STOCHASTICA, Vol. III, nº 2 (1979)

ITERATIVE SQUARE ROOTS OF ČEBYŠEV POLYNOMIALS

by

R. E. Rice

1. Introduction.

The sequence of Čebyšev polynomials, $\{T_n\}$, defined on the interval $[-1,1]$, satisfies the well known identity

$$T_n \circ T_m = T_{nm} \quad \text{for all } n,m \geqslant 0. \tag{1.1}$$

Taking n equal to m in (1.1) we see that T_{n^2} possesses an iterative square root. In general, a function mapping a set S into itself is said to have an <u>iterative square root (root of order 2)</u> if it can be expressed in the form h o h, where h, too, is a function from S into itself. Our principal result is the following .

Main Theorem. For T_n to possess an iterative square root it is both necessary and sufficient that $n \equiv 0$ or 1 (mod 4).

Any function conjugate to a function which has an iterative square root also has one [5]. Thus, in the Main Theorem, "T_n" could be replaced by "a function conjugate to T_n". Further results on iterative roots of Čebyšev polynomials may be found in [4], [8], and [9]. A general discussion of the Čebyšev polynomials may be found in [6].

The proof of the main theorem makes use of methods developed by R. Isaacs [2] and requires knowledge of the orbit structure of the function T_n. This is discussed in the next section.

The third section is devoted to a classification of the orbits of T_n, and the fourth to the proof of the Main Theorem. In the fifth section we mention extensions of the Main Theorem to further classes of functions.

2. Basic Definitions and Isaacs' Results.

For any function g we define g^0 to be the identity function with domain Dom $g \cup$ Ran g. For $n \geq 1$, g^n is defined recursively by $g^n = g \circ g^{n-1}$. It is possible that, for some n, g^n will be the empty function.

The function g can be represented graphically as shown in Figure 1. Here the nodes represent the elements of Dom g $\cup$ Ran g, and the arrows link $x \in$ Dom g to g(x). The set of nodes in a connected component of this graph is called a g-<u>orbit</u>.

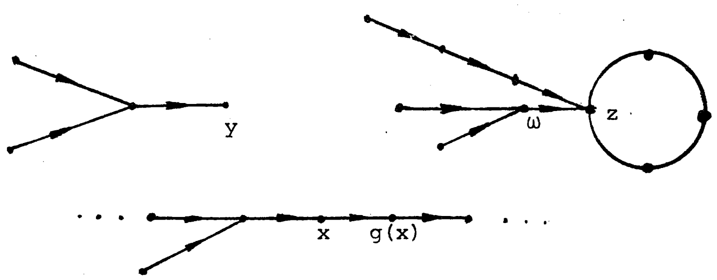


Figure 1

Moving clockwise from the upper left orbit in Figure 1 we have a <u>terminating</u>, a <u>cyclic</u> and an <u>acyclic</u> orbit. A terminating orbit is characterized by the existence of an element x in Ran g which is not in Dom g. A cyclic orbit has an element x such that for some $n \geq 1$, $g^n(x) = x$. Here, if n is minimal, the orbit is n-<u>cyclic</u> (<u>cyclic</u> of <u>order</u> n) with <u>cycle</u> $\{x, g(x), \ldots, g^{n-1}(x)\}$. Clearly a cyclic orbit has exactly one cycle, the one illustrated having a 3-cycle. All other orbits are acyclic.

Let x,y be in Dom g^0. Then x is an ancestor of y if for some $n \geqslant 1$, $g^n(x) = y$, and x is a preimage if g(x)=y. If an element z in the cycle of a cyclic orbit has a preimage w which is not in the cycle, then w is called a leader (*); and w, together with all of its ancestors determines a branch from z. Any union of brances from z is called a branch cluster from z.

Two g-orbits H and L are said to be mateable if the restriction of g to $H \cup L$ has a root of order 2 for which $H \cup L$ is an orbit. L is said to be self-mateable if the restriction of g to L has a root of order 2. Theorems 1, 2 and 3 are due to R. Isaacs.

Theorem 1. Let h be a function such that Ran $h \subseteq$ Dom h. Then h has a root of order 2 if and only if the set of h-orbits can be partitioned into disjoint sets A, B, C, such that:

(i) There is a 1-1 correspondence between the elements of A and the elements of B.

(ii) If $L \in A$ corresponds to $H \in B$ then L and H are mateable.

(iii) Each $L \in C$ is self-mateable.

