Rational Shifts of Linearly Periodic Continued Fractions

Tudor Dimofte

February 12, 2003

Contents

[1] taken from [3]

1 General Theory of Continued Fractions

Much of this report will be concerned with "linearly periodic" continued fractions. Hence it may be useful to start with a quick overview of continued fractions.

1.1 Notation

A continued fraction is something of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}, \tag{1}$$

where the coefficients $a_0, a_1, a_2, a_3, \ldots$ are numbers of some type. The expression may either terminate or continue infinitely. We can also write (1) in the neater, more compact notation

$$[a_0, a_1, a_2, a_3, \ldots]. \tag{2}$$

Most of the time we shall only be concerned with *simple* continued fractions, those for which all the coefficients are (strictly) positive integers, except perhaps a_0, which may be any integer. So from now on, "continued fraction" will be assumed to mean "simple continued fraction" unless otherwise noted. (The most common–or perhaps the only–exception will be a finite continued fraction whose last coefficient is not an integer.)

A **periodic** continued fraction is one in which the coefficients begin to repeat after a certain point. Certainly any periodic continued fraction is infinite. The continued fraction would be written as, eg,

$$[a_0, a_1, \overline{a_2, a_3, a_4}] = [a_0, a_1, a_2, a_3, a_4, a_2, a_3, a_4, a_2, \ldots]. \tag{3}$$

We shall also define a **linearly periodic** continued fraction[2] of period j and intoductory sequence length l to be of the form

$$\begin{aligned} &[\ldots, a_{l-1}, \overline{f_1(n), f_2(n), \ldots, f_j(n)}], \qquad n = 1, 2, 3, \ldots \\ &= [\ldots, a_{l-1}, f_1(1), f_2(1), \ldots, f_j(1), f_1(2), f_2(2), \ldots, f_j(2), f_1(3), \ldots], \end{aligned} \tag{4}$$

where the functions $f_1, f_2, \ldots, f_j$ are linear in the sense that $f_i(n) = b_i n + c_i$ $(\forall i)$. Since the coefficients must all be integers, the constants b_i and c_i must be integers as well. To see this, first note that $b_i(1) + c_i = b_i + c_i = m$ (for some integer m). Then $b_i(2) + c_i = m + b_i$ must also be an integer $\Rightarrow b_i$ is an integer. And from $c_i = m - b_i$ we have that c_i is an integer. In fact, we must also have $b_i \geq 0$ and $c_i > -b_i$ $(\forall i)$ if the coefficients are to be strictly positive. Note that any periodic continued fraction is also a linearly periodic continued fraction with

[2] these are also clearly infinite

$b_i = 0 \, \forall i$. Also note that we could imagine defining all sorts of "quasi-periodic" continued fractions with (4) if we take the f_i to be various different types of integer-valued functions.

1.2 A few pertinent results

We shall now *sketch* proofs of the following preliminary results[3]:

- Every finite continued fraction is a rational number and every rational number can be written as a finite continued fraction.
- Every infinite continued fraction converges to an irrational number and every irrational number can be written as an infinite continued fraction.
- If we assume that the last coefficient of any finite continued fraction is not 1, then the continued fraction expansion of any number is unique.
- A continued fraction is periodic if and only if it converges to a root of a quadratic.

For any (finite or infinite) continued fraction, define the $\mathbf{n^{th}}$ **convergent** x_n to be

$$x_n = [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}, \quad (p_n, q_n) = 1 \tag{5}$$

where $n \leq N$ if the continued fraction is finite, $[a_0, a_1, \ldots, a_N]$, and p_n and q_n are polynomials in the a_i. Note that we have $p_0 = a_0, p_1 = a_0 a_1 + 1, q_0 = 1, q_1 = a_1$. If we further define $p_{-1} = 1$ and $q_{-1} = 0$ we have

Lemma 1 *For any $n \geq 1$, $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$. In other words,*

$$\begin{aligned} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} &= \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \end{aligned} \tag{6}$$

Proof. We have already considered the cases $n = 1, 2$. Assume that for a given n in the continued fraction $[a_0, a_1, \ldots, a_N, \ldots]$ with $N > n$ and possibly no coefficients after a_N we have $p_n = a_n p_{n-1} + p_{n-2}$ and $q_n = a_n q_{n-1} + q_{n-2}$, i.e.

$$x_i = [a_0, \ldots, a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}. \tag{7}$$

[3]Ideas for the proofs were taken from [4], Chapters 5-8, 11 and [1], Section 2.

Then we consider[4]

$$\begin{aligned} x_{n+1} = \frac{p_{n+1}}{q_{n+1}} &= [a_0, a_1, \ldots, a_{n+1}] \\ &= a_0 + \cfrac{1}{a_1 + \cfrac{\ddots}{a_n + \frac{1}{n+1}}} \\ &= [a_0, a_1, \ldots, a_n + \tfrac{1}{a_n+1}] \end{aligned}$$

$$\begin{aligned} &= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \qquad \textit{by (7)} \\ &= \frac{(a_n a_{n+1} + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_n a_{n+1} + 1)q_{n-1} + a_{n+1}q_{n-2}} \\ &= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}. \end{aligned} \tag{8}$$

The lemma follows by induction. $\diamondsuit$

Corrolary 1 *Taking determinants of the matrices in* (6)*, we get*

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1} \tag{9}$$

Corrolary 2 *Writing* $p_n q_{n-2} - q_n p_{n-2} = (a_n p_{n-1} + p_{n-2})q_{n-2} - (a_n q_{n-1} + q_{n-2})p_{n-2} = a_n(p_{n-1}q_{n-2} - q_{n-1}p_{n-2}) + (p_{n-2}q_{n-2} - p_{n-2}q_{n-2}) = (-1)^{n-2}a_n$ *we get*

$$p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n. \tag{10}$$

Corrolary 3 *For any* n *and any continued fraction (with more than* $n+1$ *coefficients) we have*

$$(p_n, q_n) = 1 \tag{11}$$

Proof. Suppose $d|p$. Then d divides the LHS or (9), so we must have $d = \pm 1$.

Corrolary 4 *For any continued fraction (more than* n *terms) we have* $\forall n \geq 1$*:*

$q_n \geq q_{n-1}$*, strict inequality for* $n > 1$

$q_n \geq n$*, strict inequality for* $n > 3$*.*

[4]The third step is slightly sloppy, since the last coefficient is no longer an integer. No great harm is done, and this can be interpreted as a continued fraction in the more general sense.

