SQUARE ROOTS IN FINITE FULL TRANSFORMATION SEMIGROUPS

by MARY SNOWDEN and J. M. HOWIE

Let X be a finite set and let $\mathcal{T}(X)$ be the full transformation semigroup on X, i.e. the set of all mappings from X into X, the semigroup operation being composition of mappings. This paper aims to characterize those elements of $\mathcal{T}(X)$ which have square roots. An easily verifiable necessary condition, that of being *quasi-square*, is found in Theorem 2, and in Theorems 4 and 5 we find necessary and sufficient conditions for certain special elements of $\mathcal{T}(X)$. The property of being *compatibly amenable* is shown in Theorem 7 to be equivalent for all elements of $\mathcal{T}(X)$ to the possession of a square root.

The work reported here formed part of an M.Sc. Thesis [4] submitted to the University of St Andrews in 1979 by the first-named author.

1. Preliminaries. For unexplained terms in semigroup theory see [2]. Mapping symbols will be written on the right. We shall denote the range of a mapping $\alpha : X \to X$ by $X\alpha$ or by ran α, and by $\alpha \circ \alpha^{-1}$ we shall mean the equivalence relation

$$\{(x, y) \in X \times X : x\alpha = y\alpha\}.$$

If $|X| = n$ then the $\mathcal{J}$-classes of $\mathcal{T}(X)$ are $J^{(1)}, \ldots, J^{(n)}$, where

$$J^{(r)} = \{\alpha \in \mathcal{T}(X) : |X\alpha| = r\}$$

is the set of mappings of rank r. (See [2, Ex.II.10].) Clearly

$$J^{(1)} < J^{(2)} < \ldots < J^{(n)}.$$

The principal factors of $\mathcal{T}(X)$ are thus $J^{(1)}$ (completely simple) and $J^{(r)} \cup \{0\}$, $r = 2, \ldots, n$ (completely 0-simple).

Notice that $J^{(n)} = \mathcal{G}(X)$, the symmetric group on X. Since

$$J_{\alpha^2} \leq J_\alpha$$

for each α in $\mathcal{T}(X)$ it follows that an element of $J^{(n)}$ has a square root in $\mathcal{T}(X)$ if and only if it has a square root in $J^{(n)}$. Thus the characterization of squares in $J^{(n)}$ is a purely group theoretical problem. It is solved by the following theorem, which is deducible from the results of Isaacs [3], but which is proved here for completeness.

THEOREM 1. *Let X be a finite set. An element α of $\mathcal{G}(X)$ is a square if and only if for each even number k the decomposition of α into disjoint cycles involves an even number of cycles of length k.*

Proof. Disjoint cycles, since they operate non-trivially on disjoint subsets of X, commute with each other. Thus if $C_1, \ldots, C_r$ are disjoint cycles then

$$(C_1 \ldots C_r)^2 = C_1^2 \ldots C_r^2.$$

Suppose now that α in $\mathcal{G}(X)$ has a square root β in $\mathcal{G}(X)$. Writing β as $C_1 \ldots C_r$, a product of disjoint cycles, we then have that

$$\alpha = \beta^2 = C_1^2 \ldots C_r^2.$$

If we write the cycle C_i as $(a_1 a_2 \ldots a_l)$ then if l is odd we have

$$C_i^2 = (a_1 a_3 \ldots a_l a_2 a_4 \ldots a_{l-1}),$$

a cycle of (odd) length l; while if l is even then

$$C_i^2 = (a_1 a_3 \ldots a_{l-1})(a_2 a_4 \ldots a_l),$$

a product of two disjoint cycles of equal length $l/2$. The decomposition of α into disjoint cycles is obtained by decomposing each of $C_1^2, \ldots, C_r^2$, and cycles of even length arise only when C_i is of length divisible by 4. The effect is that even cycles occur in pairs of equal length, so that α has the property described in the theorem.

Conversely, suppose that in the disjoint cycle decomposition of α there is an even number of cycles of each even length k. Each odd cycle $(a_1 a_2 \ldots a_{2k+1})$ is a square, since

$$(a_1 a_2 \ldots a_{2k+1}) = (a_1 a_{k+2} a_2 a_{k+3} \ldots a_k a_{2k+1} a_{k+1})^2.$$

Also, the product of two disjoint cycles of equal even length l is a square:

$$(a_1 a_2 \ldots a_l)(b_1 b_2 \ldots b_l) = (a_1 b_1 a_2 b_2 \ldots a_l b_l)^2.$$

By these devices one expresses α as a product $C_1^2 \ldots C_t^2$, where $C_1, \ldots, C_t$ are disjoint cycles. Thus $\alpha = \beta^2$, where $\beta = C_1 \ldots C_t$. This completes the proof.

In analysing elements of $\mathcal{T}(X)$ it is useful to observe that since X is finite the descent

$$X \supseteq X\alpha \supseteq X\alpha^2 \supseteq \ldots$$

cannot continue indefinitely. Evidently if $X\alpha^i = X\alpha^{i+1}$ then $X\alpha^{i+1} = X\alpha^{i+2}$; hence there exists $k \geq 0$ such that

$$X \supset X\alpha \supset \ldots \supset X\alpha^k = X\alpha^{k+1} = X\alpha^{k+2} = \ldots.$$

Let us refer to k as the *contraction factor* of α and write $k = \operatorname{cont} \alpha$. The subset $X\alpha^k$ will be called the *stable range* of α and will be written as $\operatorname{stran} \alpha$. If $\operatorname{cont} \alpha = 0$ then $X = X\alpha$ and so α is a permutation of X. Elements α such that $\operatorname{cont} \alpha = 1$ occur in all J-classes $J^{(r)}$ with $r < n(=|X|)$: for such elements, $\alpha \,|\, X\alpha$ is a permutation of $X\alpha$. In all cases $\alpha \,|\, \operatorname{stran} \alpha$ is a permutation of $\operatorname{stran} \alpha$. We say that α is a *quasi-square* element of $\mathcal{T}(X)$ if the permutation $\alpha \,|\, \operatorname{stran} \alpha$ has a square root in the symmetric group $\mathcal{G}(\operatorname{stran} \alpha)$.