A contraction equivalence (on g) is an equivalence relation, $\sim$, defined on Dom g^0 such that for all a,b in Dom g^0, if $a \sim b$, then either i) a and b both belong to Ran g - Dom g, or ii) a and b belong to Dom g with g(a) = g(b). The function $\tilde{g}$ defined by

$$\tilde{g} = \{([a]_\sim, [g(a)]_\sim) \mid a \in \text{Dom } g\} \tag{2.1}$$

is called a contraction of g. $\tilde{g}$ is defined on the set of equivalence classes of $\sim$. A curtailment of g is the restriction of g to a set $A \in$ Dom g such that if $x \in$ Dom g - A then $x \notin$ Ran g.

(*) The terms leader, branch, branch-cluster, mateable, and self-mateable appear in Isaacs [2] .

The functions f and g are <u>isomorphic</u> (or <u>conjugate</u>), and we write $f \approx g$, if there is a bijection, ω, from Dom f^0 onto Dom g^0 such that for all $x \in$ Dom f^0

(i) $x \in$ Dom f if and only if $\omega(x) \in$ Dom g, (2.2)

and

(ii) if $x \in$ Dom f then $\omega(f(x)) = g(\omega(x))$.

Note that since g-orbits, branches, and branch clusters of g-orbits may be identified with the restrictions of g to these sets, we may speak of contractions curtailments and isomorphisms of these objects.

<u>Theorem 2.</u> Two distinct orbits H and L are mateable if and only if a contraction of one is isomorphic to a curtailment of the other.

Note that two distinct isomorphic orbits can always be mated. A necessary condition for two orbits to be mateable is that they either both be acyclic or both be cyclic with equal orders.

<u>Theorem 3.</u> A necessary and sufficient condition for an h-orbit, L, to be self mateable is that:

(i) L is m-cyclic with m odd, say $m = 2k + 1$.
(ii) The elements of $L \setminus L^c$ are disjointedly the union of two collections of sets $\{B_\alpha\}$, $\{\bar{B}_\alpha\}$ indexed by some set A such that, for each $\alpha \in A$, B_α is a branch, and either $\bar{B}$ is a branch cluster or $\bar{B}_\alpha = \emptyset$. A curtailment of B_α is isomorphic to a contraction of $\bar{B}_\alpha$. If B_α is from z then, if $\bar{B}_\alpha \neq \emptyset$, $\bar{B}_\alpha$ is from $h^k(z)$.

3. Classification of the Orbits of Čebyšev Polynomials.

The sequence of Čebyšev polynomials, $\{T_n\}$, defined on $[-1,1]$ are the functions defined recursively via

$$T_0(x) = 1, \tag{3.1}$$

$$T_1(x) = x,$$

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \quad \text{for all} \quad x \in [-1,1].$$

We have the well known identity:

$$T_n(x) = \cos(n \arccos(x)).$$

For $n \geq 0$, T_n is a polynomial of degree n. When $n \geq 2$, T_n attains all n - 1 possible local maxima and minima within the interval $(-1,1)$. All local minimum values are -1, and all local maximum values are 1.

We next list some well known, and some easily verified properties of the set of Čebyšev polynomials [6]. For any set A, #A denotes the number of elements in A.

<u>Lemma 1.</u> Let $m,n \geq 1$. Then:

(a) $T_m \circ T_n = T_{mn}$,

(b) T_n maps $[-1,1]$ onto itself,

(c) If $x \in (-1,1)$ then $\#T_n^{-1}(\{x\}) = n$,

(d) $T_n(1) = 1$.

If in addition, $n \geq 2$ then:

(e) T_n has exactly n fixed points in the interval $[-1,1]$.

If furthermore n is even, then:

(f) $T_n(-1) = 1$,

(g) $\#T_n^{-1}(\{1\}) = n/2 + 1$,

(h) $T_n^{-1}(\{-1\}) = n/2$.

If on the other hand n is odd, then:

(i) $T_n(-1) = -1$,

(j) $\#T_n^{-1}(\{1\}) = (n+1)/2$,

(k) $\#T_n^{-1}(\{-1\}) = (n+1)/2$.

Lemma 1 provides the necessary information to determine the orbit structure of T_n for all $n \geqslant 2$. These orbits fall into two major classes which we label with the Roman numerals I and II. Within these classes we use "even" and "odd" as superscripts to distinguish between orbits associated with polynomials of even and odd degree respectively.

