Composing Functions to Reduce Image Size

N. Sauer and M.G. Stone

University of Calgary[1]

Abstract. If f and g are self-maps on a finite set M with $n = |M|$, then the images of various composite functions such as f^2gf and g^2f^2g may have diferent size. There is of course a minimal image size which can be achieved by the composition of particular functions. It can be difficult however to discover the size of this minimal image. We seek to determine "words" over a finite alphabet S which, by specifying function compositions when letters are interpreted as functions, allow one to test for each k whether or not there exists among all compositions an image of size $n-k$ or less. For two functions f and g, $W_1 = fg$ is clearly such a "word" for $k = 1$, since no composition of functions f and g has an image smaller than or equal to $|M| - 1$, if $W_1 = fg$ fails to do so. We prove the existence of such a word W_k for each k, and exhibit a recursive procedure for the generation of W_{k+1} from W_k. The words W_k depend only upon the finite alphabet S, and are independent of the size of the finite set M over which the symbols from S are to be interpreted as functions.

Introduction

A problem of some current interest is the characterization of all identities which hold in H_n, the monoid of all self-maps on an n-element set. The authors in [2] give a new proof of a result from [1]: the existence for each n, of non-trivial identities which hold in H_n but not in H_{n+1}. Central to our investigations of H_n is the existence of a certain word W in the free semigroup S^* on a finite alphabet S. This word should have a minimal image among all compositions of specified functions from H_n, when the letters of S are interpreted among those functions. Equivalently, every other word V in S^* should be one-to-one on the image of W, when V and W are interpreted as composite functions via a common interpretation of S in H_n. In H_2 for example, $W_1 = AB$ is such a word for the two generator free semigroup S^* over the alphabet $S = \{A, B\}$. In H_3, $W_2 = ABA^2B^2AB$ is also such a word, although this is already rather more troublesome to verify! More surprisingly perhaps W_1 and W_2 fulfill a similar purpose in all H_n. If any word V in S^* for $S = \{A, B\}$ has the property that $|imageV| \leq n-1$ for a particular interpretation of A and B as functions in H_n then $W_1 = AB$ has that property. Likewise if any word V in S^* over $S = \{A, B\}$ has the property that $|imageV| \leq n-2$ for an interpretation of A, B in H_n then $W_2 = ABA^2B^2AB$ as well has the property that $|imageV| \leq n-1$ for that same interpretation of A and B. We provide below a general framework for the description of words with such properties.

[1]This research has been supported in part by NSERC grants 69-1325 and 69-3039.

1. Deficiency

Let S be a finite alphabet and M a set with $|M| = n$. A function $\alpha : S \to M^M$ is an interpretation of the alphabet S as self-maps on M. We extend α naturally to an interpretation of S^*. For $V = A_1 A_2 \ldots A_t, \alpha(V) = \alpha(A_1)\alpha(A_2)\ldots\alpha(A_t)$ where concatenation is of course interpreted as composition of functions. For $V \in S^*$ and α an interpretation of S as self maps on M we define the deficiency of $\alpha(V)$ and the deficiency of α when M is finite:

Definition 1.1.

$$def\,(\alpha(V)) = |M| - |image\ \alpha(V)|$$

$$def\,(\alpha) = max\{def\,(\alpha(V)); V \in S^*\}$$

Definition 1.2. *For any natural number k we say that $V \in S^*$ has property Δ_k for S, provided that for all interpretations α of S as self-maps on any finite set M: if $def\,(\alpha) \geq k$ then $def\,(\alpha(V)) \geq k$.*

Example 1.3: Observe that for $S = \{A_1, \ldots, A_t\}$ the product $W_1 = A_1 A_2 \ldots A_t$ has property Δ_1 for S. That is to say: if any word V in S^*, interpreted as self-maps in a finite set M, has image smaller than $|M|$, then $|image(\alpha W_1)| < |M|$, for the same interpretation α.