2. Quasi-square elements.　We begin by proving

LEMMA 1. *Let $\alpha \in J^{(r)} \subseteq \mathcal{T}(X) \setminus \mathcal{G}(X)$ and suppose that $\operatorname{cont} \alpha = 1$. Let $k \geq 2$ be an integer. If there exists β in $\mathcal{T}(X)$ such that $\beta^k = \alpha$ then $\beta \,|\, \operatorname{ran} \alpha$ is a permutation of $\operatorname{ran} \alpha$ and $(\beta \,|\, \operatorname{ran} \alpha)^k = \alpha \,|\operatorname{ran} \alpha$.*

Proof. Let ran $\alpha = \{a_1, \ldots, a_r\}$. Since cont $\alpha = 1$ we have that $\alpha \,|\, \text{ran}\, \alpha$ is a permutation. Thus

$$a_i \alpha = a_{i\mu} \qquad (i = 1, \ldots, r),$$

where μ is a permutation of $\{1, \ldots, r\}$. If we write $a_{i\mu} \alpha^{-1} = A_i$ $(i = 1, \ldots, r)$, we have $a_i \in A_i$ and we may write

$$\alpha = \begin{pmatrix} A_1, \ldots, A_r \\ a_{1\mu}, \ldots, a_{r\mu} \end{pmatrix}.$$

If $\beta^k = \alpha$ then β must be of rank $s \geq r$ and $\beta \circ \beta^{-1} \subseteq \alpha \circ \alpha^{-1}$. Since $a_i(\alpha \circ \alpha^{-1}) = A_i$ we have

$$a_i(\beta \circ \beta^{-1}) = B_i \subseteq A_i \qquad (i = 1, \ldots, r).$$

If $a_i \beta (= B_i \beta) = b_i$ $(i = 1, \ldots, r)$, then

$$b_i \beta^{k-1} = a_i \beta^k = a_i \alpha = a_{i\mu}.$$

Hence, for $i = 1, \ldots, r$,

$$a_i = b_{i\mu^{-1}} \beta^{k-1},$$

and so

$$b_i = a_i \beta = b_{i\mu^{-1}} \beta^k = b_{i\mu^{-1}} \alpha \in \{a_1, \ldots, a_r\}.$$

Thus $\{b_1, \ldots, b_r\} \subseteq \{a_1, \ldots, a_r\}$, and since $b_1, \ldots, b_r$ are all distinct the two sets are in fact equal. Hence $\beta \,|\, \text{ran}\, \alpha$ is a permutation of ran $\alpha = \{a_1, \ldots, a_r\}$. Since $\beta^k = \alpha$ it is now obvious that

$$(\beta \,|\, \text{ran}\, \alpha)^k = \alpha \,|\, \text{ran}\, \alpha.$$

THEOREM 2. *Let $\alpha \in \mathscr{T}(X)$ where X is a finite set. If α has a square root in $\mathscr{T}(X)$ then α is quasi-square.*

Proof. If cont $\alpha = 0$ this is trivial, while if cont $\alpha = 1$ Lemma 1 shows that the existence of a square root for α implies that $\beta \,|\, \text{ran}\, \alpha$ is a square root within $\mathscr{G}(\text{ran}\, \alpha)$ for the permutation $\alpha \,|\, \text{ran}\, \alpha$. Suppose now that cont $\alpha = k > 1$ and that α has a square root β in $\mathscr{T}(X)$. Then $X\alpha^k = X\alpha^{2k}$ and so cont $(\alpha^k) = 1$. Moreover $\beta^{2k} = \alpha^k$ and so by Lemma 1, $\beta \,|\, \text{ran}\, \alpha^k$ is a permutation of ran $\alpha^k = \text{stran}\, \alpha$. Since $\beta^2 = \alpha$ it is now easily seen that

$$(\beta \,|\, \text{stran}\, \alpha)^2 = \alpha \,|\, \text{stran}\, \alpha.$$

Thus α is quasi-square.

The main usefulness of this theorem lies in its contrapositive form: if α is not quasi-square then it cannot have a square root in $\mathscr{T}(X)$. Thus, for example, if $X = \{1, \ldots, 9\}$ and

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 3 & 8 & 9 & 8 & 9 & 7 \end{pmatrix}$$

then $\operatorname{stran} \alpha = X\alpha^2 = \{3, 4, 7, 8, 9\}$ and $\alpha \mid \operatorname{stran} \alpha = (34)(789)$. By Theorem 1 this has no square root in $\mathscr{G}(\{3, 4, 7, 8, 9\})$ and so α has no square root in $\mathscr{T}(\{1, \ldots, 9\})$.

In the case where $\operatorname{cont} \alpha = 1$ we have a converse to Theorem 2.

THEOREM 3. *Let* $\alpha \in \mathscr{T}(X)$ *and suppose that* $\operatorname{cont} \alpha = 1$. *Then* α *has a square root in* $\mathscr{T}(X)$ *if and only if it is quasi-square.*

Proof. Half of this is included in Theorem 2. Suppose now that α, with contraction factor 1, is quasi-square. We may, as in the proof of Lemma 1, write α as

$$\begin{pmatrix} A_1, \ldots, A_r \\ a_{1\mu}, \ldots, a_{r\mu} \end{pmatrix}$$

where $a_i \in A_i$ $(i = 1, \ldots, r)$ and where μ is a permutation of $\{1, \ldots, r\}$. The permutation $\alpha \mid \operatorname{ran} \alpha$ is described by $a_i \to a_{i\mu}$ $(i = 1, \ldots, r)$. Since α is quasi-square there exists a permutation ν of $\{1, \ldots, r\}$ such that $\nu^2 = \mu$. Then the element

$$\beta = \begin{pmatrix} A_1, \ldots, A_r \\ a_{1\nu}, \ldots, a_{r\nu} \end{pmatrix}$$

of $\mathscr{T}(X)$ is a square root for α.