Any point $x \in (-1,1)$ which is not in a cycle of some T_n-orbit has exactly n preimages, each of which is in $(-1,1)$ and clearly not in a cycle of T_n. Each of these n preimages, in turn, has exactly n preimages, each of which ..., etc.

Accordingly, we let the symbol $\ast\!\!\rightarrow\!\bullet$ represent the recursive orbit structure illustrated in Figure 2.

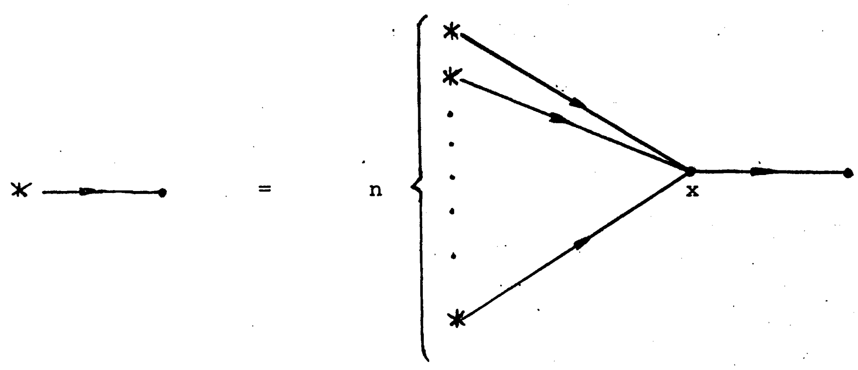
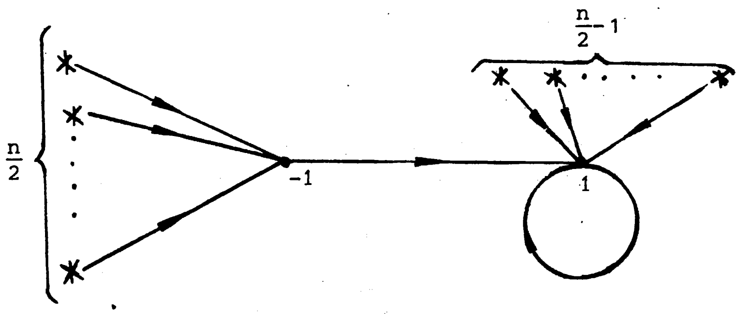


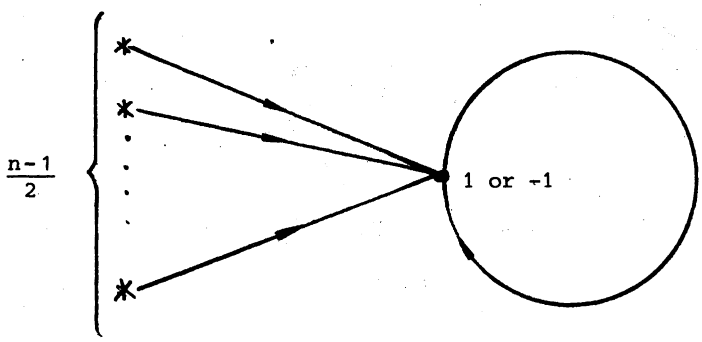
Figure 2

Orbits of type I are those containing 1 and -1. By appealing to (d), (f), (g), and (h) of Lemma 1 it is readily seen that these have the structure I^{even}, illustrated in Figure 3 when n is even, and by appealing to (d), (i), (j) and (k), the structure I^{odd} illustrated in Figure 4 when n is odd.



Orbits of Type I^{even}

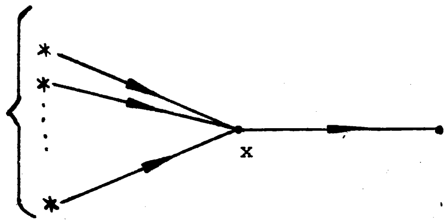
Figure 3



Orbits of Type I^{odd}

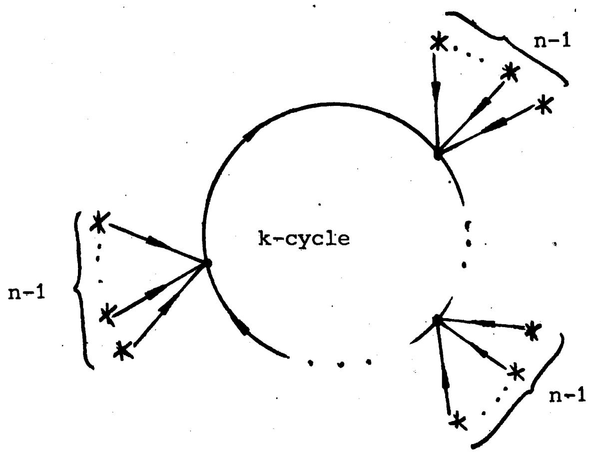
Figure 4

Orbits not containing 1 or -1 are of type II. All such acyclic orbits have the orbit structure illustrated in Figure 5 and are labeled II_0. All such k-cyclic orbits have the orbit structure illustrated in Figure 6 and are labeled II_k.