Proof. The first part follows from $q_0 = 1$, $q_1 = a_1$, Lemma 1, and the fact that all coefficients after the first are strictly positive. The second part follows from the first and the fact that the coefficients are strictly positive. $\diamondsuit$

Lemma 2 *The sequences x_{2i} and x_{2i+1} are increasing and decreasing sequence, respectively. Moreover, we have $x_{2n} < x_{2n+1}$ for every n (assuming of course that the continued fraction has more than $2n+1$ coefficients).*

Proof. Taking into account that the coefficients (thus all p_i and q_i for $i \geq 0$) are strictly positive, and that equations (9) and (10) can be rewritten as

$$x_n - x_{n-1} = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \tag{12}$$

and

$$x_n - x_{n-2} = \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}, \tag{13}$$

the right substitutions yield the Lemma. $\diamondsuit$

We want to study one more aspect of continued fractions before we can really say things about the numbers they represent. Since any finite continued fraction can be written in two ways,

$$[\ldots, a_N] = [\ldots, (a_N - 1), 1], \tag{14}$$

let us adopt the convention that the last term is never 1. For a given continued fraction of more than n terms, let α_n denote its "tail end," $[a_n, a_{n+1}, \ldots]$. If $\lfloor x \rfloor$ denotes the greatest integer $\leq x$, then we have

Lemma 3 $\lfloor \alpha_n \rfloor = a_n$ *for all n.*

Proof. If the continued fraction is finite and $N = n$, the result is trivial. Otherwise, $\alpha_n = a_n + \frac{1}{a_{n+1}+\ldots}$. If the continued fraction is finite and $N = n+1$ then nothing follows a_{n+1}, which is > 1 by the above convention, so the result follows. If not, then the "$\ldots$" are some other continued fraction, which is strictly positive because all the coefficients are strictly positive, so the denominator of $\frac{1}{a_{n+1}+\ldots}$ is strictly greater than 1 and the result follows. $\diamondsuit$

From this, we can prove the important result on uniqueness.

Theorem 1 *Let $x = [a_0, \ldots, a_N] = [b_0, \ldots, b_M]$ be two finite continued fractions. Then $N = M$ and $a_i = b_i$ for all i.*

Proof. Certainly $\lfloor x \rfloor = a_0 = b_0$. Then

$$\lfloor x \rfloor + \frac{1}{[a_1, \ldots, a_N]} = \lfloor x \rfloor + \frac{1}{[b_1, \ldots, b_M]} \tag{15}$$

$$\Rightarrow [a_1, \ldots, a_N] = [b_1, \ldots, b_M], \tag{16}$$

and the proof follows by induction. $\diamondsuit$

Corrolary 5 *If two (convergent) infinite continued fractions are equal,* $[a_0, a_1, \ldots] = [b_0, b_1, \ldots]$*, then* $a_i = b_i$ *for all* i*.*

Proof. Pick an arbitrary integer N. Then the above induction argument can be used to show that the first $N+1$ coefficients of the two continued fractions are equal. Note that (as we shall demonstrate shortly) all the "tail end" continued fractions converge very nicely and pose no problem to the induction argument. $\diamondsuit$

Now we are finally ready to prove the results on the continued fractions of rational and irrational numbers. To every real number x we can associate a continued fraction in the following way. Let

$$a_0 = \lfloor x \rfloor, \quad \alpha_1 = \frac{1}{x - a_0}. \tag{17}$$

Then we will have

$$x = a_0 + \frac{1}{\alpha_1}. \tag{18}$$

We continue recursively, defining[5]

$$a_i = \lfloor \alpha_i \rfloor, \quad \alpha_{i+1} = \frac{1}{\alpha_i - a_i}. \tag{19}$$

Certainly every finite continued fraction is a rational number, and by Theorem 1 this continued fraction is unique. In the other direction,

Theorem 2 *The continued fraction expansion of every rational number is finite.*

Proof. In view of equations (17)-(19), we want to show that the recursive process must terminate at some point.

Let $x = h/k$, $(h, k) = 1$, $k>0$, be a rational number. Using the above recursion to find coefficients, we have $a_0 = \lfloor x \rfloor$, so $h/k = a_0 + \xi_0$ for some $0 \leq \xi < 1$. Then we can write $h = a_0 k + \xi_0 k$ and we see that the integer $\xi_0 k$ is in fact the remainder of dividing h by k–note that $0 \leq \xi_0 k < k$.

We can continued in this way. Let $k_1 = \xi_0 k$. Then

$$\alpha_1 = \frac{1}{x - a_0} = \frac{1}{\xi} = \frac{k}{k_1} = a_1 + \xi_1 \tag{20}$$

with $0 \leq \xi_1 < 1$, so $0 \leq \xi_1 k_1 < k_1$. Then we define $k_2 = \xi_1 k_1$, and so on. We obtain a strictly decreasing sequence of nonnegative integers $k > k_1 > k_2 > \ldots$, which must eventully terminate. When this sequence terminates, we will have

$$\alpha_n - \lfloor \alpha_n \rfloor = \xi_n = 0 \tag{21}$$

[5]Here we use α to denote the tail end of continued fractions. Note that in other parts of this paper we also use primed a's. For example, we might write the continued fraction $[a_0, a_1, \ldots]$ as $[a_0, a_1']$ where $a_1' = \alpha_1 = [a_1, a_2, \ldots]$.

for some n, and the continued fraction will terminate. $\diamondsuit$

For irrational numbers, the results are

Theorem 3 *Every infinite continued fraction converges to an irrational limit.*

Proof. From Lemma 2 we know that the convergents to an infinite continued fraction satisfy $x_2, x_4, x_6, \ldots, x_5, x_3, x_1$, and both of the bounded monotone sequences $\{x_{2n}\}$ and $\{x_{2n+1}\}$ must converge to a real limit. But from Lemma 2 and Corollary 4 we have

$$|x_{2n+1} - x_{2n}| = \frac{1}{q_{2n}q_{2n+1}} \leq \frac{1}{(2n)(2n+1)} \to 0 \quad as\ n \to \infty, \tag{22}$$

so the two limits must in fact be equal. And since we know that every rational number has a finite continued fraction expansion and continued fractions are (semi)unique, the limit of this infinite continued fraction must irrational. $\diamondsuit$

Theorem 4 *Defined by the recursive method in equations* (17)-(19)*, the continued fraction expansion of an irrational number is infinite and converges to the number.*

Proof. If the expansion were finite, the recursive process would have to terminate somewhere. This means that the greatest integer of a rational function of x involving just integer coefficients is zero, which is impossible. So the continued fraction of an irrational number must be infinite and must converge. We need to show that it actually converges to the number itself.