This completes the proof of Theorem 3. Notice, however, that by [2, Ex.II.10] the square root β obtained for α has the property that $\beta \mathscr{H} \alpha$; for α and β have the same range $\{a_1, \ldots, a_r\}$, and $\alpha \circ \alpha^{-1}$, $\beta \circ \beta^{-1}$ both have equivalence classes $A_1, \ldots, A_r$. We thus have:

COROLLARY. *Let* $\alpha \in \mathscr{T}(X)$, *with* $\operatorname{cont} \alpha = 1$. *If* α *has a square root in* $\mathscr{T}(X)$ *then it has a square root in its own* $\mathscr{H}$-*class.*

3. Elements in extremal $\mathscr{J}$-classes. We have seen (Theorem 1) how to recognise squares in the top $\mathscr{J}$-class $J^{(n)}$. The bottom $\mathscr{J}$-class $J^{(1)}$ presents no problem at all. It consists of all the constant mappings of X and is a right zero semigroup. Every element is its own square root.

We now examine the $\mathscr{J}$-classes $J^{(n-1)}$ and $J^{(2)}$.

THEOREM 4. *Let* $|X| = n \geq 3$ *and let* $\alpha \in J^{(n-1)}$. *Then* α *has a square root in* $\mathscr{T}(X)$ *if and only if* α *is quasi-square and* $\operatorname{cont} \alpha = 1$.

Proof. In view of Theorem 3 we require to show only that if $\alpha \in J^{(n-1)}$ and $\operatorname{cont} \alpha > 1$ then α has no square root. A square root β for such an α would have to lie in $J^{(n-1)}$, since $\beta \in J^{(n)}$ implies $\beta^2 \in J^{(n)}$. If $\operatorname{cont} \beta = 1$ then $X\beta^2 = X\beta^4$; hence $\operatorname{cont}(\beta^2) = 1$ and so β^2 cannot equal α. On the other hand if $\operatorname{cont} \beta > 1$ then $X\beta^2 \subset X\beta$ and so

$$J_{\beta^2} < J_\beta = J^{(n-1)};$$

hence again β^2 cannot equal α, and so no square root of α can exist.

THEOREM 5. *Let $|X| = n \geqslant 4$ and let $\alpha \in J^{(2)}$. Then α has a square root in $\mathcal{T}(X)$ if and only if either* (i) *α is idempotent or* (ii) *cont $\alpha = 2$ and ran α is contained in an $(\alpha \circ \alpha^{-1})$-class containing at least 3 elements.*

Proof. If cont $\alpha = 1$ we may write

$$\alpha = \begin{pmatrix} A_1 & A_2 \\ a_{1\mu} & a_{2\mu} \end{pmatrix},$$

where μ is a permutation of $\{1, 2\}$ and where $a_1 \in A_1$, $a_2 \in A_2$. If α is to be quasi-square then μ must be the identical permutation and so

$$\alpha = \begin{pmatrix} A_1 & A_2 \\ a_1 & a_2 \end{pmatrix},$$

an idempotent. It is now obvious that if $\alpha \in J^{(2)}$ and cont $\alpha = 1$ then α has a square root if and only if it is idempotent.

Now suppose that cont $\alpha = 2$; this is the only other possibility since $X\alpha \supset X\alpha^2$ implies $|X\alpha^2| = 1$ and no further descent is possible. Writing

$$\alpha = \begin{pmatrix} A_1 & A_2 \\ x_1 & x_2 \end{pmatrix},$$

with $x_1, x_2 \in A_1$, we suppose that $|A_1| \geqslant 3$. Choose y in $A_1 \setminus \{x_1, x_2\}$ and let

$$\beta = \begin{pmatrix} A_1 \setminus \{y\}, & y & A_2 \\ x_1, & x_2, & y \end{pmatrix};$$

then $\beta^2 = \alpha$.

Conversely, suppose that cont $\alpha = 2$ and that

$$\alpha = \begin{pmatrix} A_1 & A_2 \\ x_1 & x_2 \end{pmatrix} \text{ (with } x_1, x_2 \text{ in } A_1)$$

has a square root β. Let $z \in A_2$ and let $z\beta = y$. Then

$$y\beta = z\alpha = x_2.$$

If $y \in A_2$ then $y\alpha = x_2$ and so

$$x_2 = y\alpha = y\beta^2 = x_2\beta.$$

But then

$$x_1 = x_2\alpha = x_2\beta^2 = x_2\beta = x_2,$$

which is a contradiction. Hence $y \in A_1$.

If $y = x_1$ then $x_1\beta = x_2$; hence

$$x_2\beta = x_1\beta^2 = x_1\alpha = x_1$$

and so

$$x_2 = x_1\beta = x_2\beta^2 = x_2\alpha = x_1,$$

again a contradiction. Hence $y \neq x_1$. If $y = x_2$ we have $x_2\beta = x_2$, which as we saw in the last paragraph leads to a contradiction. Hence $y \neq x_2$ and so there must exist y in A_1 distinct from both x_1 and x_2. Thus $|A_1| \geq 3$ as required.

4. Duals; amenable elements.   The results of Section 3 make it clear that Theorem 3 will not extend to elements α for which cont $\alpha \geq 2$. For example, if $X = \{1, 2, 3\}$ and

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix},$$

then α is certainly quasi-square but by Theorem 4 cannot have a square root. Some further concepts are now required.