Structure about each point x
in an orbit of Type II_0

Figure 5



Orbit of Type II_k, $k \geq 1$

Figure 6

Having determined the structural types of the orbits, for a given $n \geq 2$, we now determine the number of distinct orbits of each type. Clearly there is only one orbit of type I^{even} and there are exactly two orbits of type I^{odd}. Next, T_n has n fixed points, all in $[-1,1]$, whence there are n 1-cyclic T_n-orbits. Thus there are n - 1 orbits of type II_1^{even} and n - 2 of type II_1^{odd}. Similarly, for any fixed $k > 1$, T_n has a finite number of k-cyclic orbits. Now, each T_n-orbit is a countable set. Consequently, the union of all cyclic T_n-orbits is also countable. Its complement in the interval $[-1,1]$, is the union of orbits of type II_0. Since this complement is uncountable, the number of type II_0 orbits is infinite.

To compute the number of orbits of type II_k for $k>1$ we need several results (Lemmas 2 and 5 and Theorem 5) due to A. Sklar.

Lemma 2. Let h be any function and $k \geqslant 1$. Then

$$Z_k(h) = \frac{1}{k}\sum_{d|k} \mu(d) Z_1(h^{k/d}), \qquad (3.2)$$

where $Z_k(h)$ is the number of k-cyclic orbits of h, and μ is the Mobius function.

Proof: We set $R_m(h)$ equal to the set of all elements in Dom h left fixed by h^m, and we set $C_d(h)$ equal to the union of all d-cycles of h. Now, for any $m \geqslant 1$, x is a fixed point of h^m if and only if it is a fixed point of h^d where d divides m. It follows that

$$R_m(h) = \bigcup_{d|m} C_d(h), \qquad (3.3)$$

where, since the sets $C_d(h)$ in (3.3) are disjoint,

$$\#R_m(h) = \sum_{d|m} \#C_d(h). \qquad (3.4)$$

Now, $\#R_m(h) = Z_1(h^m)$ and $\#C_d(h) = dZ_d(h)$, whence

$$Z_1(h^m) = \sum_{d|m} dZ_d(h). \qquad (3.5)$$

Applying the Mobius transformation to (3.5) yields 3.2.

Lemma 3. If $n \geqslant 2$ and $k \geqslant 1$, then

$$Z_k(T_n) = \frac{1}{k}\sum_{d|k} \mu(d) n^{k/d}. \qquad (3.6)$$

Proof: If $n \geqslant 2$ and $k \geqslant 1$, then by Lemma 1, (i), (vi), $Z_1(T_n^k) = Z_1(T_{n^k}) = n^k$. Thus (3.6) follows from Lemma 2.

We summarize the results obtained above in Table 1, where c denotes the cardinal number of the continuum.

ORBIT TYPE	NUMBER OF ORBITS
I^{even}	1
I^{odd}	2
II_0	c
II_1^{even}	n - 1
II_1^{odd}	n - 2
II_k, k > 1	$\frac{1}{k}\sum_{d\mid k} n^{\frac{k}{d}}$

Table 1

4. Proof of the Main Theorem.

Necessity. If $n \equiv 2$ or 3 (mod 4) then T_n has no iterative root of order 2.

Proof: By Lemma 3,

$$Z_2(T_n) = \frac{1}{2}\sum_{d\mid 2} \mu(d)n^{\frac{2}{d}} = \frac{1}{2}(n^2 - n).$$

However, it follows from Theorems 1 and 3 that if T_n has a root of order 2 then $Z_2(T_n)$ is divisible by 2, i.e. $(n^2 - n)/2 \equiv 0 \pmod 2$. This is equivalent to $n^2 \equiv n \pmod 4$ which, in turn, is equivalent to $n \equiv 0$ or 1 (mod 4). Positive integer m. Then

$$x^{2^{L+1}} = (x^{2^L})^2 = m^2 2^{2(k+L)} + m2^{k+L+1} + 1 \equiv$$

$$1 \pmod{2^{k+L+1}}.$$

Lemma 4. If $n,k \geqslant 2$ and $n \equiv 0$ or $1 \pmod 4$ then, $Z_k(T_n) \equiv 0 \pmod 2$.

