq f[Y]$.

2000 *Mathematics Subject Classification*: Primary 03E20, 03E05; Secondary 05C20, 08A50.

Our work lies in the area of universal terms; see [1] and [2]. A word w is said to be *universal in a monoid* G iff for each $g \in G$ there is a homomorphism $h(w,g) : w^* \to G$ such that $h(w,g)(w) = g$, where w^* is the free monoid of the letters occurring in w. Theorem 1 is a tool for the study of equations in the composition monoids G which are submonoids of the monoid $P(X \times X) := \{b : b \subseteq X \times X\}$ of all binary relations on X. These G include $G = \mathrm{Prt}(X) := \{p : p \text{ is a function}\} \cap P(X \times X)$, the monoid of partial transformations on X. They include the submonoid $G = {}^X X$ of $\mathrm{Prt}(X)$, where $X := \{t : t \in \mathrm{Prt}(X) \text{ and } X = \mathrm{Dom}(t)\}$. And they include the groups of permutations of the set X.

By [2] our Corollary 4 implies that, if $w := x^p y^m x^q$ is a word such that for each X and each $f \in \mathrm{Prt}(X)$ there exists a homomorphism h satisfying the equation $f = h(w)$, then $|p| = |q| = 1$. Hence w is universal in $\mathrm{Prt}(X)$, for X infinite, if and only if $|p| = |q| = 1$.

The present paper applies to $\mathrm{Prt}(X)$. A sequel will append to the list of conditions which Corollary 4 declares to be equivalent, another which extends to $P(X \times X)$ the study of equations in composition monoids.

The set of all nonnegative integers is written ω. When $k \in \omega$ then $k := \{0, 1, \ldots, k-1\}$. When S is a set and f is a function, $f{\restriction}S$ is the restriction $\{\langle s, f(s)\rangle : s \in S\}$ of f to S, and $f[S]$ denotes $\{f(s) : s \in S\}$. When $f \subseteq X \times X$ then $\$(f) := \mathrm{Dom}(f) \cup \mathrm{Rng}(f)$. The expression $\mathrm{id}{\restriction}X$ denotes the identity permutation on X. The expression h^0 denotes $\mathrm{id}{\restriction}X$ when $h \in \mathrm{Prt}(X)$. Henceforth m denotes an arbitrary positive integer. The word "function" may mean "partial function" in this paper. For convenience we write C to denote the finite set $X \setminus Y$. There is another purpose in our doing so: The idea is that the finite set C is fixed, but the sets Y and X vary according to circumstances.

2. Proof of the Theorem. Theorem 1 is immediate from Lemmas 2 and 3 below. Both make claims about an entity we call a "liable quadruple". Accordingly we now introduce this notion.

For a set X, a (partial) function $h \subseteq X \times X$, $\langle x, y\rangle \in X \times X$, and $\emptyset \neq S \subseteq X$ we define

$$\begin{aligned}
\mathrm{hgt}(h,x,y) &:= \min(\{\infty\} \cup \{j : j \in \omega \text{ and } h^j(x) = y\}),\\
\mathrm{Hgt}(h,x,S) &:= \min\{\mathrm{hgt}(h,x,s) : s \in S\},\\
\Lambda(X,S,m,h) &:= \{x : \exists i \in m+1\,(h^i(x) \in h^m[S])\}.
\end{aligned}$$

The quadruple $\langle X, S, m, h\rangle$ is said to be *liable* if and only if the following three criteria are satisfied:

L1. $\Lambda(X,S,m,h) \subseteq h^m[X \setminus S]$.
L2. $h^m{\restriction}(X \setminus S)$ is injective.
L3. $S \subseteq \mathrm{Dom}(h^m)$.

Lemma 2. *Let Y be infinite with $Y \cap C = \emptyset$, and let $X := Y \cup C$. Let there be a function $h \subseteq X \times X$ such that $h^m \restriction Y$ is a bijection from Y onto X. Then there is a function f such that $\langle X, C, m, f\rangle$ is a liable quadruple.*

Proof. Note that $X \setminus \mathrm{Dom}(h) \subseteq C$, since $Y \subseteq \mathrm{Dom}(h^m) \subseteq \mathrm{Dom}(h) \subseteq X$. Define $f := h \cup \mathrm{id}\restriction(X \setminus \mathrm{Dom}(h))$. Since $\Lambda(X, C, m, f) \subseteq X = h^m[Y] = f^m[Y]$, the quadruple $\langle X, C, m, f\rangle$ satisfies the condition L1. Since $f^m\restriction Y = h^m\restriction Y$, it also satisfies L2. Finally, since $X = \mathrm{Dom}(f)$, it satisfies L3. Therefore $\langle X, C, m, f\rangle$ is liable. ∎

Lemma 3. *Let $\langle X, C, m, f\rangle$ be a liable quadruple for some X and f. Then m is a factor of the integer $|C|$.*

Proof. Arguing by induction on $|C|$ we suppose that for each pair of sets Z and $D \subseteq Z$ with $|D| < |C|$, if there exists $g \in \mathrm{Prt}(Z)$ for which $\langle Z, D, m, g\rangle$ is liable then m is a factor of $|D|$.