If $\alpha \in \mathcal{T}(X)$ then for each x in X we have a sequence

$$x, x\alpha, x\alpha^2, \ldots$$

of elements of X, and since X is finite these elements cannot all be distinct. If r is the least element of the non-empty set

$$\{w \in \mathbb{N} \cup \{0\} : (\exists z > w)x\alpha^w = x\alpha^z\}$$

we call r the *index* of x relative to α and write either $r = i_\alpha(x)$ or (where no confusion will arise) $r = i(x)$. Notice that $i(x) \geq 1$ unless $x \in \operatorname{stran} \alpha$ and that in all cases $x\alpha^{i(x)} \in \operatorname{stran} \alpha$. If q is the least element of the non-empty set

$$\{z \in \mathbb{N} : x\alpha^{i(x)} = x\alpha^{i(x)+z}\},$$

we call q the *period* of x relative to α and write either $q = p_\alpha(x)$ or $q = p(x)$. It is always the case that $p(x) \geq 1$.

In attempting to find necessary and sufficient conditions for an element α of $\mathcal{T}(X)$ to have a square root we are led to consider what we shall call a 'γ-dual' of an element x in $X \setminus \operatorname{ran} \alpha$. Because of Theorem 2 we may confine attention to quasi-square elements; i.e. we may suppose that $\alpha \,|\, \operatorname{stran} \alpha$ is a permutation of $\operatorname{stran} \alpha$ having square root γ. Now define y to be a γ-*dual* of x if $y \in X \setminus \operatorname{ran} \alpha$ and one of the following four conditions is satisfied:

(D1) $i(y) = i(x)$ and $(x\alpha^{i(x)})\gamma = y\alpha^{i(y)}$;

(D2) $i(y) = i(x)$ and $x\alpha^{i(x)} = (y\alpha^{i(y)})\gamma$;

(D3) $i(y) = i(x) + 1$ and $(x\alpha^{i(x)})\gamma = y\alpha^{i(y)}$;

(D4) $i(y) = i(x) - 1$ and $x\alpha^{i(x)} = (y\alpha^{i(y)})\gamma$.

If it is necessary to specify more exactly the relationship of y to x we shall say (for example) that 'y is a γ-dual of x under rule (D1)'. It is easy to see that if y is a γ-dual of x then x is a γ-dual of y.

We define an $(\alpha \circ \alpha^{-1})$-class A in X to be *basic* if $A \cap \operatorname{ran} \alpha = \varnothing$, and we say that $x \in X$ is a *basic element* if it belongs to a basic $(\alpha \circ \alpha^{-1})$-class, i.e. if $x(\alpha \circ \alpha^{-1}) \cap \operatorname{ran} \alpha = \varnothing$.

We say that α is *amenable* if it is quasi-square and if there exists a square root γ of the permutation $\alpha \,|\,\mathrm{stran}\,\alpha$ such that every basic element of X has a γ-dual. Then we have

THEOREM 6. *Let $\alpha \in \mathcal{T}(X)$. If α has a square root in $\mathcal{T}(X)$ then α is amenable.*

Proof. Let $\alpha \in \mathcal{T}(X)$ and suppose that α has a square root β. Let x be a basic element of X. Then $i(x) \geqslant 2$, since $i(x) \leqslant 1$ would imply that there exists $m \geqslant 1$ such that $x\alpha = x\alpha^{m+1}$. This would give $x\alpha^m \in x(\alpha \circ \alpha^{-1})$, in contradiction to the definition of a basic element.

By the definition of index and period we have

$$x\alpha^{i(x)} = x\alpha^{i(x)+p(x)}$$

and

$$(\forall m \in \mathbb{N}) \ x\alpha^{i(x)-1} \neq x\alpha^{i(x)-1+m}.$$

Hence

$$x\beta^{2i(x)} = x\beta^{2i(x)+2p(x)}$$

and

$$(\forall m \in \mathbb{N}) \ x\beta^{2i(x)-2} \neq x\beta^{2i(x)-2+2m}.$$

Rewriting these slightly, we get

$$(x\beta)\beta^{2i(x)-1} = (x\beta)\beta^{2i(x)-1+2p(x)}$$

and

$$(\forall m \in \mathbb{N}) \ (x\beta)\beta^{2i(x)-3} \neq (x\beta)\beta^{2i(x)-3+2m}.$$

It follows that

$$(x\beta)\beta^{2i(x)} = (x\beta)\beta^{2i(x)+2p(x)}$$

and

$$(\forall m \in \mathbb{N}) \ (x\beta)\beta^{2i(x)-4} \neq (x\beta)\beta^{2i(x)-4+2m},$$

i.e. that

$$(x\beta)\alpha^{i(x)} = (x\beta)\alpha^{i(x)+p(x)} \tag{A}$$

and

$$(\forall m \in \mathbb{N}) \ (x\beta)\alpha^{i(x)-2} \neq (x\beta)\alpha^{i(x)-2+2m}. \tag{B}$$

From (A) it follows that $i_\alpha(x\beta) \leqslant i(x)$ and from (B) it follows that $i_\alpha(x\beta) > i(x) - 2$. Thus either $i(x\beta) = i(x)$ or $i(x\beta) = i(x) - 1$.

We now find it convenient to consider four cases as follows:
(1) $x\beta \notin \mathrm{ran}\,\alpha$, $i(x\beta) = i(x) - 1$;
(2) $x\beta \notin \mathrm{ran}\,\alpha$, $i(x\beta) = i(x)$;
(3) $x\beta \in \mathrm{ran}\,\alpha$, $i(x\beta) = i(x) - 1$;
(4) $x\beta \in \mathrm{ran}\,\alpha$, $i(x\beta) = i(x)$.