Proof: We split cases.

Case 1: $k \equiv 1 \pmod 2$: If n is even then, by (3.6),

$$kZ_k(T_n) = \sum_{d|k} \mu(d) n^{\frac{k}{d}} \equiv 0 \pmod 2.$$

If n is odd, then

$$kZ_k(T_n) = \sum_{d|k} \mu(d) n^{\frac{k}{d}} \equiv \sum_{d|k} \mu(d) \pmod 2.$$

But, since $k \geqslant 2$, $\sum_{d|k} \mu(d) = 0$ (see e.g. [1; pp. 234-237]). Thus, for all $n \geqslant 2$, $kZ_k(T_n) \equiv 0 \pmod 2$ whence, since $k \equiv 1 \pmod 2$, $Z_k(T_n) \equiv 0 \pmod 2$.

Case 2: $k \equiv 0 \pmod 2$: Let $k = 2^{\alpha}\beta$ where $\alpha \geqslant 1$ and β is odd. Then,

$$kZ_k(T_n) = \sum_{d|k} \mu(d) n^{\frac{k}{d}} = \sum_{d|\beta} \mu(d) \left(n^{2^{\alpha}}\right)^{\frac{\beta}{d}} - \sum_{d|\beta} \mu(d) \left(n^{2^{\alpha-1}}\right)^{\frac{\beta}{d}}. \tag{4.1}$$

Now, if $n \equiv 0 \pmod 4$, then $n^{2^{\alpha-1}} \equiv 0 \pmod{2^{\alpha+1}}$, whence it follows from (4.1) that

$$kZ_k(T_n) \equiv 0 \pmod{2^{\alpha+1}}. \tag{4.2}$$

On the other hand, if $n \equiv 1 \pmod 4$ an easy induction shows that $n^{2^{\alpha-1}} \equiv 1 \pmod{2^{\alpha+1}}$ whence, by (4.1),

$$kZ_k(T_n) \equiv \left(\sum_{d|\beta} \mu(d) - \sum_{d|\beta} \mu(d)\right) \pmod{2^{\alpha+1}}. \tag{4.3}$$

Therefore, (4.2) holds for all $n \geqslant 2$. It follows that $\beta Z_k(T_n) \equiv 0 \pmod 2$ whence, since $\beta \equiv 1 \pmod 2$,

$Z_k(T_n) \equiv 0 \pmod 2$.

Sufficiency. If $n \equiv 0$ or 1 (mod 4) then, T_n has an iterative root of order 2.

Proof: By Theorem 1, it suffices to show that the set of orbits of T_n may be partitioned into a set of mateable pairs of orbits and a set of self-mateable orbits. Since the cases n=0 and n=1 are trivial, we shall assume that $n \geqslant 4$.

From Table 1 and Lemma 4 it follows that the number of orbits of type II_k, $k \neq 1$, is either even or infinite. We may thus decompose each of these sets into a disjoint collection of pairs. The orbits in any such pair are isomorphic, whence, by Theorem 2, they may be mated. This leaves only the 1-cyclic orbits to be either mated or self-mated.

Case 1: $n \equiv 0$ (mod 4): If $n \equiv 0$ (mod 4) then, by Table 1, there is one orbit of type I^{even} and there are n - 1 isomorphic orbits of type II_1. Since n - 1 is odd we may mate all but one orbit of type II_1. This remaining orbit, say H, can be mated with the one orbit of type I^{odd}, say L, as follows. Let $\sim$ be the contraction equivalence defined on L which identifies -1 and 1. It is clear from Figure 7 that $L/\sim$ is isomorphic to H.