Now suppose that $\langle X, C, m, f\rangle$ is liable. By L3 there exists a maximal connected subdigraph f_0 of f such that $C \cap \$(f_0) \neq \emptyset$. Let $X_0 := \$(f_0)$, $C_0 := C \cap X_0$, $X_1 := X \setminus X$, $C_1 := C \cap X_1$, and $f_1 := f \setminus f_0$. Notice that both quadruples $\langle X_i, C_i, m, f_i\rangle$ for $i \in 2$ are liable, and $|C_0| + |C_1| = |C|$. If $C_1 \neq \emptyset$ then both C_0 and C_1 are finite, nonempty, and with fewer than $|C|$ elements. So by the inductive hypothesis, m is a factor of $|C_0|$ and of $|C_1|$ and consequently of $|C|$. So henceforth we may and do suppose that f as a digraph is connected, and furthermore that $X = \$(f)$.

For the remainder of the proof we select a subset M of $\$(f)$ satisfying the following three conditions:

P1. $f\restriction M$ is injective.
P2. If $x \in M \cap \mathrm{Dom}(f)$ then $f(x) \in M$.
P3. If $x \in M \cap \mathrm{Rng}(f)$ then $x = f(y)$ for some $y \in M$.

Such a set M does exist. Indeed, if f has a subset g which is a directed cycle then $M := \$(g)$ satisfies P1–P3. On the other hand, if f has no such subset g then with the aid of Zorn's Lemma we can choose a maximal $h \subseteq f$ such that h is injective and connected; in this event we let $M := \$(h)$, and note that P1–P3 are satisfied.

By hypothesis the quadruple $\langle X, C, m, f\rangle$ is liable, and so $\Lambda(X, C, m, f) \subseteq f^m[X \setminus C]$, $f^m\restriction(X \setminus C)$ is injective and $C \subseteq \mathrm{Dom}(f^m)$. Now obviously $f^m[M \cap C] \subseteq f^m[C] \subseteq \Lambda(X, C, m, f)$. Therefore $f^m[M \cap C] \subseteq f^m[X \setminus C]$. Hence, by L2, for every $x \in M \cap C$ there is a unique element $\eta(x) \in X \setminus C$ such that $f^m(\eta(x)) = f^m(x)$. This defines a function $\eta : M \cap C \to X \setminus C$. Since $f^m\restriction M$ is injective by P1 and P2, η is also injective. Define

$$C_1 := (C \setminus M) \cup \eta[M \cap C].$$

We establish the following claim:

A1. $|C_1| = |C|$ *and the quadruple* $\langle X, C_1, m, f\rangle$ *is liable.*

That $|C_1| = |C|$ is evident by the injectivity of η. Clearly $f^m[\eta[M\cap C]] = f^m[M \cap C]$. So

$$f^m[C_1] = f^m[C \setminus M] \cup f^m[\eta[M \cap C]] = f^m[C \setminus M] \cup f^m[M \cap C] = f^m[C].$$

Consequently, $\Lambda(X, C_1, m, f) = \Lambda(X, C, m, f)$. Note that $X \setminus C_1 = (M \cap C) \cup ((X \setminus C) \setminus \eta[M \cap C])$. Then

$$\begin{aligned} f^m[X \setminus C_1] &= f^m[M \cap C] \cup f^m[(X \setminus C) \setminus \eta[M \cap C]] \\ &= f^m[\eta[M \cap C] \cup ((X \setminus C) \setminus \eta[M \cap C])] = f^m[X \setminus C]. \end{aligned}$$

Summarizing, we have $\Lambda(X, C_1, m, f) = \Lambda(X, C, m, f) \subseteq f^m[X \setminus C] = f^m[X \setminus C_1]$. That is, the quadruple $\langle X, C_1, m, f\rangle$ satisfies the condition L1.

Next we show that $f^m{\restriction}(X \setminus C_1)$ is injective. To this end, note that $f^m{\restriction}(M \cap C)$ is injective by P1 and P2. Moreover, $f^m{\restriction}((X \setminus C) \setminus \eta[M \cap C])$ is injective. Of course $(M \cap C) \cap ((X \setminus C) \setminus \eta[M \cap C]) = \emptyset$. And now recall that $X \setminus C_1 = (M \cap C) \cup ((X \setminus C) \setminus \eta[M \cap C])$. So $f^m{\restriction}(X \setminus C_1)$ is injective if $f^m(x) \neq f^m(x')$ for every pair $\langle x, x'\rangle \in (M \cap C) \times ((X \setminus C) \setminus \eta[M \cap C])$. Clearly $x' \neq \eta(x)$. But $\{x', \eta(x)\} \subseteq X \setminus C$. Moreover, $f^m{\restriction}(X \setminus C)$ is injective since $\langle X, C, m, f\rangle$ is liable. It follows that $f^m(x') \neq f^m(\eta(x))$. Hence the quadruple $\langle X, C_1, m, f\rangle$ satisfies L2.