Let x be irrational and denote by $[a_0, a_1, \ldots]$ its continued fraction expansion. We know that for any finite n we will have $x = [a_0, \ldots, a_n, \alpha_{n+1}]$, with α_{n+1} defined as in equations[6] (17)-(19). The $(n+1)$st convergent to *this* continued fraction is equal to the entire continued fraction, hence equal to x. So by Lemma 1 we have

$$x = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} \tag{23}$$

and (by Corrolary 9)

$$\begin{aligned} \left| x - \frac{p_n}{q_n} \right| &= \left| \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \right| \\ &= \left| \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} \right| \\ &= \frac{1}{q_nq'_{n+1}}, \end{aligned} \tag{24}$$

with $q'_{n+1} = \alpha_{n+1}q_n + q_{n-1}$. For any n, this is a measure of how well the nth partial convergent of the (simple) continued fraction of x converges to x.

[6] This is of course not a simple continued fraction.

Since $a_{n+1} = \lfloor \alpha_{n+1} \rfloor < \alpha_{n+1} < a_{n+1} + 1$ (strict inequality because the continued fraction is infinite) and $a_{n+2} \geq 1$, we have

$$\begin{aligned} q_{n+1} = a_{n+1}q_n + q_{n-1} < q'_{n+1} < (a_{n+1}+1)q_n + q_{n-1} = q_{n+1} + q_n, \\ q_{n+1} + q_n \leq a_{n+2}q_{n+1} + q_n = q_{n+2} \\ \Rightarrow \; q_{n+1} < q'_{n+1} < q_{n+2}. \end{aligned} \tag{25}$$

Therefore, from (24) and Corrolary 4 we have

$$\frac{1}{q_n q_{n+2}} < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \tag{26}$$

$$\Rightarrow \left| x - \frac{p_n}{q_n} \right| < \frac{1}{n^2} \; \to \; 0 \tag{27}$$

as $n \to \infty$. $\diamondsuit$

The last result we want is

Theorem 5 *An irrational number x has a periodic continued fraction if and only if it satisfies a quadratic equation $Ax^2+Bx+C = 0$ with integer coefficients.*

$\Rightarrow$

Let $x = [a_0, a_1, \ldots, a_{l-1}, \overline{a_l, \ldots, a_{l+k-1}}]$, a continued fraction with period k. Then

$$\alpha_l = [\overline{a_l, \ldots, a_{l+k-1}}] = [a_l, \ldots, a_{l+k-1}, \overline{a_l, \ldots, a_{l+k-1}}] = [a_l, \ldots, a_{l+k-1}, \alpha_l].$$

If $\frac{p_i}{q_i}$ are the convergents to α_l, then

$$\alpha_l = \frac{\alpha_l p_{k-2} + p_{k-3}}{\alpha_l q_{k-2} + q_{k-3}}, \tag{28}$$

which translates into a quadratic equation for α_l. But if $\frac{p'_i}{q'_i}$ are the convergents for x, then

$$\begin{aligned} x &= [a_0, \ldots, a_{l-1}, \alpha_l] \\ \Rightarrow x &= \frac{\alpha_l p'_{l-1} + p'_{l-2}}{\alpha_l q'_{l-1} + q'_{l-2}} \\ \Rightarrow \alpha_l &= \frac{p'_{l-2} - x q'_{l-2}}{x q'_{l-1} - p'_{l-1}} \\ \Rightarrow \alpha_l &= \frac{\alpha_l p_{k-2} + p_{k-3}}{\alpha_l q_{k-2} + q_{k-3}} \cdot \frac{x q'_{l-1} - p'_{l-1}}{x q'_{l-1} - p'_{l-1}}, \end{aligned}$$

which becomes a quadratic equation for x with integer coefficients. Note that the leading coefficient must be non-zero, for otherwise x would be rational and the continued fraction could not be infinite.

$\Leftarrow$

Assume x solves the irreducible quadratic

$$ax^2 + bx + c = 0 \tag{29}$$

with integer coefficients. Further assume that this is irreducible (otherwise, x would be rational). Write

$$x = [a_0, a_1, \ldots] = [a_0, \ldots, a_{n-1}, \alpha_n] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}. \tag{30}$$

By substituting this in (29), clearing denominators, and collecting terms, we get

$$A_n(a_n')^2 + B_n a_n' + C_n = 0, \tag{31}$$

with (in particular)

$$A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \neq 0, \quad C_n = A_{n-1} \tag{32}$$

and

$$B_n^2 - 4A_nC_n = b^2 - 4ac. \tag{33}$$

Note that $A_n \neq 0$ because otherwise the rational p_{n-1}/q_{n-1} would solve the irreducible (29).

Now, by (26) we can find $|\delta_{n-1}| < 1$ such that

$$x - \frac{p_{n-1}}{q_{n-1}} = -\frac{\delta_{n-1}}{q_{n-1}^2}, \tag{34}$$

$$p_{n-1} = xq_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}, \tag{35}$$

and we substitute this into the expression for A_n, expand, and take the absolute value (and note that $ax^2 + bx + c = 0$) to get

$$|A_n| \leq 2|ax| + |b| + |a|. \tag{36}$$

Likewise, since $C_n = A_{n-1}$ we have

$$|C_n| \leq 2|ax| + |b| + |a|, \tag{37}$$

and from (33) we have

$$B_n \leq \sqrt{|4A_nC_n| + |b^2 - 4ac|} \leq \sqrt{4(2|ax| + |b| + |a|)^2 + |b^2 - 4ac|}. \tag{38}$$

Therefore (since these relations hold for all n), there exists a bound M such that $|A_n|, |B_n|, |C_n| < M$ for all n.

Since there are only a finite number of possible values for the triplet (A_n, B_n, C_n) and we go through infinite values of n, we must be able to find three values of n that have the same triplet, say n_1, n_2, and n_3. So three tail ends $a_{n_1}, a_{n_2}, a_{n_3}$ all satisfy the nonzero quadratic (31). But this implies that two of them must be equal, which implies periodicity. $\diamondsuit$

1.3 Kuzmin's Theorem

This theorem will be important when we consider the distribution of coefficients in various linearly periodic continued fractions. The proof is rather intricate and has been left out; consult [2].

Theorem 6 *Let k be an integer ≥ 1. Let $[a_0(x), a_1(x), \ldots]$ be the continued fraction of x. Then for* almost any *number x, the probability that $a_n(x) = k$ is*

$$P(a_n(x) = k) = \log_2\left(1 + \frac{1}{k(k+2)}\right) + O\left(\frac{1}{k(k+1)}e^{-C\sqrt{n+1}}\right), \tag{39}$$

with C independent of n and k.

This result was in fact be improved to

$$P(a_n(x) = k) = \log_2\left(1 + \frac{1}{k(k+2)}\right) + O(e^{-C'n}) \tag{40}$$

by Levy, which is nice though not entirely relevant to the problem at hand.