Let $\gamma = \beta \,|\, \text{stran } \alpha$; by Lemma 1, γ is a permutation of stran α and $\gamma^2 = \alpha \,|\, \text{stran } \alpha$. Since in case (1) we have

$$i(x\beta) = i(x) - 1 \quad \text{and} \quad x\alpha^{i(x)} = [(x\beta)\alpha^{i(x)-1}]\gamma,$$

the element $x\beta$ is a γ-dual for x under rule (D4). Similarly in case (2) the element $x\beta$ is a γ-dual for x under rule (D1).

The element $x\beta$ cannot be a γ-dual in cases (3) and (4), since one of the requirements for a γ-dual is that it belong to $X \backslash \text{ran } \alpha$. In both these cases, however, there exists an element x_1 in X such that $x_1\alpha = x\beta$. Then $x_1 \notin \text{ran } \alpha$, since if we had $x_1 = t\alpha (t \in X)$ it would follow that

$$x\alpha = x\beta^2 = x_1\alpha\beta = t\alpha^2\beta = (t\beta\alpha)\alpha;$$

hence

$$t\beta\alpha \in x(\alpha \circ \alpha^{-1}) \cap \text{ran } \alpha,$$

in contradiction to the hypothesis that x is a basic element.

Notice next that

$$x_1\alpha^{i(x\beta)+1} = (x\beta)\alpha^{i(x\beta)} = (x\beta)\alpha^{i(x\beta)+p(x\beta)}.$$
$$= x_1\alpha^{i(x\beta)+1+p(x\beta)},$$

so that $i(x_1) \le i(x\beta) + 1$. This is in fact an equality, since if

$$x_1\alpha^r = x_1\alpha^{r+m} \qquad (m > 0)$$

then $r \ge 1$ and so

$$(x\beta)\alpha^{r-1} = (x\beta)\alpha^{r-1+m}.$$

By the definition of $i(x\beta)$ it then follows that $r - 1 \ge i(x\beta)$. Hence $r \ge i(x\beta) + 1$ and it is now clear that

$$i(x_1) = i(x\beta) + 1.$$

In case (3) we now have

$$i(x_1) = i(x) \quad \text{and} \quad x\alpha^{i(x)} = (x_1\alpha^{i(x)})\gamma,$$

so that x_1 is a γ-dual of x under rule (D2). Similarly in case (4) we find that x_1 is a γ-dual of x under rule (D3). Thus α is amenable.

5. Compatibly amenable elements. The refined necessary condition for the existence of a square root given by Theorem 6 is unfortunately still not sufficient. We shall eventually give an example, but this will be easier to explain if we defer it until we have introduced some further concepts. Let us begin by noticing that in checking for amenability we do not need to check every basic element, for if x and x' are basic elements in the same basic $(\alpha \circ \alpha^{-1})$-class then $x\alpha = x'\alpha$; hence $i(x) = i(x')$ (≥ 2) and any element y of $X \backslash \text{ran } \alpha$ that is a γ-dual for x is also a γ-dual for x'. It is thus sufficient to check that γ-duals exist for the elements in a cross-section of the basic $(\alpha \circ \alpha^{-1})$-classes.

Suppose now that α is an amenable element of $\mathcal{T}(X)$, and choose a cross-section Bas α of the basic $(\alpha \circ \alpha^{-1})$-classes. We can express the amenability of α by saying that for some square root γ of the permutation $\alpha \mid \text{stran}\ \alpha$ there is a mapping $\Delta : \text{Bas}\ \alpha \to X \backslash \text{ran}\ \alpha$ associating each x in Bas α with a γ-dual $x\Delta$ in $X \backslash \text{ran}\ \alpha$. We shall refer to Δ as a *dualizar mapping*. If $(y, z) \in \Delta$ (i.e. if $y \in \text{Bas}\ \alpha$ and $z = y\Delta$) define

$$(y, z)^{(1)} = \{(y, z), (z, y\alpha), (y\alpha, z\alpha), (z\alpha, y\alpha^2), \ldots\},$$

$$(y, z)^{(2)} = \{(z, y), (y, z\alpha), (z\alpha, y\alpha), (y\alpha, z\alpha^2), \ldots\}.$$

Both these sets are in fact finite, with size dependent on the index and period of y and z. For each subset A of Δ we define

$$\Delta_A = \bigcup_{(y, z) \in A} (y, z)^{(1)} \cup \bigcup_{(y, z) \in \Delta \backslash A} (y, z)^{(2)},$$

and we say that Δ is a *compatible* dualizer mapping if for some $A \subseteq \Delta$ the relation Δ_A is a partial mapping, i.e. if Δ_A satisfies

$$(v, w) \in \Delta_A \quad \text{and} \quad (v, w') \in \Delta_A \Rightarrow w = w'.$$

We say that an element α of $\mathcal{T}(X)$ is *compatibly amenable* if it is amenable and if there exists a compatible dualizer mapping.

Before describing an example of an amenable element that is not compatibly amenable, we establish two fairly easy properties of compatible dualizer mappings.

LEMMA 2. *If* $\Delta : \text{Bas}\ \alpha \to X \backslash \text{ran}\ \alpha$ *is a compatible dualizer mapping, then* Δ *is one-one*.

Proof. Suppose that $(x, z), (y, z) \in \Delta$, where $x, y \in \text{Bas}\ \alpha$. Since Δ is compatible, there exists $A \subseteq \Delta$ for which Δ_A is a partial mapping. On the face of it there are four possibilities:

(i) $(x, z) \in A$, $(y, z) \in A$;
(ii) $(x, z) \in A$, $(y, z) \in \Delta \backslash A$;
(iii) $(x, z) \in \Delta \backslash A$, $(y, z) \in A$;
(iv) $(x, z) \in \Delta \backslash A$, $(y, z) \in \Delta \backslash A$.