The liability of $\langle X, C, m, f\rangle$ gives $C \subseteq \mathrm{Dom}(f^m)$. Moreover, $\eta[M \cap C] \subseteq \mathrm{Dom}(f^m)$. So $C_1 = (C \setminus M) \cup \eta[M \cap C] \subseteq \mathrm{Dom}(f^m)$. Hence $\langle X, C_1, m, f\rangle$ satisfies L3. So $\langle X, C_1, m, f\rangle$ is liable, and A1 is proved.

We will need some terminology: For $f \in \mathrm{Prt}(X)$ and $x \in X$, let

$$\begin{aligned} &f^-(x) := \{y : \exists i \in \omega(f^i(y) = x)\}, \qquad f^+(x) := \{f^i(x) : i \in \omega\}, \\ &I(x, f) := \{y : f(y) = x\}. \end{aligned}$$

For B a set, let $f^-(B) := \bigcup\{f^-(b) : b \in B\}$ and let $f^+(B) := \bigcup\{f^+(b) : b \in B\}$.

Let $h := \max\{\mathrm{Hgt}(f, t, M) : t \in C_1\}$. By A1 we know that C_1 is a finite subset of X. Since the digraph f is connected, we have $\$(f) = f^-(M)$. Therefore h is a nonnegative integer. Choose $d \in C_1$ for which $h = \mathrm{Hgt}(f, d, M)$. From A1 and L1 we have $C_1 \subseteq \Lambda(X, C_1, f, m) \subseteq f^m[X \setminus C_1]$. Hence there exists $x \in X \setminus C_1$ such that $f^m(x) = d$. By our choice of d we have $f^{m-1}(x) \in X \setminus C_1$. Next we establish the following claim.

A2. *If* $h < m$ *then for every integer* $k \geq 1$ *the following two assertions hold*:

(i) $k \leq h$.

(ii) *There is a subdigraph* $y_{h-k} \mapsto y_{h-k+1} \mapsto \ldots \mapsto y_{h-1} \mapsto y_h \mapsto f^h(d)$ *of* f *with* $\{y_{h-k}, y_{h-k+1}, \ldots, y_{h-1}, y_h\} \subseteq M$.

Suppose that $h < m$. We need $M \cap C_1 = \emptyset$. It suffices to prove that $M \cap \eta[M \cap C] = \emptyset$. So, assume that $\eta(v) \in M \cap \eta[M \cap C]$ for some $v \in M \cap C$. By the definition of η then $f^m(\eta(v)) = f^m(v)$. But $f^m \restriction M$ is injective, by P1 and P2, and hence $\eta(v) = v$. Recalling that $\mathrm{Rng}(\eta) \subseteq X \setminus C$ we then get $v = \eta(v) \in X \setminus C$; this contradicts $v \in M \cap C$. So $M \cap C_1 = \emptyset$. This, by the definitions of h and d, gives $h \geq 1$ and $d \notin M \cap C_1$.

Now we argue by induction on k.

Let $k := 1$. Then $h \geq 1$ implies that $k \leq h$. So to show A2 we only need to prove the existence of y_{h-1} and y_h in M such that $y_{h-1} \mapsto y_h \mapsto f^h(d)$ is a subdigraph of f. Obviously $f^h(d) \in M \cap \mathrm{Rng}(f)$. Therefore, by P3 we know that M contains an element y_h with $f(y_h) = f^h(d)$. So, since $1 \leq h < m$, we have $0 < m-h$ and $2 \leq m-h+1 \leq m$. Thus $f^{m-h+1}(y_h) = f^{m-h}(f(y_h)) = f^{m-h}(f^h(d)) = f^m(d) \in f^m[C_1]$, whence $y_h \in \Lambda(X, C_1, m, f)$. So, by A1 we have $y_h \in f^m[X \setminus C_1]$. Furthermore, since $y_h \in M \cap \mathrm{Rng}(f)$, P3 shows that there exists $y_{h-1} \in M$ with $f(y_{h-1}) = y_h$. It follows that f has a subdigraph $y_{h-1} \mapsto y_h \mapsto f^h(d)$ with $\{y_{h-1}, y_h\} \subseteq M$.

Now let k be arbitrary, and suppose that the assertions of A2 hold for this k. Then $k \leq h$, and $y_{h-k} \mapsto y_{h-k+1} \mapsto \ldots \mapsto y_{h-1} \mapsto y_h \mapsto f^h(d)$ is a subdigraph of f for some $\{y_{h-k}, y_{h-k+1}, \ldots, y_{h-1}, y_h\} \subseteq M$.

First we show as required that $k + 1 \leq h$. Assume that $k + 1 > h$. Then the inductive hypothesis $k \leq h$ implies that $k = h$. Observe that $f^{h+1}(f^{m-1}(x)) = f^h(f^m(x)) = f^h(d)$. Then $y_0 = y_{h-k} \in M$ and $f^{h+1}(y_{h-k}) = f^{h+1}(y_0) = f^h(d)$ because $k = h$. Thus $f^{h+1}(f^{m-1}(x)) = f^{h+1}(y_{h-k})$. Since $f^m \restriction (X \setminus C_1)$ is injective, $f^i \restriction (X \setminus C_1)$ is injective for all nonnegative integers $i \leq m$. Now recall that $y_{h-k} \in M \subseteq X \setminus C_1$, $f^{m-1}(x) \in X \setminus C_1$, and $h + 1 \leq m$. It follows that $f^{m-1}(x) = y_{h-k}$. Hence $d = f(f^{m-1}(x)) = f(y_{h-k}) = y_{h-k+1}$. Since $y_{h-k+1} \in M$ by the inductive hypothesis, we reach the impossibility $d \in M \cap C = \emptyset$. So $k + 1 \leq h$ as we wish.