Note that no linearly periodic continued fraction, of the form (4), can satisfy Kuzmin's Theorem. All periodic coefficients $f_i(n)$ fall into one of two categories: coefficients which remain constant from period, and coefficients which increase by a fixed amount from period to period. If we pick any number k that is greater than the constant coefficients, it may occur a finite number of times as a value of an increasing coefficient and then never again. So $P(a_n = k) = 0$ for sufficiently large n. Likewise, $P(a_n = k)$ is non-zero but fixed for any of the constant coefficients. So the continued fraction cannot possibly satisfy the theorem. This observation, incidentally, implies that the set of all linearly periodic continued fractions has measure 0; otherwise, Kuzmin's theorem could not fail.

Nevertheless, we *will* be interested in the distribution of the constant periodic coefficients in comparison to Kuzmin's Theorem. For this we can simply take n as large as we want and the error in the theorem as small as we want. For future reference, Table 1.3 lists a few probabilities, disregarding error.

2 The Lang-Trotter Algorithm

The initial motivation behind studying rational shifts of linearly periodic continued fractions was the Lang-Trotter algorithm for finding continued fraction expansions of roots of a polynomial. In order to use Equations (17)-(19) to calculate the continued fraction of a number, one must know the number to very high accuracy (at least in order to retreive a significant number of coefficients). On the other hand, to use the following algorithm nothing needs to be known about an algebraic number except its polynomial and the greatest integer less than or equal to it.

$\mathbf{k}$	$\mathbf{P(a_n = k)}$ (%)	$\mathbf{k}$	$\mathbf{P(a_n = k)}$ (%)
1	41.50	11	1.01
2	16.99	12	0.86
3	9.31	13	0.74
4	5.89	14	0.64
5	4.06	15	0.56
6	2.97	16	0.50
7	2.27	17	0.45
8	1.79	18	0.40
9	1.45	19	0.36
10	1.20	20	0.33

Table 1: Kuzmin Probabilities

2.1 The algorithm[7]

Let ξ be an irrational root of a polynomial $p_0(x)$ of degree d such that

1. the leading coefficient of $p_0(x)$ is positive
2. the root ξ is simple
3. $\xi > 1$
4. there are no other positive roots.

Then let $a_0 = \lfloor \xi \rfloor$ = the greatest integer k such that $p_0(k) < 0$ (this is the case since a positive leading coefficient implies that $f_0(x)$ will go from negative to positive at its last real root) and let $q_0 = p_0(x + a_0)$, $p_1(x) = -x^d q_0(x^{-1}) = -x^d p_0(a_0 + x^{-1})$. The roots of $q_0(x)$ are exactly those of $p(x)$ shifted by $-a_0$ units. So $q_0(x)$ has the root corresponding to ξ between 0 and 1 and no other positive roots. Then the roots of $p_1(x)$ are the reciprocals of those of $q_0(x)$, so $(\xi - a_0)^{-1} > 1$ and is the unique positive root of $p_1(x)$. Also notice that the leading coefficient of $p_1(x)$ is positive. Thus we have constructed another polynomial that satisfies (1) - (4).

For all $i \geq 1$ we define the recursion

$$\begin{aligned} a_i &= \lfloor p_i(x) \rfloor \\ p_{i+1}(x) &= -x^d p_i\big(\frac{1}{x} + a_i\big), \end{aligned} \tag{41}$$

where $\lfloor p_i(x) \rfloor$ is the greatest integer k such that $p_i(k) < 0$. If we let ξ_i denote the unique positive root of $p_i(x)$ then we have $a_i = \lfloor \xi_i \rfloor$. So, with $\xi_0 = \xi$, the effects of our recursion are just

$$a_i = \lfloor \xi_i \rfloor, \qquad \xi_{i+1} = \frac{1}{\xi_i - a_i}, \tag{42}$$

[7] taken from [3]

which is identical to equations (17) - (19). Therefore, the algorithm simply generates the continued fraction coefficients of ξ.

2.2 Loosening constraints

While it is nice that the $p_i(x)$ all satisfy conditions (1) - (4), one might wonder whether, for practical applications, these conditions are really necessary. They certainly restrict the possibility of using the algorithm on any given algebraic number. We shall thus endeavor to eliminate most of them.

Let's begin with condition (1). The main advantage of having a positive leading coefficient is that a polynomial is negative to the left of its largest root and positive to its right. Then it is always possible to find the greatest integer less than that root by testing $p_i(k) \stackrel{?}{<} 0$ for $k = 1, 2, \ldots$. But we could simply test for a sign change instead and remove the condition. Or, with a program (such as *Mathematica*) or an algorithm (such as Newton's method) that finds roots very precisely, we could find the largest positive root ξ_i of $p_i(x)$ and take $\lfloor \xi_i \rfloor$. We remove condition (1) and reformulate the algorithm as:

$$\begin{aligned} \mathit{largest\ root}(p_i(x)) &= \xi_i \\ a_i &= \lfloor \xi_i \rfloor \\ p_{i+1}(x) &= x^d p_i\left(\frac{1}{x} + a_i\right). \end{aligned} \tag{43}$$

Now consider condition (2). If the root is not simple, then testing $f_i(k)$ for a sign change will not work. However, the reformulted algorithm will do just fine. So we can delete condition (2).

Granted, eliminating conditions (1) and (2) is not incredibly useful. A polynomial with negative leading coefficient could have been multiplied by -1 to satisfy (1). And we can try to factor the polynomial so that it no longer has simple roots. If we can find the irreducible polynomial for ξ, we know it cannot have any repeated irrational roots.[8] But the reformulated algorithm will also allow us to loosen the other two conditions, which are much more limiting.

The idea of the algorithm is that it finds the greatest integer less than or equal to some root, shifts the polynomial so that the root is in $(0, 1)$, and then inverts the polynomial so that the initial root becomes the largest positive root. Suppose we have a root ξ of $p_o(x)$ such that all other real roots[9] are at least one unit away. In other words, for all other roots r_j we have $|\xi - r_j| > 1$. We take $a_0 = \lfloor \xi \rfloor$ as usual. Then ξ becomes the only root of $q_0(x) = p_0(x - a_0)$ between 0 and 1; so $\xi_1 = (\xi - a_0)^{-1}$ is the only root of $p_1(x) = x^d q_0(x^{-1})$ that is > 1. Following the algorithm through to $p_2(x)$, we see that $\xi_2 = (\xi_1 - a_1)^{-1} > 1$ is the single positive root of $p_2(x)$, so conditions (3) and (4) are satisfied from that point on. Therefore, we can weaken these conditions to

[8] We are in a field of characteristic zero, so all polynomials are seperable.

[9] Note we do not care about complex roots; the recursion will always preserve their complexity and they will not interfere with the process.

$3'$. For all roots $r_j \neq \xi$ of $p_0(x)$, $|\xi - r_j| > 1$.