In case (i) we have, by definition of Δ_A,

$$(z, x\alpha), (z, y\alpha) \in \Delta_A.$$

Hence, by the partial mapping property, $x\alpha = y\alpha$; hence, since x, y are members of a cross-section of $(\alpha \circ \alpha^{-1})$-classes, $x = y$.

Case (ii) cannot arise, since we have $(x, z), (z, y) \in \Delta_A$ and hence $y = x\alpha \in \text{ran}\ \alpha$, a contradiction. A similar argument shows that case (iii) is impossible. In case (iv) we have $(z, x), (z, y) \in \Delta_A$ and so $x = y$.

LEMMA 3. *Suppose that* x_1, x_2, y_1, y_2 *are distinct elements of* Bas α *such that each of* y_1, y_2 *is a γ-dual for each of* x_1, x_2. *If the γ-dualizer mapping* Δ *contains the pairs* (x_1, y_1), (x_2, y_2), (y_1, x_2), (y_2, x_1), *then it is not compatible.*

Proof. Suppose by way of contradiction that Δ is compatible, i.e. that there exists $A \subseteq \Delta$ for which Δ_A is a partial mapping. Suppose first that $(x_1, y_1) \in A$. Then $(x_1, y_1) \in \Delta_A$ and so $(y_2, x_1) \in A$ (since otherwise $(x_1, y_2) \in \Delta_A$ in contradiction to the partial mapping property). Hence $(x_1, y_2\alpha) \in \Delta_A$ and so $y_1 = y_2\alpha$. This is a contradiction since $y_1 \in \text{Bas } \alpha \subseteq X \setminus \text{ran } \alpha$.

Hence $(x_1, y_1) \notin A$ and so $(y_1, x_1) \in \Delta_A$. But this implies $(y_1, x_2) \notin A$ (since otherwise $(y_1, x_2) \in \Delta_A$ and the partial mapping condition is violated). Hence $(y_1, x_2\alpha) \in \Delta_A$ and so $x_1 = x_2\alpha$, again a contradiction, since $x_1 \in \text{Bas } \alpha$. This completes the proof.

EXAMPLE. Let $X = \{1, \ldots, 13\}$ and let

$$\alpha = \begin{pmatrix} \{1,2\}, & \{3,4\}, & \{5,6\}, & \{7,8\}, & 9, & 10, & 11, & 12, & 13 \\ 5, & 1, & 3, & 2, & 7, & 8, & 4, & 6, & 11 \end{pmatrix}$$

Here $\text{stran } \alpha = X\alpha^3 = \{1, 3, 5\}$ and $\alpha \,|\, \text{stran } \alpha = (153)$, a cycle of length 3. This has the unique square root $\gamma = (135)$ and so α is quasi-square. The basic $(\alpha \circ \alpha^{-1})$-classes are

$$\{9\}, \{10\}, \{12\}, \{13\}$$

and so the only possible choice for $\text{Bas } \alpha$ is $\{9, 10, 12, 13\}$. Notice that in this case we have $\text{Bas } \alpha = X \setminus \text{ran } \alpha$.

About the basic elements we summarise the relevant information in a table:

x	$i(x)$	$x\alpha^{i(x)}$	$(x\alpha^{i(x)})\gamma$
9	3	5	1
10	3	5	1
12	2	3	5
13	3	1	3

Possible γ-duals of 9 are 12 (rule (D4)) and 13 (rule (D1)); possible γ-duals of 10 are 12 (rule (D4)) and 13 (rule (D2)). Hence, bearing in mind the restrictions imposed by Lemmas 2 and 3, we see that the only possible compatible dualizer mappings are

$$\Delta^{(1)} = \{(9, 12), (10, 13), (13, 10), (12, 9)\},$$

$$\Delta^{(2)} = \{(9, 13), (10, 12), (12, 10), (13, 9)\}.$$

For brevity let us now write

$$K = \{(2, 1), (1, 5), (5, 5), (5, 3), (3, 3), (3, 1), (1, 1)\}.$$

Routine calculation show that

$$(9, 12)^{(1)} = \{(9, 12), (12, 7), (7, 6), (6, 2), (2, 3), (3, 5), (5, 1), (1, 3)\},$$
$$(9, 12)^{(2)} = \{(12, 9), (9, 6), (6, 7), (7, 3), (3, 2)\} \cup K,$$
$$(9, 13)^{(1)} = \{(9, 13), (13, 7), (7, 11), (11, 2), (2, 4), (4, 5), (5, 1), (1, 3), (3, 5)\},$$
$$(9, 13)^{(2)} = \{(13, 9), (9, 11), (11, 7), (7, 4), (4, 2)\} \cup K,$$
$$(10, 12)^{(1)} = \{(10, 12), (12, 8), (8, 6), (6, 2), (2, 3), (3, 5), (5, 1), (1, 3)\},$$
$$(10, 12)^{(2)} = \{(12, 10), (10, 6), (6, 8), (8, 3), (3, 2)\} \cup K,$$
$$(10, 13)^{(1)} = \{(10, 13), (13, 8), (8, 11), (11, 2), (2, 4), (4, 5), (5, 1), (1, 3), (3, 5)\},$$
$$(10, 13)^{(2)} = \{(13, 10), (10, 11), (11, 8), (8, 4), (4, 2)\} \cup K.$$

Hence, since $(9, 12)^{(2)}(=(12, 9)^{(1)})$, $(9, 13)^{(2)}$, $(10, 12)^{(2)}$ and $(10, 13)^{(2)}$ all lack the partial mapping property, the only possible choice for $A \subseteq \Delta^{(1)}$ giving a partial mapping $\Delta_A^{(1)}$ is

$$A = \{(9, 12), (10, 13)\}.$$

But even this does not work, since examination of $(9, 12)^{(1)}$ and $(10, 13)^{(1)}$ shows that $(2, 3), (2, 4) \in \Delta_A^{(1)}$. Thus $\Delta^{(1)}$ is not a compatible dualizer mapping.