In order to conclude the inductive step it now suffices to show that there exists $y_{h-k-1} \in M$ with $f(y_{h-k-1}) = y_{h-k}$. Since by hypothesis $h < m$, we have $m - h + k + 1 > m - h > 0$. Hence $f^{m-h+k+1}(y_{h-k}) = f^{m-h}(f^{k+1}(y_{h-k})) = f^{m-h}(f^h(d)) = f^m(d) \in f^m[C_1]$. Since $k + 1 \leq h$, we have $m - h + k + 1 \leq m$, and hence $y_{h-k} \in \Lambda(X, C_1, m, f)$. But $\Lambda(X, C_1, m, f) \subseteq f^m[X \setminus C_1]$ by A1. So $y_{h-k} \in f^m[X \setminus C_1]$. In particular $y_{h-k} \in \mathrm{Rng}(f)$. So, since $y_{h-k} \in M$, by P3 we have $y_{h-k} = f(u)$ for some $u \in M$. Let $y_{h-k-1} := u$. This completes the proof of A2.

Since h is finite, from A2 we infer that $m \leq h$.

Next we prove

A3. *If* $0 \leq i \leq m - 2$ *then* $I(f^{i+1}(d), f) = \{f^i(d)\}$.

Choose any y for which $f(y) = f^{i+1}(d)$. Since $f^{m-i}(y) = f^{m-(i+1)}(f(y)) = f^{m-(i+1)}(f^{i+1}(d)) = f^m(d) \in f^m[C_1]$, and since $\langle X, C_1, m, f\rangle$ is liable by

A1, we have $y \in f^m[X \setminus C_1]$. It follows that $y = f^m(x')$ for some $x' \in X \setminus C_1$. Since $i \leq m-2 \leq h-2$, we get

$$\begin{aligned} f^{h+(m-1)-i}(f(x')) &= f^{h-i}(f^m(x')) = f^{h-i}(y) = f^{h-m}(f^{m-i}(y)) \\ &= f^{h-m}(f^m(d)) = f^h(d). \end{aligned}$$

So $\mathrm{hgt}(f, f(x'), f^h(d)) \leq h + (m-1) - i$. Now assume that there is a nonnegative integer $q < h + (m-1) - i$ with $f^q(f(x')) = f^h(d)$. Recalling that $f^h(d) \in M$, by P2 we have $f^j(f(x')) \in M$ for all $j \geq q$. In particular $f^{h+(m-2)-i}(f(x')) \in M$. But

$$\begin{aligned} f^{h+(m-2)-i}(f(x')) &= f^{h-i-1}(f^{m-1}(f(x'))) = f^{h-i-1}(f^m(x')) = f^{h-i-1}(y) \\ &= f^{h-m}(f^{m-i-1}(y)) = f^{h-m}(f^{m-i-2}(f(y))) \\ &= f^{h-m}(f^{m-i-2}(f^{i+1}(d))) = f^{h-m}(f^{m-1}(d)) \\ &= f^{h-1}(d) \notin M, \end{aligned}$$

giving a contradiction. It follows that $\mathrm{hgt}(f, f(x'), f^h(d)) = h + (m-1) - i$. Therefore, since $f^{h-1}(d) \notin M$, we infer from P2 that $\mathrm{Hgt}(f, f(x'), M) = h + (m-1) - i$. Since $i \leq m-2$, we see that $h+1 \leq h+(m-1)-i$. Consequently, $f(x') \in X \setminus C_1$ because $h := \max\{\mathrm{Hgt}(f, t, M) : t \in C_1\}$. However, $f^m(f(x')) = f(f^m(x')) = f(y) = f^{i+1}(d) = f^{i+1}(f^m(x)) = f^m(f^{i+1}(x))$, and of course $f^{i+1}(x) \in X \setminus C_1$ by our choice of d. Thus $f(x') = f^{i+1}(x)$ since $f^m \restriction (X \setminus C_1)$ is injective. So finally we have $y = f^{m-1}(f(x')) = f^{m-1}(f^{i+1}(x)) = f^i(f^m(x)) = f^i(d)$. That is to say, $I(f^{i+1}(d), f) = \{f^i(d)\}$. The assertion A3 is proved.

Since $d \in C_1$, we have $f^m(d) \in \Lambda(X, C_1, m, f) \subseteq f^m[X \setminus C]$ since by A1 the quadruple $\langle X, C_1, m, f \rangle$ is liable. So there exists $z \in X \setminus C_1$ such that $f^m(d) = f^m(z)$.

Our next task is to establish

A4. $\{f^i(z) : 0 \leq i \leq m-1\} \cap \{f^i(d) : 0 \leq i \leq m-1\} = \emptyset$.