We might even go a step further. For suppose we have a root ξ of $f_0(x)$ and the two real roots closest to ξ, $r_1 < \xi < r_2$, satisfy

$3''$. There is an integer between r_1 and ξ, and

$4''$. If $a_0 = \lfloor \xi \rfloor$, there is an integer between $\dfrac{1}{r_2 - a_o}$ and $\dfrac{1}{\xi - a_0}$.

Then because of $(3'')$ the root $\xi_1 = (\xi - a_0)^{-1}$ will be the largest positive root of $p_1(x)$ and by $(4'')$ there is an integer separating ξ_1 and the next largest root. Thus $p_2(x) = x^d p_1(x^{-1} + \lfloor \xi_1 \rfloor)$ will have a unique positive root > 1, $\xi_2 = (\xi_1 - \lfloor \xi_1 \rfloor)^{-1}$ and the algorithm will work just fine from then on.

We have succeeded in *almost* taking out all the original conditions, provided we keep track of where the first few roots are mapped to (before they become the unique positive root > 1). But what happens if we let ξ be *any* root of *any* polynomial $p_0(x)$?

2.3 Can we do it?

We generate incorrect continued fraction coefficients if there is *not* an integer between a ξ_i and the next largest root. Conditions $(3'')$ and $(4'')$ were sufficient to prevent this. But, *in general*, they are also necessary.

Proposition 1 *If $(3'')$ does not hold, and we assume that the roots of $p_0(x)$ are randomly distributed*[10] *(mod 1) in $(0,1)$, then the probability that the algorithm will fail is at least $2 - 2\log 2 \approx .6137$.*

Proof. Suppose $(3'')$ doesn't hold, and let $r \neq \xi$ be the smallest root (there may be several) such that $a_0 = \lfloor \xi \rfloor = \lfloor r \rfloor$. After being shifted, both of these roots will end up in $(0,1)$; so $\xi_1 = \frac{1}{\xi - a_0}$ and $r_1 = \frac{1}{r - a_0}$ will both be positive roots > 1, with $\xi_1 < r_1$. If there is an integer between ξ_1 and r_1 the algorithm will fail, generating $a_1 = \lfloor r_1 \rfloor \neq \lfloor \xi_1 \rfloor$. We know that an integer will separate the two roots if $r_1 - \xi_1 > 1$, so let's find the probability of this happening. Let $x = \xi - a_0 = \xi \pmod 1$ and $y = r - a_0 = r \pmod 1$. We want

$$\begin{aligned} \frac{1}{y} - \frac{1}{x} &> 1 \\ \Rightarrow \frac{x - y}{xy} &> 1 \\ \Rightarrow x - y &> xy \\ \Rightarrow y &< \frac{x}{x+1}. \end{aligned}$$

[10] There are several ways roots that satisfy $(3'')$ might be randomly distributed, leading to slightly different probability bounds. For now, we assume that "randomly distributed" means the points (x, y) (see definitions in the beginning of the proof) are randomly distributed in the triangle below the diagonal $y = x$ of $(0,1) \times (0,1)$. This definition is best for applications of concepts that will be developed later in this section.

So, given ξ, the probability of $r_1 - \xi_1 > 1$ should be $\frac{\xi - \lfloor \xi \rfloor}{\xi - \lfloor \xi \rfloor + 1}$. And averaging this over all possible values of ξ, i.e. all values of x, we get

$$Avg\ Prob = \int_0^1 \frac{x}{x+1}\, dx = 1 - \log 2 \approx .30685\,. \tag{44}$$

But to obtain this we assumed that r was randomly distributed in $(\lfloor \xi \rfloor, \lfloor \xi \rfloor + 1)$, which is not quite true since we know by assumption that $r \in (\lfloor \xi \rfloor, \xi)$. If we take the definion of "randomly distributed" in the footnote to the Proposition, and consider points (x, y) in the unit box $(0,1) \times (0,1)$ we see that what we have actually calculated is the area under the curve $y = x/(x+1)$. Our restriction (that these roots violate $(3'')$) implies that all possible points are situated (and randomly distributed) below the line $y = x$. So the lower bound on the probability of the algorithm failing is the fraction of points below $y = x$ that are also below $y = x/(x+1)$, which is just $2(1 - \log 2) \approx 0.6137$. $\diamondsuit$

Let's pursue success and failure of the algorithm a bit further. Suppose $(3'')$ fails for a root r such that $\lfloor \xi \rfloor < r < \xi$, and r is the only root within a unit of ξ. As noted previously, the algorithm will certainly fail if there is an integer between $\frac{1}{\xi - \lfloor \xi \rfloor}$ and $\frac{1}{r - \lfloor \xi \rfloor}$ and *may* succeed otherwise. So we have possible success if

$$\frac{1}{\xi - \lfloor \xi \rfloor} < \frac{1}{r - \lfloor \xi \rfloor} < \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor + 1. \tag{45}$$

We solve this for r:

$$\xi > r > \left(\lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor + 1 \right)^{-1} + \lfloor \xi \rfloor. \tag{46}$$

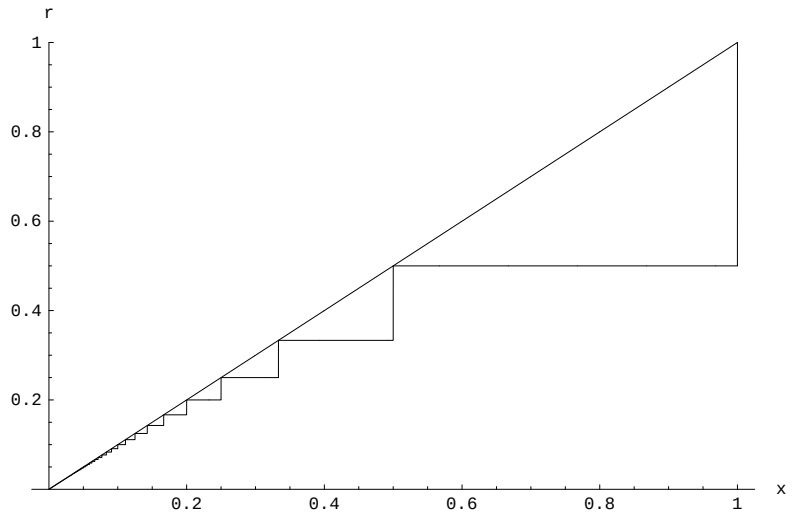
Now assume for the moment that $\lfloor \xi \rfloor = 0$, since we are essentially looking at things mod 1. So our condition is

$$\xi > r > \left(\lfloor \frac{1}{\xi} \rfloor + 1 \right)^{-1}. \tag{47}$$

If ξ is the reciprocal of an integer, then the RHS is just $\left(\frac{1}{\xi} + 1 \right)^{-1} = \frac{\xi}{\xi + 1}$. Then if we change ξ to be just a little less than the reciprocal of an integer, the RHS will remain constant. But if ξ becomes just a little more than the reciprocal of an integer the RHS will jump to what it would have been for the next highest integer. In this way we can see that the algorithm fails if (ξ, r) is below the step-like function in Figure 1, and *may* succeed otherwise.