Our main result, proved in the next two sections, is the following:

Theorem 1.5. *For every finite alphabet S and each natural number k there is a word $W_k \in S^*$ which has property Δ_k for S.*

This result follows from the more explicit Theorem 3.3. The reader is invited however to first verify that $W_2 = ABA^2B^2AB$ has property Δ_2 for $S = \{A, B\}$. Even to test the truth of this observation in a specific case, say on a three element set, is not entirely trivial.

2. A Combinatorial Lemma

We require a simple combinatorial fact, which we state here as:

Lemma 2.1. *If $C_1, C_2, \ldots, C_t$ is a partition of a finite set S with $|S| = n$ into t mutually disjoint non-empty classes, then the product of the class sizes is small:*

$$\prod_{j=1}^{t} |C_j| \leq 2^{n-t}$$

Moreover, equality holds iff $|C_j| \leq 2$ for all j.

Proof: Let $D = \{T \subset S; T \text{ is a transversal, ie: } |T \cap C_j| = 1 \text{ for } j = 1, 2, \ldots, t\}$. Thus $|D| = \prod_{j=1}^{t} |C_j|$. Fix $A \in D$. Observe that the function $\varphi : D \to powerset\,(S - A)$ given by $\varphi(T) = (T - A)$ maps each $T \in D$ to a subset of $S - A$. It is easy to verify that φ is one-to-one, hence $|D| \leq 2^{n-t}$ as required. If moreover φ is onto $S - A$, each $|C_j| \leq 2$, and $\prod_{j=1}^{t} |C_j| = 2^{n-t}$ holds if each $|C_j| \leq 2$. ∎

Lemma 2.2. *For any self-map g from M into M with $|M| = n$ finite, if $|image(g)| = n - k$, then g is one-to-one on at most 2^k subsets of M of size $n-k$. Moreover g is one-to-one on exactly 2^k sets of size $(n-k)$ iff each class of $ker(g)$ has size one or two.*

Proof: Let $C_1, C_2, \ldots, C_t$ be the equivalence classes of the kernel for g, that is $x \sim y$ iff $g(x) = g(y)$. Then there are exactly $t = n - k$ of these classes, and each subset of M of size $n-k$ on which g is one-to-one consists of a transversal from these classes. There are at most $\prod_{j=1}^{t} |C_j| \leq 2^{n-t} = 2^{n-(n-k)} = 2^k$ such transversals, by Lemma 2.1. The number of transversals is exactly 2^k iff each class has size 1 or 2. ∎

3. Proof of Theorem 1.5

We wish to show the existence of W_k with property Δ_k for each natural number k. Observe that if $S = \{A_j : j \in s\}$, then trivially $W_1 = \prod_{j=1}^{s} A_j$ has property Δ_1 for S.

If $U = VW$ we shall say that W is an initial subword of U. We use $||W||$ to denote the length of a word W in S^*. Thus if $A, B \in S$ we have $||A^2BA|| = 4$. Also, when we work within a fixed interpretation $\alpha : S \to H^n$, we will write simply W in place of αW and rely on context to make it clear that we deal with the interpretation of the words in question. Finally notice that the empty word will be consistently interpreted as the identity function. We prove:

Lemma 3.1. *Let $k \geq 1$, S a finite alphabet and $\alpha : S \to n^n$. If $|imW| = n-k$ and $|imWVW| = n-k$ for every word V with $1 \leq ||V|| \leq 1 + \frac{3}{4}2^k$, then $|imU| \geq n-k$ for every word U.*

Proof: Suppose some word U satisfies $|imU| < n-k$, then $|imWUW| < n-k$ as well. Let U be the shortest word with $|imWUW| < n-k$. It suffices to see $||U|| \leq 1 + \frac{3}{4}2^k$. We know (Lemma 2.2) that W is one-to-one on at most 2^k sets of size $n-k$. We distinguish two cases:

Case 1: W is one-to-one on fewer than 2^k sets of size $n-k$.