Assume A4 to be false. Then $f^p(z) = f^r(d)$ for some $\{p, r\} \subseteq m$. Assume additionally that $p > r$. Since $m + r - p \geq 0$ while $m - p \geq 0$, we have $f^{m+r-p}(d) = f^{m-p}(f^r(d)) = f^{m-p}(f^p(z)) = f^m(z) = f^m(d)$. But we also have $h + r - p \geq m + r - p \geq 0$, and consequently $f^{h+r-p}(d) = f^{h-m}(f^{m+r-p}(d)) = f^{h-m}(f^m(d)) = f^h(d) \in M$. But $f^{h+r-p}(d) \in M$ implies $h \leq h + r - p$ by the choice of d, contrary to the assumption that $p > r$.

It follows that $p \leq r$. So now we have $0 \leq r - p \leq r \leq m-1$. By A3 and the assumption $f^p(z) = f^r(d)$ we get $z = f^{r-p}(d)$. It follows that $p < r$, since $\langle z, d \rangle \in (X \setminus C_1) \times C_1$ entails that $z \neq d$. So $r - p > 0$, and $f^{r-p}(f^m(d)) = f^m(f^{r-p}(d)) = f^m(z) = f^m(d)$. We inferred $m \leq h$ from A2. Thus there is a least integer $s \geq 0$ such that $h \leq (r-p)s + m$.

Since $f^{r-p}(f^m(d)) = f^m(d)$ (see above), $f^{(r-p)s}(f^m(d)) = \ldots = f^m(d)$, whereupon $f^m(d) = f^{(r-p)s+m}(d) = f^{(r-p)s+m-h}(f^h(d))$. Therefore, since $f^h(d) \in M$, P2 shows that $f^m(d) \in M$ and every vertex in the cycle $f^m(d) \mapsto f^m(d) \mapsto \ldots \mapsto f^{m+r-p-1}(d) \mapsto f^{m+r-p}(d) = f^m(d)$ is an element of M. Among these vertices there is one, u, satisfying the condition $f^{m-(r-p)}(u) = f^m(d)$. Since $f^{m-(r-p)}(z) = f^m(d)$ and $\{u, z\} \subseteq X \setminus C_1$, and $f^{m-(r-p)}\restriction(X \setminus C_1)$ is injective, it follows that $u = z$. Thus $z \in M$. Hence $f^{r-p}(d) \in M$ as $z = f^{r-p}(d)$. So, by the choice of d, we have $h \leq r - p$. But $r - p \leq m - 1$. So $h \leq m - 1$, contradicting the previously established fact that $m \leq h$. The proof of A4 is complete.

The function $f^i\restriction(X \setminus C_1)$ is injective for every nonnegative integer $i \leq m - 1$, and furthermore $f^m(z) = f^m(d)$. Hence, we deduce from A4 that if $j \leq m - 1$ and $f^j(d) \in X \setminus C_1$ then $f^j(z) \in C_1$. Let τ be the involution on X whose only nontrivial cycles are those transpositions $(f^i(z)f^i(d))$ for which $i \leq m - 1$ and at the same time $f^i(d) \in X \setminus C_1$.

Define

$$\begin{aligned} A &:= \{f^i(z) : 0 \leq i \leq m - 1 \text{ and } f^i(d) \in X \setminus C_1\}, \\ C_2 &:= (C_1 \setminus A) \cup \tau[A]. \end{aligned}$$

Our next task is to prove

A5. $|C_2| = |C_1|$ *and* $\langle X, C_2, m, f\rangle$ *is liable.*

Since $|A| = |\tau[A]|$, and since $A \subseteq C_1$ while $\tau[A] \subseteq X \setminus C_1$, we get immediately the desired conclusion $|C_2| = |C_1|$. So it remains to prove that $\langle X, C_2, m, f\rangle$ is liable. Notice that

$$X \setminus C_2 = ((X \setminus C_1) \setminus \tau[A]) \cup A.$$

From this, together with the facts $\tau[A] \subseteq X \setminus C_1$ and $f^m[A] = f^m[\tau[A]]$, we can easily deduce that $f^m[X \setminus C_2] = f^m[X \setminus C_1]$ and $f^m[C_2] = f^m[C_1]$. It follows that $\Lambda(X, C_2, m, f) = \Lambda(X, C_1, m, f)$. Since $\langle X, C_1, m, f\rangle$ is liable, we now have $\Lambda(X, C_2, m, f) \subseteq f^m[X \setminus C_1] = f^m[X \setminus C_2]$. Thus the quadruple $\langle X, C_2, m, f\rangle$ satisfies L1.