Let's go another step, assuming "possible success" on the first cycle. If we run the algorithm again, the image of ξ will be greater than the image of r, so there will be definite success if there is an integer between the two and definite

Figure 1: Possible success, first cycle



failure otherwise. The condition for possible failure is:

$$\begin{aligned} \lfloor \xi_2 \rfloor &< r_2 \\ \Rightarrow \lfloor \frac{1}{\xi_1 - \lfloor \xi_1 \rfloor} \rfloor &< \frac{1}{r_1 - \lfloor \xi_1 \rfloor} \\ \Rightarrow r_1 &< \left(\lfloor \frac{1}{\xi_1 - \lfloor \xi_1 \rfloor} \rfloor \right)^{-1} + \lfloor \xi_1 \rfloor \end{aligned} \tag{48}$$

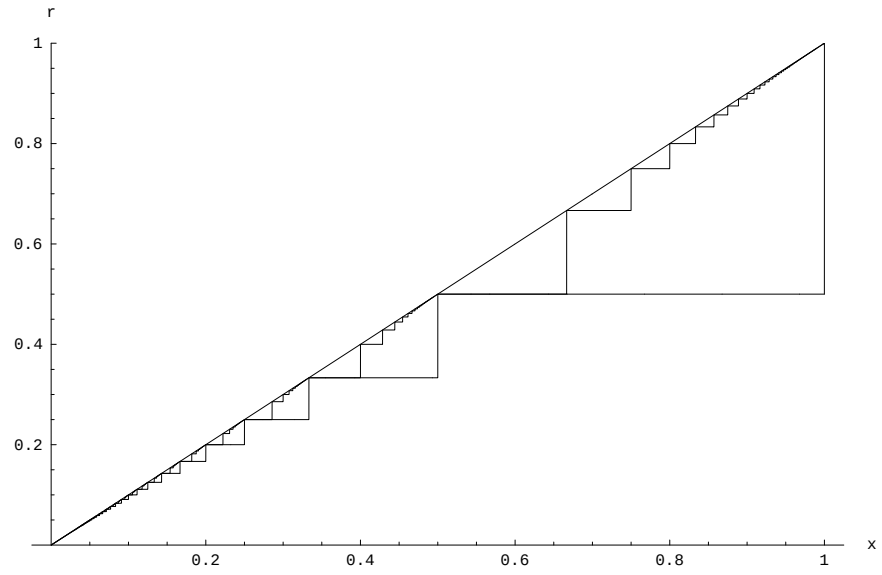
$$\begin{aligned} \Rightarrow \frac{1}{r - \lfloor \xi \rfloor} &< \left(\lfloor \frac{1}{\frac{1}{\xi - \lfloor \xi \rfloor} - \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor} \rfloor \right)^{-1} + \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor \\ \Rightarrow r &> \left(\left(\lfloor \frac{1}{\frac{1}{\xi - \lfloor \xi \rfloor} - \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor} \rfloor \right)^{-1} + \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor \right)^{-1} + \lfloor \xi \rfloor, \end{aligned} \tag{49}$$

which we plot in Figure 2, along with the previous condition. Observe that there is definite failure below the bottom step function, definite success between the two step functions, and possible failure between ξ and the step functions.

We can continue in this way, alternating between conditions for definite failure (odd cycles) and definite success (even cycles). The algebra becomes more tedious, so the exact conditions are not included here.[11] *Mathematica* notebook rless.nb can be used to generate the formulas. The notebook also

[11] Actually, the observation that the formulas are in fact continued fractions does allow them to be written explicitly in a nice way. See Proposition 2.

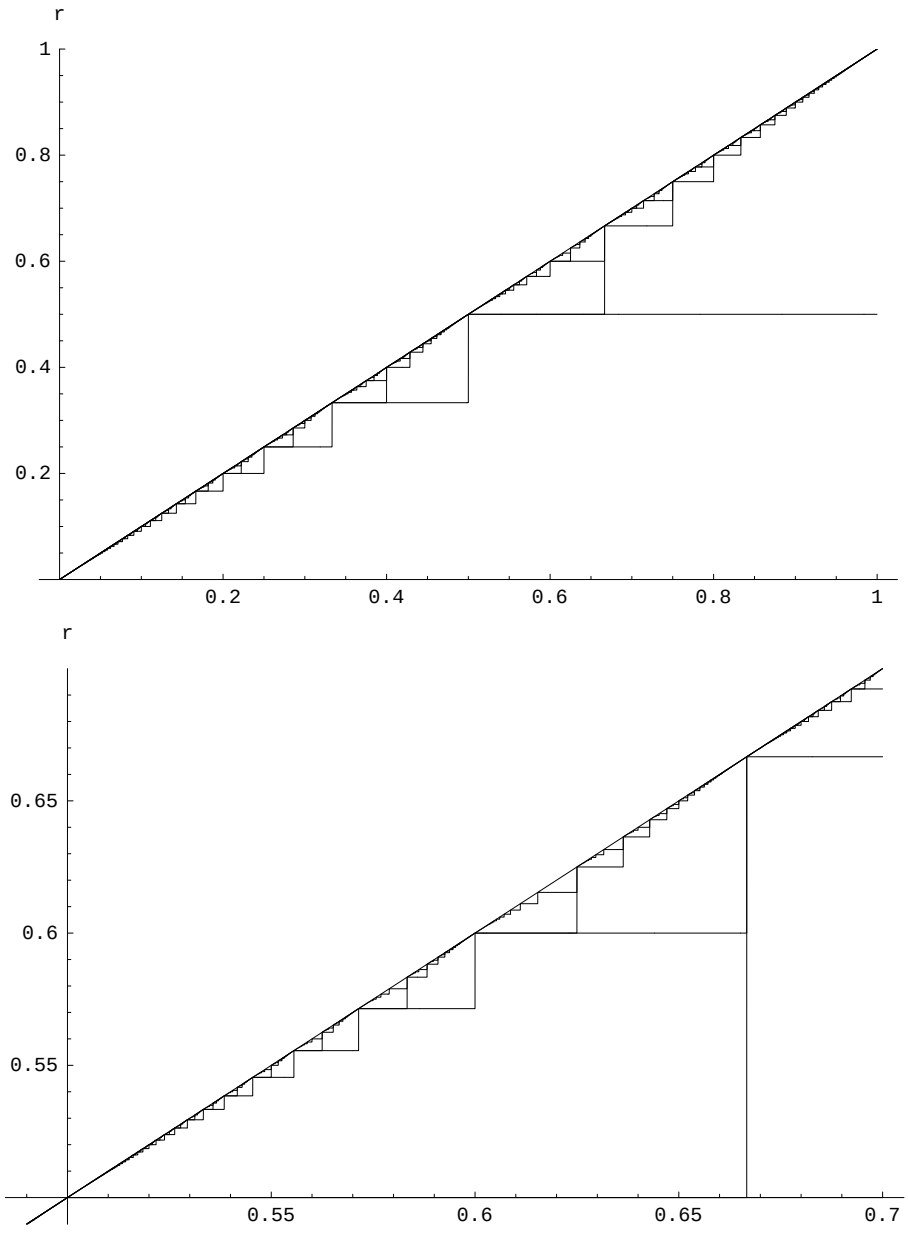
Figure 2: Possible failure, second cycle