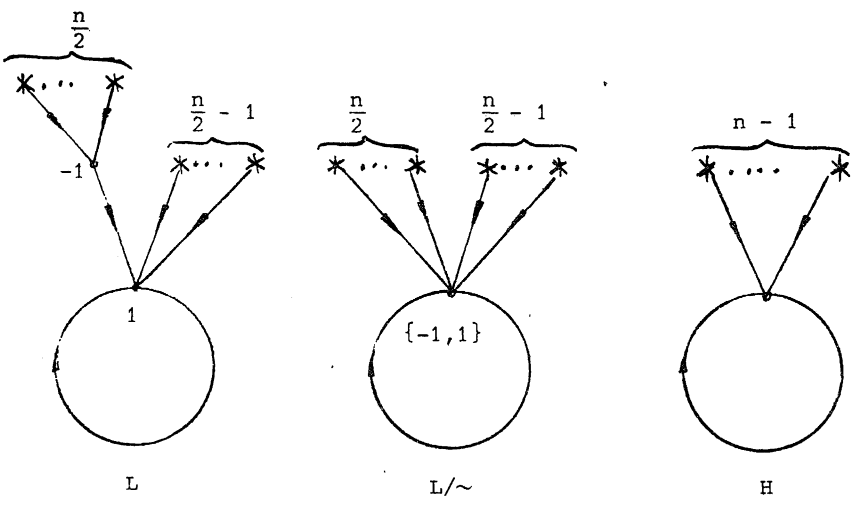


Figure 7

But H is trivially a curtailment of itself whence, by Theorem 2, L and H are mateable.

Case 2: $n \equiv 1 \pmod 4$: If $n \equiv 1 \pmod 4$ then by Table 1 there are two isomorphic orbits of type I^{odd}. These are mateable. The remaining orbits are all of type II_1. If L is one of these then L has $n-1 = 2m$ branches.

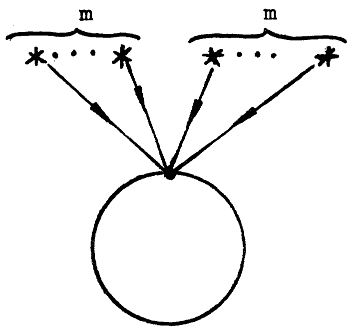


Figure 8

We now verify that L is self-mateable, i.e., satisfies conditions (i) and (ii) of Theorem 3. Since L is 1-cyclic it satisfies (i) with $k = 0$. Next, partition the branches of L into two disjoint sets, $\{B_\alpha\}_{\alpha=1}^m$ and $\{\bar{B}_\alpha\}_{\alpha=1}^m$, each containing m branches (see Figure 8). For each $\alpha = 1,\ldots,m$, B_α is a branch; and since a branch is clearly a branch cluster, $\bar{B}_\alpha$ is a branch cluster. Since all the branches of L are isomorphic, $B_\alpha \approx \bar{B}_\alpha$, whence, trivially, a curtailment of B_α is isomorphic to a contraction of $\bar{B}_\alpha$. B_α is from Z, and $\bar{B}_\alpha$ is from $z = g^0(z) = g^k(z)$. Thus (ii) of Theorem 3 is satisfied, and the sufficiency part of the Main Theorem is proved.

5. Epilogue.

In the introduction it was stated that the Main Theorem applied to any sequence of functions which are conjugate to the Čebyšev polynomials defined on $[-1,1]$. Among these sequences are the hat functions [6] and the Čebyšev polynomials defined on the complex plane by (3.1).

Extending the domain of a Čebyšev polynomial T_n, $n \geq 1$, from $[-1,1]$ to the real line via (3.1) simply introduces an infinite number of pair wise isomorphic acyclic orbits. It follows that the Main Theorem applies to the Čebyšev polynomials defined on the real line [4] though these function are not conjugate to the Čebyšev polynomials defined on the interval $[-1,1]$.

References.

[1] G. H. HARDY and E.M. WRIGHT, An Introduction to the Theory of Numbers, 4th. ed., Clarendon Press, Oxford,(1960).

[2] R. ISAACS, Iterates of fractional order, Canadian J. Math., 2 (1950), 409-416.

[3] R. E. RICE, Iterative square roots of Čebyšev polynomials, Notices AMS 23, Oct. 1976, A-565, Abstract 76T-A199.

[4] R. E. RICE, Fractional Iterates, Ph. D. Dissertation, University of Massachusetts, Amherst, Massachusetts, 1977.

[5] R. E. RICE, B. SCHWEIZER, and A. SKLAR, When is $f(f(z)) = az^2 + bz + c$ for all complex z?, American Math, Monthly (to appear).

[6] T. J. RIVLIN, The Chebysev Polynomials, Wiley - Interscience, New York, (1974).

[7] A. SKLAR, Notes on functional equations, unpublished.

[8] A. SKLAR, On the talk of Miss Riggert (Remark and Problem), Aequat. Math., 14 (1976) 226.

[9] G. ZIMMERMANN, Iterative roots of Čebyšev polynomials, (Abstract) Aequat. Math. 17 (1978) 368.