By A1, $f^m\restriction(X \setminus C_1)$ is injective. Therefore so is $f^m\restriction\tau[A]$ since $\tau[A] \subseteq X \setminus C_1$. Hence $f^m\restriction A$ is injective since $f^m\restriction A = (f^m\restriction\tau[A]) \circ (\tau\restriction A)$. Since $X \setminus C_2 = ((X \setminus C_1) \setminus \tau[A]) \cup A$ and $((X \setminus C_1) \setminus \tau[A]) \cap A = \emptyset$, in order to prove that $f^m\restriction(X \setminus C_2)$ is injective it suffices to show that $f^m(t) \neq f^m(f^i(z))$ for every pair $\langle t, f^i(z)\rangle \in ((X \setminus C_1) \setminus \tau[A]) \times A$. Note that $((X \setminus C_1) \setminus \tau[A]) \times \tau[A] \subseteq (X \setminus C_1) \times (X \setminus C_1)$, and of course $((X \setminus C_1) \setminus \tau[A]) \cap \tau[A] = \emptyset$. So, since $f^m\restriction(X \setminus C_1)$ is injective, and since $f^i(d) = \tau(f^i(z)) \in \tau[A]$, we surely have $f^m(t) \neq f^m(f^i(d))$. However $f^i(z) = \tau(f^i(d))$, and therefore $f^m(f^i(d)) = f^m(\tau(f^i(d)) = f^m(f^i(z))$. So $f^m(t) \neq f^m(f^i(z))$ as required. Hence $f^m\restriction(X \setminus C_2)$ is injective, and thus $\langle X, C_2, m, f\rangle$ satisfies L2.

By A1 we have $C_1 \subseteq \mathrm{Dom}(f^m)$. Consequently, since $A \subseteq C_1$, we have both $C_1 \setminus A \subseteq \mathrm{Dom}(f^m)$ and $A \subseteq \mathrm{Dom}(f^m)$. But the latter implies $\tau[A] \subseteq \mathrm{Dom}(f^m)$: For $f^i(z) \in A$ we have $f^m(f^i(z)) = f^i(f^m(z)) = f^i(f^m(d)) = f^m(f^i(d))$ and therefore $f^i(d) = \tau(f^i(z)) \in \mathrm{Dom}(f^m)$. We have established that $C_2 = (C_1 \setminus A) \cup \tau[A] \subseteq \mathrm{Dom}(f^m)$. It follows that the quadruple $\langle X, C_2, m, f\rangle$ satisfies L3, and therefore is liable. So the proof of the assertion A5 is finished.

We now prove the following three claims grouped under the title A6.

A6.1. $\{f^i(d) : 0 \le i \le m-1\} \subseteq C_2$.

A6.2. $f^-(f^{m-1}(x)) \subseteq X \setminus C_2$.

A6.3. $f{\restriction}f^-(f^{m-1}(d))$ *is injective.*

A6.1: Choose any nonnegative integer $i \le m-1$. Then by A4 and the definition of A we have $f^i(d) \notin A$. So if $f^i(d) \in C_1$ then $f^i(d) \in C_1 \setminus A \subseteq C_2$. But if $f^i(d) \in X \setminus C_1$ then $f^i(z) \in A$ and so $f^i(d) = \tau(f^i(z)) \in \tau[A] \subseteq C_2$. The assertion A6.1 follows.

A6.2: Recall that d was chosen so that $d \in C_1$ and $h = \mathrm{Hgt}(f, d, M)$. Recall also $f^m(x) = d$ and $f^h(d) \in M$. Indeed h is the largest "height" of any point in C_1 above the set M. Therefore $f^-(f^{m-1}(x)) \subseteq X \setminus C_1$. Since $X \setminus C_2 = ((X \setminus C_1) \setminus \tau[A]) \cup A$, in order to establish that $f^-(f^{m-1}(x)) \subseteq X \setminus C_2$ it suffices to show that $f^-(f^{m-1}(x)) \cap \tau[A] = \emptyset$. So we assume on the contrary that there exists $v \in \tau[A]$ such that $f^j(v) = f^{m-1}(x)$ for some nonnegative integer j. Since $v = \tau(f^i(z))$ for some nonnegative integer $i \le m-1$ with $f^i(d) \in X \setminus C_1$, we have $v = f^i(d)$ by the definition of τ. Therefore $f^{1+j+i}(d) = f^{1+j}(f^i(d)) = f^{1+j}(v) = f(f^j(v)) = f(f^{m-1}(x)) = f^m(x) = d$. Since $f^h(d) \in M$, by P2 we thus infer that if $h \le 1+j+i$ then $d = f^{1+j+i}(d) \in M$. So, since $d \in C_1$, it follows that $d \in M \cap C_1$. But we know that $M \cap C_1 = \emptyset$. So we must have instead $h > 1+j+i$, whence for any integer k such that $(1+j+i)k \ge h$ we again infer that $f^{(1+j+i)k}(d) = d$; thus again by P2 we get the impossibility $d \in M$. The assertion A6.2 is proved.

A6.3: We have $f^-(f^{m-1}(d)) = \{f^i(d) : 0 \le i \le m-1\} \cup f^-(d)$ by A3. Now, $\{f^i(d) : 0 \le i \le m-1\} \cap f^-(f^{m-1}(x)) = \emptyset$ by A6.1 and A6.2. Also, since $f{\restriction}(X \setminus C_1)$ is injective and $f^-(f^{m-1}(x)) \subseteq X \setminus C_1$, we find that $f{\restriction}f^-(f^{m-1}(x))$ is injective. Thus we see by A3 that A6.3 will be proved when we show that $I(d, f) = \{f^{m-1}(x)\}$. But $I(d, f) \subseteq X \setminus C_1$ by the choice of d. Therefore $I(d, f) = \{f^{m-1}(x)\}$ since $f{\restriction}(X \setminus C_1)$ is injective and $f(f^{m-1}(x)) = d$. The assertion A6.3 follows.