Similarly, for $\Delta^{(2)}$ the only subset A that has any chance of providing a partial mapping $\Delta_A^{(2)}$ is

$$A = \{(9, 13), (10, 12)\},$$

and this fails since $(2, 3), (2, 4) \in \Delta_A^{(2)}$. We conclude that α is amenable but not compatibly amenable.

Hence α has no square root, by virtue of our final theorem:

THEOREM 7. *Let X be a finite set and let α be an element of the full transformation semigroup $\mathcal{T}(X)$. Then α has a square root in $\mathcal{T}(X)$ if and only if it is compatibly amenable.*

Proof. Suppose first that α has a square root β. Then α is amenable, by Theorem 6. Recalling the method of proof of that theorem, we return to the four cases there considered. Effectively we divided Bas α into four disjoint subsets $A_1, \ldots, A_4$:

$$A_1 = \{x \in \text{Bas } \alpha : x\beta \notin \text{ran } \alpha, \ i(x\beta) = i(x) - 1\},$$
$$A_2 = \{x \in \text{Bas } \alpha : x\beta \notin \text{ran } \alpha, \ i(x\beta) = i(x)\},$$
$$A_3 = \{x \in \text{Bas } \alpha : x\beta \in \text{ran } \alpha, \ i(x\beta) = i(x) - 1\},$$
$$A_4 = \{x \in \text{Bas } \alpha : x\beta \in \text{ran } \alpha, \ i(x\beta) = i(x)\}.$$

We defined γ as $\beta \mid \text{stran } \alpha$ and chose $x\beta$ as γ-dual of x if $x \in A_1 \cup A_2$. If $x \in A_3 \cup A_4$ we introduced a new element x_1 such that $x_1\alpha = x\beta$ and took x_1 as γ-dual of x. We do not change this latter procedure, but in order to ensure that our dualizer mapping Δ is compatible we need to be a little more careful in choosing the γ-dual of an element of $A_1 \cup A_2$. It may be that $x\beta \notin \text{Bas } \alpha$ but that there exists an element z in $(x\beta)(\beta \circ \beta^{-1}) \cap \text{Bas } \alpha$. There certainly will not exist more than one such z, since two distinct elements of Bas α cannot be $(\alpha \circ \alpha^{-1})$-equivalent. But if there does exist such a z we choose it rather than $x\beta$ to be the γ-dual of x. Since $(x\beta)\beta^m = z\beta^m$ for all $m \geq 1$ it certainly serves as well. If

$$(x\beta)(\beta \circ \beta^{-1}) \cap \text{Bas } \alpha = \varnothing$$

we choose γ-dual $x\beta$ as before. Notice that for all x in $A_1 \cup A_2$ and for all $m \geq 1$ we have

$$(x\Delta)\alpha^m = x\beta\alpha^m = x\alpha^m\beta;$$

also,

$$(x\Delta)\beta = x\alpha.$$

Now let $A = \{(x, x\Delta) : x \in A_1 \cup A_2\}$, so that

$$\Delta_A = \bigcup_{x \in A_1 \cup A_2} (x, x\Delta)^{(1)} \cup \bigcup_{x \in A_3 \cup A_4} (x, x_1)^{(2)}.$$

We show that Δ_A is a partial mapping.

For each y in $A_1 \cup A_2$,

$$(y, y\Delta)^{(1)} = \{(y, y\Delta), (y\Delta, y\alpha), (y\alpha, y\alpha\beta), (y\alpha\beta, y\alpha^2), \ldots, (y\alpha^l, y\alpha^l\beta), \ldots\},$$

and for each z in $A_3 \cup A_4$,

$$(z, z_1)^{(2)} = \{(z_1, z), (z, z\beta), (z\beta, z\alpha), (z\alpha, z\alpha\beta), \ldots, (z\alpha^l, z\alpha^l\beta), \ldots\}.$$

Thus for the most part the relation Δ_A coincides with the function β. The only exceptions are some elements y in $A_1 \cup A_2$, and elements z_1 ($z \in A_3 \cup A_4$). If $y \in A_1 \cup A_2$ and $(y\beta)(\beta \circ \beta^{-1}) \cap \operatorname{Bas} \alpha \neq \varnothing$ then $y\Delta \in A_3 \cup A_4$. Thus

$$(y\Delta, y\alpha) \in (y, y\Delta)^{(1)} \subseteq \Delta_A$$

and

$$(y\Delta, (y\Delta)\beta) \in (y\Delta, (y\Delta)_1)^{(2)} \subseteq \Delta_A.$$

Since $(y\Delta)\beta = y\alpha$ this does not destroy the partial mapping property of Δ_A.

If $z \in A_3 \cup A_4$ we may have $z_1 \in A_1 \cup A_2$. But in that case the set $(z_1\beta)(\beta \circ \beta^{-1}) \cap \operatorname{Bas} \alpha$ contains the (necessarily unique) element z and so the pair $(z_1, z_1\Delta)$ in $(z_1, z_1\Delta)^{(1)}$ coincides with the pair (z_1, z) in $(z, z_1)^{(2)}$. We conclude that Δ_A is a partial mapping and thus that α is compatibly amenable.