generates plots of any iteration. Notice that after every even number of cycles, we are essentially in the same position we started from. So, given a plot of all the cycles, we would expect to see the same structure in a triangle derived from an even cycle as in the entire plot. Likewise, the interior of a triangle derived from an odd cycle should resemble the interior of any other triangle derived from an odd cycle. Figure 3 shows two plots of success and failure for the first five cycles of the algorithm. Observe that our prediction about the similar interiors of triangles is mostly valid. The triangle expanded in the bottom plot is similar (in the non-rigorous sense) to the entire top plot, but the relative sizes of the respective subtriangles are not to scale. The lengths of the largest subtriangle generated by the first cycle (the largest subtriangle in the top plot) are half the lengths of the triangle it is contained in (i.e. the bottom-right half of the entire plot). But the lengths of the largest subtriangle generated by the third cycle (the largest subtriangle in the bottom plot) are $2/5$ of the lengths of the triangle it is contained in. Whether this ratio remains $2/5$ for subtriangles of subsequent even cycles or changes is uncertain at the moment.

Now that we have a better understanding of the conditions for success or failure of the algorithm, we might hope to achieve better bounds on probabilities thereof. First, however, we show another interesting and helpful result.

Figure 3: Fifth cycle



2.3.1 A visualization of continued fractions

Proposition 2 *Let $R_n(x)$ be the step-like function corresponding to the definite success or failure of the nth cycle of the algorithm. Then $R_n(x) = x$ if and only if the continued fraction expansion of x has $\leq n+1$ coefficients.*

Note that we are really looking at $\lim_{y \to x^+} R_n(y)$ with y irrational since the algorithm will always "fail" for rational numbers after a finite number of steps, mapping the root 0 to ∞.
Also note that although the algorithm is not applicable to transcendental irrationals, the $R_n(x)$ are definded for all reals (as we shall show). So for this proof we do not restrict ourselves to algebraic irrationals.
Finally note that this argument takes into account the duality of continued fraction notation. For any x whose continued fraction has $n+1$ coefficients, we will have either $R_{n-1}(x) = x$ or $R_{n+1}(x) = x$ as well as $R_n(x) = x$.

Corrolary 6 *The set of numbers x for which $R_n(x) = x$ (for some n) is precisely the set of rational numbers (by the results of Section 1).*

Proof. Recall that $\lfloor \xi_k \rfloor$ is the kth continued fraction coefficient of ξ (provided the algorithm has not failed). Above we were looking at the algorithm's effect on a root ξ. Here x takes the role of that root and to avoid confusion in this proof we formally define

$$x_0 = x, \qquad x_k = \frac{1}{x_{k-1} - \lfloor x_{k-1} \rfloor} \tag{50}$$

$$r_0 = r, \qquad r_k = \frac{1}{r_{k-1} - \lfloor x_{k-1} \rfloor}. \tag{51}$$

The condition (for definite success[12]) for the nth cycle, n even, is

$$\begin{aligned} r_n &< \lfloor x_n \rfloor \qquad (52)\\ \Rightarrow r_{n-1} &> \frac{1}{\lfloor x_n \rfloor} + \lfloor x_{n-1} \rfloor \\ \Rightarrow r_{n-2} &< \frac{1}{\frac{1}{\lfloor x_n \rfloor} + \lfloor x_{n-1} \rfloor} + \lfloor x_{n-2} \rfloor \\ &\vdots \\ \Rightarrow r = r_0 &< [\lfloor x \rfloor, \lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor], \qquad (53)\\ R_n^{(e)}(x) &= [\lfloor x \rfloor, \lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor]. \end{aligned}$$

[12] of course assuming the conditions for definite success or failure for all the other cycles have failed

Likewise the condition (for definite failure) for n odd is

$$\begin{aligned} r_n &> \lfloor x_n \rfloor + 1 && (54) \\ &\vdots \\ \Rightarrow r = r_0 &< [\lfloor x \rfloor, \ldots, \lfloor x_{n-1} \rfloor, \lfloor x_n \rfloor + 1], && (55) \\ R_n^{(o)}(x) &= [\lfloor x \rfloor, \ldots, \lfloor x_{n-1} \rfloor, \lfloor x_n \rfloor + 1]. \end{aligned}$$

So both conditions take the form of continued fractions. Now pick some irrational x with continued fraction expansion $[a_0, a_1, \ldots]$. Then for even n, $R_n(x)$ is the rational number $[a_0, \ldots, a_n]$; and for odd n, $R_n(x) = [a_0, \ldots, a_{n-1}, a_n+1]$. We can decrease x by a very small amount (keeping it irrational) and $R_n(x)$ will not change. In fact, $R_n(x)$ will not change as long as $x > R_n(x)$. To see this, consider the fact that we can change an irrational number a little bit and not have its first $n+1$ continued fraction coefficients change. Or look at the triangles of Figure 3: the bottom edges of all the triangles are horizontal, so we can start on the bottom edge of any triangle and move to the left a little ways without changing $R_n(x)$.

Now (with $x = [a_0, \ldots]$ fixed as above) imagine taking

$$X_n(x) = \inf_{y \notin Q} \{y : R_n(y) = R_n(x)\} \tag{56}$$

. Note that two continued fractions of the same length are equal if and only if all their coefficients are equal.[13] So to find $X_n(x)$, we slowly, *continuously*, decrease y until some coefficient(s) of the continued fraction $R_n(y)$ change (recall that for $y = x$, $R_n(y) = [a_0, \ldots, a_n(+1)]$). Since we are continuously varying y and $R_n(y)$ is a monotonically increasing function of y, the change in the value of $R_n(y)$ must be the smallest one possible.[14] Thus, the change occurs in the last continued fraction coefficient, or the last two if changing the last one is impossible.