Define $b := f{\restriction}f^-(f^{m-1}(d))$. Then let

$$X_3 := X \setminus f^-(f^{m-1}(d)), \qquad C_3 := C_2 \cap X_3.$$

We next need to show

A7. *$\langle X_3, C_3, m, f \setminus b\rangle$ is liable*, *and* $|C_3| = |C_2| - m$.

Since $f(f^{m-1}(x)) = d$, we deduce from A6 that $C_2 \cap f^{-}(f^{m-1}(d)) = \{f^i(d) : 0 \le i \le m-1\}$. By A3 we see that $|\{f^i(d) : 0 \le i \le m-1\}| = m$. Therefore $|C_2 \cap f^{-}(f^{m-1}(d))| = m$, whence $|C_3| = |C_2| - m$ as claimed. It is clear by A6 that $\Lambda(X_3, C_3, m, f \setminus b) = X_3 \cap \Lambda(X, C_2, m, f)$ and $X_3 \cap f^m[X \setminus C_2] = (f \setminus b)^m[X_3 \setminus C_3]$. Therefore, since $\Lambda(X, C_2, m, f) \subseteq f^m[X \setminus C_2]$ by A5, we get $\Lambda(X_3, C_3, m, f \setminus b) \subseteq (f \setminus b)^m[X_3 \setminus C_3]$. Obviously $(f \setminus b)\restriction(X_3 \setminus C_3) = f\restriction(X_3 \setminus C_3)$ and $X_3 \setminus C_3 \subseteq X \setminus C_2$. Therefore, since $f\restriction(X \setminus C_2)$ is injective by A5, we find that $(f \setminus b)\restriction(X_3 \setminus C_3)$ is also injective. Since $\mathrm{Dom}((f \setminus b)^m) = X_3 \cap \mathrm{Dom}(f^m)$, and since $C_2 \subseteq \mathrm{Dom}(f^m)$ by A5, we deduce furthermore that $C_3 \subseteq \mathrm{Dom}((f \setminus b)^m)$. Hence the quadruple $\langle X_3, C_3, m, f \setminus b\rangle$ is liable. The assertions A7 are now proved.

Recall now that our original aim was to show that m is a factor of $|C|$. By A1, A5, and A7 we have $|C| = |C_3| + m$. However, by A7 and the inductive hypothesis, since $|C_3| < |C|$ we know that m is a factor of $|C_3|$. It follows that m is a factor of $|C|$. ∎

Theorem 1 is an immediate consequence of Lemmas 2 and 3.

3. Concluding remarks. The following corollary supplies a correct proof of [2, Theorem 1].

Corollary 4. *The following four assertions are equivalent*:

(4.1) *m is a factor of $|C|$.*

(4.2) *For each infinite set X with $C \subset X$ there is a function $g : X \to X$ such that g^m is a bijection from X onto $X \setminus C$.*

(4.3) *For each infinite set X with $C \subset X$ there is a function $f \subseteq X \times X$ such that $f^m\restriction(X \setminus C)$ is a bijection from $X \setminus C$ onto X.*

Proof. (4.1)⇒(4.2): Without loss of generality we suppose that $mq = C \subseteq \omega \subset X$ for some integer $q \ge 0$. For any permutation p on the set $X \setminus \omega$ we define $g := p \cup \{\langle i, i+q\rangle : i \in \omega\}$. Clearly g^m is a bijection of X onto $X \setminus C$.

(4.2)⇒(4.3): Let $g : X \to X$ be a function such that g^m is a bijection from X onto $X \setminus C$. Then g is injective. So $g^{-1} \in \mathrm{Prt}(X)$. Let $f := g^{-1}$. The equality $(r^{-1})^m = (r^m)^{-1}$ holds for every binary relation r. Thus $f^m = (g^m)^{-1}$. But $(g^m)^{-1}$ is a bijection from $X \setminus C$ onto X. It follows that $(g^m)^{-1}\restriction(X \setminus C) = (g^m)^{-1} = f^m = f^m\restriction(X \setminus C)$ is a bijection from $X \setminus C$ onto X.

(4.3)⇒(4.1): Use Theorem 1. ∎

We conclude this paper by offering two examples that help illuminate the result established above. Example 1 displays a finite C and an integer m for which (4.1) holds, and also a function h such that for every set $Y \subseteq X \setminus C$

the injective function $h^m{\restriction}Y$ fails to be a bijection from Y onto X. It is clear that $\mathrm{Prt}(X)$ contains an extension H of h for which $H^m{\restriction}(X \setminus C)$ is a bijection from $X \setminus C$ onto X if and only if the set X is infinite. Incidentally, for no set $Y := X \setminus C$ is it the case that the quadruple $\langle X, C, m, h\rangle$ is liable, since $0 \in C \setminus \mathrm{Dom}(h^m)$.

Example 1. Let $15 \subseteq X$. Let $m := 3$. Let $C := 6$. Let $h := \{\langle i, i-3\rangle : 3 \le i \le 14\}$. Then the finite injective function $h^3{\restriction}Y$ merely slides a portion of the set $Y := X \setminus C$ over to cover the set C.