Now suppose that α is compatibly amenable, with γ as square root of $\alpha \,|\, \operatorname{stran} \alpha$, with $\operatorname{Bas} \alpha$ as the chosen cross-section of the basic $(\alpha \circ \alpha^{-1})$-classes, with Δ as compatible dualizer mapping and with subset A of Δ such that Δ_A is a partial mapping. We find it convenient to partition X into three disjoint subsets, P, Q, R as follows:

$$P = \bigcup_{r=0}^{\infty} [\operatorname{Bas} \alpha \cup (\operatorname{Bas} \alpha)\Delta]\alpha^r,$$

$$Q = \operatorname{stran} \alpha \setminus (P \cap \operatorname{stran} \alpha),$$

$$R = X \setminus (P \cup Q).$$

Notice that if $x \in \operatorname{ran} \alpha \setminus \operatorname{stran} \alpha$ then $x \in P$; for either $x \in (\operatorname{Bas} \alpha)\alpha$ or there exists $x_1 \in \operatorname{ran} \alpha$ such that $x_1\alpha = x$; then either $x_1 \in (\operatorname{Bas} \alpha)\alpha$, giving $x \in (\operatorname{Bas} \alpha)\alpha^2$, or there exists $x_2 \in \operatorname{ran} \alpha$ such that $x_2\alpha = x$; and so on. Thus $\operatorname{ran} \alpha \subseteq P \cup Q$ and so R consists of those elements in $X \setminus \operatorname{ran} \alpha$ not in $\operatorname{Bas} \alpha \cup (\operatorname{Bas} \alpha)\Delta$. If $x \in R$ then either

$$x(\alpha \circ \alpha^{-1}) \cap \operatorname{Bas} \alpha \neq \varnothing$$

(which happens if $x(\alpha \circ \alpha^{-1})$ is a basic $(\alpha \circ \alpha^{-1})$-class) or $x(\alpha \circ \alpha^{-1})$ intersects with $\operatorname{ran} \alpha$. Thus either $x(\alpha \circ \alpha^{-1}) \cap P \neq \varnothing$ or $x(\alpha \circ \alpha^{-1}) \cap Q \neq \varnothing$.

From the definitions of P and Δ_A it is clear that $\operatorname{dom} \Delta_A = P$. We now define a mapping $\beta : X \to X$ as follows: if $x \in P$ let $x\beta = x\Delta_A$; if $x \in Q$ let $x\beta = x\gamma$. If $x \in R$ then either (i) $x(\alpha \circ \alpha^{-1}) \cap P \neq \varnothing$ in which case we choose y in $x(\alpha \circ \alpha^{-1}) \cap P$, or (ii) $x(\alpha \circ \alpha^{-1}) \cap P = \varnothing$ and $x(\alpha \circ \alpha^{-1}) \cap Q \neq \varnothing$, in which case we choose y in $x(\alpha \circ \alpha^{-1}) \cap Q$. In either case $y\beta$ is already defined and we define $x\beta = y\beta$.

We show that $\beta^2 = \alpha$. Let $x \in P$. Then the definition of Δ_A makes it clear that

$x\Delta_A \in P$, and so $x\beta^2 = x\Delta_A^2$. But the construction of Δ_A entails that $x\Delta_A^2 = x\alpha$ for all x in $P = \mathrm{dom}\,\Delta_A$.

Now let $x \in Q$, so that $x\beta = x\gamma$. Then $x\gamma \in \mathrm{stran}\,\alpha$. We shall show that $x\gamma \in Q$. For suppose by way of contradiction, that $x\gamma \in P$. Then there exists z in $\mathrm{Bas}\,\alpha \cup (\mathrm{Bas}\,\alpha)\Delta$ such that $z\alpha^r = x\gamma$. Since $z\alpha^r \in \mathrm{stran}\,\alpha$ we must have $r \geq i(z)$ and so

$$x\alpha = (z\alpha^r)\gamma = (z\alpha^{i(z)+r-i(z)})\gamma$$
$$= z\alpha^{i(z)}\gamma\alpha^{r-i(z)}.$$

Now the element z has a dual $z\Delta$, and $(z\alpha^{i(z)})\gamma$ is equal either to $(z\Delta)\alpha^{i(z\Delta)}$ (rule (D1) or (D3)) or to $(z\Delta)\alpha^{i(z\Delta)+1}$ (rule (D2) or (D4)). Hence either

$$x\alpha = (z\Delta)^{i(z\Delta)+r-iz} \qquad \text{or} \qquad x\alpha = (z\Delta)^{i(z\Delta)+r-i(z)+1},$$

and in either case $x\alpha \in P$. Hence $x\alpha^t \in P$ for $t = 1, 2, \ldots$. But since $x \in \mathrm{stran}\,\alpha$ we have that $x\alpha^t = x$ for some $t \geq 1$. Hence $x \in P$, contrary to assumption. We conclude that $x\gamma \in Q$, and it is now obvious that

$$x\beta^2 = x\gamma^2 = x\alpha.$$

Finally, suppose that $x \in R$. Then $x\beta = y\beta$ where $y \in P \cup Q$ and $y\alpha = x\alpha$. Hence

$$x\beta^2 = y\beta^2 = y\alpha = x\alpha$$

in this case also. This completes the proof of Theorem 7.

REMARK. The criterion we have established for the existence of a square root is disappointingly complicated, but for small sets X is not too hard to apply. Moreover, as the proof makes clear, the permutation γ and the partial mapping Δ_A do actually in effect construct the square root.

If one visualises elements of $\mathscr{T}(X)$ as directed graphs it is possible to view the problem as one of finding square roots (in a natural sense) for a certain kind of digraph. The only reference we have found on this topic [1] (for which we are indebted to Dr Ian Anderson) does not seem to be very helpful in our algebraic context.

REFERENCES

1. Dennis P. Geller, The square root of a digraph, *J. Combin. Theory* **5** (1968) 320–321.
2. J. M. Howie, *An introduction to semigroup theory* (Academic Press, 1976).
3. R. Isaacs, Iterates of fractional order, *Canad. J. Math.* **2** (1950) 409–416.
4. Mary Snowden, *Square roots in full transformation semigroups*, M.Sc. thesis, University of St Andrews (1979).

FOUR PEAKS
CLAYTON ROAD
MOLD, CLWYD
WALES

MATHEMATICAL INSTITUTE
UNIVERSITY OF ST ANDREWS