Recall that W is one-to-one on exactly 2^k sets of size $n-k$ iff each block of kernel W has size one or two (Lemma 2.2). So some class of kernel W has at least three elements, say kernel $W = \{C_1, C_2, \ldots, C_{n-k}\}$ with $|C_1| = m \geq 3$. Then W is one-one on exactly as many $(n-k)$-sets as there are transversals of kernel W, which is at most $m \cdot 2^{n-m-(n-k-1)} = m \cdot 2^{k+1} \cdot 2^{-m}$. But $m \cdot 2^{k+1} \cdot 2^{-m} \leq \frac{3}{4}2^k$ for $m \geq 3$. Thus W is one to one on at most $\frac{3}{4}2^k$ sets of size $n-k$. If $U = A_r A_{r-1} \ldots A_2 A_1$ then by the minimality of U with respect to $|imWUW| < n-k$, all of the words $W, A_1W, A_2A_1W, A_3A_2A_1W, \ldots, A_{r-1}A_{r-2}\ldots A_2A_1W$ have distinct images of size $n-k$, and W is one-to-one on each of them. Thus $r \leq \frac{3}{4}2^k$ and $||U|| \leq 1 + \frac{3}{4}2^k$.

Case 2: W is one-to-one on exactly 2^k sets of size $n-k$.

Then there are exactly k kernel classes of W with size two. Every other kernel class has size one, say kernel $W = \{C_1, C_2, \ldots, C_{n-k}\}$ with $|C_j| = 2$ for $1 \leq j \leq k$ and $|C_j| = 1$ for $j > k$. Once again we consider all of the initial subwords of U, concatenated with W. The set of images of the words W, A_1W, A_2A_1W, $A_3A_2A_1W$, $\ldots$, $A_{r-1}A_{r-2}\ldots A_2A_1W$ are distinct transversals of $ker\,W$ by the minimality of U with respect to $|im\,WUW| < n-k$. Since WA_r collapses some pair (a,b) in the transversal $A_{r-1}\ldots A_2A_1W$, none of the other transversals listed above contains that pair. This follows from the minimality condition on U. There are at most $\frac{3}{4}2^k$ transversals which exclude a given pair (a,b). So $r-1 \leq \frac{3}{4}2^k$ and $r \leq 1 + \frac{3}{4}2_k$ as required. ∎

If $k = 1$ and $S = \{A, B\}$ is a two letter alphabet, we can improve the result of Lemma 3.1.

Lemma 3.2. *If $S = \{A, B\}$ and $|im\,ABAAB| = |im\,ABBAB| = (n-1)$ then for all words $U \in S^*$, $|im\,U| \geq (n-1)$.*

Proof: Either $|im\,B| = n-1$ or not.

Case 1: $|im\,B| = (n-1)$.

Observe that $ker\,B$ has exactly two transversals, X and Y. It suffices to prove that AX, AY, BX and BY are all transversals, or that $AX = BX = X$ or that $AY = BY = Y$. Observe that $im\,BAB = im\,B = im\,BBAB = im\,BAAB$ (each is obviously contained in *image* B and cannot be smaller since $|im\,ABAAB| = |im\,ABBAB| = (n-1)$). Hence each of $im\,AAB$, $im\,AB$ and $im\,BAB$ are transversals of $ker B$. Also $im\,B$ and $im\,BAB$ are transversals as well. If $im\,B = im\,AB$ then $im\,BB = im\,BAB = im\,B$. So for $X = im\,AB$ we have $AX = BX = X$. If $im\,B \neq im\,AB$ then $X = im\,B$ and $Y = im\,AB$ are the two transversals. Thus $AX = im\,AB = Y$. Also $BY = im\,BAB = im\,B = X$. Next $BX = im\,BBAB = im\,B = X$, and finally $AY = im\,AAB$ (which is a transversal). Hence AY is X or Y. This completes case 1.

Case 2: $|im\,B| = n$ and $|im\,A| = (n-1)$.

Let us denote the two transversals of $ker A$ by X and Y and proceed as in case 1. Observe that $im\,A = im\,AB = im\,AAB = im\,ABBAB$, hence $X = im\,A = im\,AB$ is a transversal of $ker A$. Note $im\,AA = im\,AAB$ (since $im\,A = im\,AB$) thus $im\,AA = im\,A$, and $AX = X$.