Is there a property R, applicable to f with $|I(y, f)| > 1$ for some $y \in Y$, such that if some $f \in \mathrm{Prt}(X)$ satisfies R then m and $|C|$ are arithmetically related? In this spirit we pose the following

Problem 1. Let $0 < k \in \omega$. Let X be infinite. Let there exist some $f \in \mathrm{Prt}(X)$ with $Y \subseteq \mathrm{Dom}(f^m)$, $|Y \cap I(x, f)| = k$ for every $x \in X$, and $f^j[Y] \subset X$ for every $j \in m$, but such that $f^m[Y] = X$. Then how must m, k, and $|C|$ be related arithmetically?

The wording of Lemma 3 is delicate: Not just any Y will serve. Indeed, if $X = C = mq$ for q a positive integer then m is a factor of $|C|$ but there is no $f \in \mathrm{Prt}(X)$ for which $\langle X, C, m, f\rangle$ is liable.

Define $\sigma(m, q)$ to be the smallest ordinal α such that there exists $f \in \mathrm{Prt}(\alpha)$ for which $\langle \alpha, mq, m, f\rangle$ is liable. It is easy to see that $\sigma(1, 1) = 3$: A smallest X for $C = mq = 1$ is attained when $X := 3$, with the function $f := \{\langle 2, 1\rangle, \langle 1, 0\rangle, \langle 0, 0\rangle\}$ or $f := \{\langle 2, 1\rangle, \langle 1, 0\rangle, \langle 0, 1\rangle\}$.

Problem 2. Characterize $\sigma(m, q)$ for all positive integers m and q.

The next example suggests that $mq < \sigma(m, q) \in \omega$ may invariably be the case.

Example 2. Let $C := \{3, 4, 5, 11, 12, 13, 14, 15, 16, 32, 33, 34, 35, 36, 42\}$ where $X := 100$, let $m := 3$, and let

$$\begin{aligned} f := \{&\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \langle 4,5\rangle, \langle 5,3\rangle,\\ &\langle 6,7\rangle, \langle 7,8\rangle, \langle 8,9\rangle, \langle 9,10\rangle, \langle 10,11\rangle, \langle 11,12\rangle, \langle 12,13\rangle, \langle 13,14\rangle,\\ &\langle 14,15\rangle, \langle 15,16\rangle, \langle 16,17\rangle, \langle 17,18\rangle, \langle 18,19\rangle, \langle 19,14\rangle, \langle 20,21\rangle,\\ &\langle 21,22\rangle, \langle 22,23\rangle, \langle 23,24\rangle, \langle 24,25\rangle, \langle 25,26\rangle, \langle 26,27\rangle, \langle 27,24\rangle,\\ &\langle 28,29\rangle, \langle 29,30\rangle, \langle 30,31\rangle, \langle 31,32\rangle, \langle 32,33\rangle, \langle 33,34\rangle, \langle 34,35\rangle,\\ &\langle 35,36\rangle, \langle 36,37\rangle, \langle 37,38\rangle, \langle 38,39\rangle, \langle 39,40\rangle, \langle 40,41\rangle, \langle 41,42\rangle,\\ &\langle 42,35\rangle, \langle 43,44\rangle, \langle 44,45\rangle, \langle 45,37\rangle\}. \end{aligned}$$

Example 2 indicates that m can be guaranteed to be a factor of $|C|$ by rather mysterious conditions. There, the set X is finite, the function $f \subseteq X \times X$ is not injective, but $\langle X, C, m, f\rangle$ is liable anyway.

It is reasonable to ask whether results analogous to our Corollary 4 hold for certain nonpower words. The first such word we would propose for consideration is the word $x^m y^n$ of "complexity two".

PROBLEM 3. Let m and n be positive integers. Let $\{f, g\} \subseteq \mathrm{Prt}(X)$ be such that $g^n \restriction Y$ and $f^m \restriction g^n[Y]$ are injective, $f^m g^n \restriction Y$ is a bijection from Y onto X, neither $g^n \restriction Y$ nor $f^m \restriction g^n[Y]$ is a restriction of $\{\langle x, x\rangle : x \in X\}$, but $f^m g^{n-1}[Y] \subset X$. Then must $m + n$ be a factor of $|X \setminus Y|$?

Acknowledgments. The clarity of our proofs benefited from our conversations with Gregory Hill and with Sylvia Bare Silberger.

References

[1] K. Rother, D. M. Silberger and M. E. Wilson, *The reverse spelling of an FPrt-universal word in two letters*, Algebra Universalis 36 (1996), 202–221.

[2] D. M. Silberger, *Universal words of complexity three*, ibid. 11 (1980), 393–395.

Department of Mathematics
University of Puerto Rico
Mayagüez, PR 00681, U.S.A.
E-mail: w_dziobiak@rumac.upr.clu.edu

Department of Mathematics
University of Colorado
Boulder, CO 80309, U.S.A.
E-mail: andrzej@cs.colorado.edu

Department of Mathematics
State University of New York
New Paltz, NY 12561, U.S.A.
E-mail: grace@mcs.newpaltz.edu
silberger@mcs.newpaltz.edu
donsilbs@idsi.net

Received 2 August 1999