If $im\,BA = im\,A$ then $BX = X$ as well and we are done. If $im\,BA \neq im\,A$, observe that $|im\,ABA| = |im\,ABAAB| = (n-1)$ so $im\,BA$ is a transversal of $ker A$. Thus $Y = im\,BA$ is the other transversal of $ker A$. Next, $im\,ABA \subset im\,A$ and $|im\,ABA| = |im\,A| = (n-1)$, because $|im\,ABAAB| = (n-1)$. Thus $im\,ABA = im\,A$ so $AY = X$. Finally, $|im\,ABBAB| = (n-1)$, so $BBAB$ is a transversal, and also $im\,BBA = im\,BBAB$ is a transversal. Thus BY is a transversal, as required. This completes case 2 and the proof of the lemma. ∎

Theorem 3.3. *Let $k \geq 1$ and $S = A_1, A_2, \ldots A_t$ be a finite alphabet. The following words W_k have property Δ_k for S:*

$$W_1 = \prod_{j=1}^{t} A_j$$

$$W_{k+1} = \prod_{V \in Q} (W_k V)\, W_k$$

where $Q = \{V \in S^*; 1 \leq \|V\| \leq 1 + \frac{3}{4}2^k\}$.

Proof: Follows from Lemma 3.1. ∎

Corollary 3.4. *For $S = \{A, B\}$ the word $W = ABA^2B^2AB$ has property Δ_2 for S.*

Proof: If some word V has $|im\, V| \leq (n-2)$ then by Lemma 3.2 one of the words $ABAAB$ or $ABBAB$ also has image size less than or equal to $(n-2)$. But each of these words occurs as a subword in $W = ABA^2B^2AB$, so $|im\, W| \leq (n-2)$. ∎

Note that Corollary 3.4 confirms our earlier remarks about the properties of ABA^2B^2AB. Theorem 3.3 provides a recursive means for the construction (over any finite alphabet) of words which discriminate for deficiency k.

Now we can answer the question posed in the introduction regarding compositions of maps which yield a minimum image. Because W_{n+1} contains as conjuncts all W_j with $1 \leq j \leq k$ we have:

Corollary 3.5. *For every finite alphabet S and each fixed n, the word W_{n-1} has for any interpretation $\alpha : S \to H_n$ the smallest image of any composition of functions corresponding to a word $W \in S^*$ under the same interpretation α.*

Proof: If the smallest such image has size one then W_{n-1} has image size one as well, since W_{n-1} has property Δ_{n-1} for S. If the smallest such image has size j for some $2 \leq j \leq (n-1)$ then W_{n-j} has this image size as well, since W_{n-j} has property Δ_{n-j} for S. But for $2 \leq j \leq (n-1)$, W_{n-j} is a conjunct in W_{n-1} and thus the image of W_{n-1} has size j as well. Finally if the smallest image has size n, then of course every $x \in S$ is interpreted as a permutation, and thus W_{n-1} has image size n as well. ∎

Open Problem: For a given alphabet S with $|S| = t$ determine for each positive integer k the length $\mu_k(t)$ of the shortest word W_k which has property Δ_k for S. We can show easily for example for $t = 2$, with say $S = \{A, B\}$, that $W_1 = AB$ and $W_2 = ABA^2B^2AB$ are minimal. Thus $\mu_1(2) = 2, \mu_2(2) = 8$. Indeed the product $W_1 = \prod_{j=1}^{s} A_j$ is clearly the shortest possible word with property Δ_1 for any finite S.

References

1. Denneke and R. Pöschel, *The characterization of Primal Algebras by Hyper-identities*, Contributions to General Algebra **6**. Krems (1988), 67–87. Verlag-Teubner, Stuttgart.
2. R.Pöschel, N.Sauer and M.G.Stone, *A problem concerning identities in full transformation Semigroups*, manuscript.