Let n be even, $R_n(x) = [a_0, \ldots, a_n]$. The value of a continued fraction is a (strictly) monotonically increasing function of its odd coefficients (eg, $a_0, a_2, \ldots$) and a (strictly) monotonically decreasing function of its even coefficients (eg, $a_1, a_3, \ldots$). As we cross the threshhold $X_n(x)$, the value of $R_n(y)$ decreases. If a_n is greater than 1, it will simply be reduced by 1. In this case, we will have $X_n(x) = R_n(x)$. To see this, write $y = [a_0, \ldots, a_{n-1}, b_n, b'_{n+1}]$ with b'_{n+1} some irrational number, the tail end of y. For $y = x$, we will have $b_n = a_n$, $b'_{n+1} = a'_{n+1}$. As we decrease y continuously but do not cross the threshhold, b_n must

[13] It is irrelevant whether or not their final coefficients are 1, since they must be of the same length.

[14] For this proof, we are not really interested in this change; but this observation is useful in further results.

not change and b'_{n+1} increases continuously. Our threshhold value is thus

$$\begin{aligned} X_n^{(e)}(x) &= \lim_{b'_{n+1}\to\infty}[a_0,\ldots,a_{n-1},a_n,b'_{n+1}] \\ &= [a_0,\ldots,a_n+\frac{1}{\infty}] \\ &= [a_0,\ldots,a_n] \\ &= R_n(x). \end{aligned} \tag{57}$$

Immediately on the other side of this threshhold (the limit in the other direction), $R_n(y)$ is $[a_0,\ldots,a_n-1]$ and y is $[a_0,\ldots,a_n-1,1']$, where $1'$ is a really a limit along irrationals greater than 1.

In the case that n is even and $a_n = 1$, we cannot simply decrease a_n by 1. Nevertheless, Equation 57 will still hold since, from the right, the same limiting process will determine y; the only way to decrease y without affecting its first $n+1$ coefficients is to increase b'_{n+1}. But on the other side of the threshhold what we get is

$$\begin{aligned} y &= \lim_{b'_n\to\infty}[a_0,\ldots,a_{n-1}+1,b'_n] \\ &= [a_0,\ldots,a_{n-1}+1] \\ &= [a_0,\ldots,a_{n-1},1]. \end{aligned}$$

Note that this implies that $R_n(y)$ changes infinitesimally across the threshhold; approaching the threshhold from the left, it takes on values $[a_0,\ldots,a_{n-1}+1,b]$ for infinitely large integers b.

Now let n be odd, $R_n(x) = [a_0,\ldots,a_{n-1},a_n+1]$. We use essentially the same techniques as with even n. With $y = [a_0,\ldots,b_n,b'_{n+1}]$ as above, we find the threshhold value by starting with $y = x$ and continuously decreasing y so that $R_n(y)$ does not change. This corresponds to continuously *decreasing* b'_{n+1} while keeping $b_n = a_n$ constant. Note that this means $b'_{n+1} > 1$, since when $b'_{n+1} \le 1$ we are effectively increasing the value of b_n. So the limit we want is

$$\begin{aligned} X_n^{(o)} &= \lim_{b'_{n+1}\to 1^+}[a_0,\ldots,a_n,b'_{n+1}] \\ &= [a_0,\ldots,a_n,1] \\ &= [a_0,\ldots,a_{n-1},a_n+1] \\ &= R_n(x), \end{aligned} \tag{58}$$

the same result we get in the even n case. We can also investigate values across the thresshold. On the right we have $R_n(y) = [a_0,\ldots,a_{n-1},a_n+1]$, and we want the smallest possible decrease in this, so on the left we will get $R_n(y) = [a_0,\ldots,a_{n-1},(a_n+1)+1]$ (we can always increase the last coefficient). The corresponding limit in y is

$$\lim_{b'_{n+1}\to\infty}[a_0,\ldots,a_{n-1},a_n+1,b'_{n+1}] = [a_0,\ldots,a_{n-1},a_n+1].$$

There is one more case that should be discussed. Suppose n is odd and consider $R_n(x) = [a_0, \ldots, a_{n-1}, 1]$. This cannot really happen, since the final coefficient should be 1 plus the corresponding coefficient of x, which is not 0. Nevertheless, we can think of this as a limit of $R_n = [a_0, \ldots, a_{n-1} + 1, b]$ as $b \to \infty$ along integers. Essentially, we are passing to the left through lots of threshhold values of the kind described in the preceding paragraph, spaced closer and closer together. As we continuously decrease $y = [a_0, \ldots, a_{n-2}, b_{n-1}, b'_n]$ so that $b_{n-1} = a_{n-1} + 1$ and $b'_n \to \infty$, we arrive at a limit

$$\begin{aligned} X &= [a_0, \ldots, a_{n-1} + 1, \infty] \\ &= [a_0, \ldots, a_{n-1} + 1] \\ &= [a_0, \ldots, a_{n-1}, 1]. \end{aligned}$$

X is a much "stronger" threshhold value than the infinitely many small ones crossed to get to it, because to its left we have $R_n(y) = [a_0, \ldots, a_{n-1}, 2]$, a significant change. (Taking the corresponding limit from the left is left to the reader.) Moreover, we do have $R_n(X) = X$, defined by a limit from the right. To see this, note that to get to X we considered $y = [a_0, \ldots, a_{n-2}, a_{n-1}+1, b'_n]$ with very large b'_n. As b'_n goes to infinity, $R_n(y) = [a_0, \ldots, a_{n-2}, a_{n-1} + 1, \lfloor b'_n \rfloor + 1]$ also approaches $[a_0, \ldots, a_{n-2}, a_{n-1} + 1] = [a_0, \ldots, a_{n-2}, a_{n-1}, 1]$, so

$$\lim_{y \to X^+} R_n(y) = X. \tag{59}$$

Before continuing with some more observations, we can finish the proof. We have shown that (for some n) every threshhold value X is a value for which $R_n(X) = X$ (definited by a limit). Let z be a rational number whose continued fraction has lengths n+1 and n+2 (with the final coefficient 1 in the latter case). If n is even, we can find an irrational number x whose first n+1 continued fraction coefficients are the same as those of z. Then $X_n(x) = z$ and z is a threshhold value, hence a fixed point. But we can also consider the continued fraction of length n+2 whose final coefficient is 1. When we consider $R_{n+1}(y)$, with y an irrational infinitesimally greater than x, we are in the situation described the last case examined above. Taking the limit as $y \to z$ we arrive at a threshhold value for which $R_{n+1}(z) = z$.

If n is odd and $z = [a_0, \ldots, a_{n-1}, a_n]$, we take an irrational number $x = [a_0, \ldots, a_{n-1}, \underline{a_n - 1}, b'_{n+1}]$ slightly larger than z. Then $X_n(x) = z$ and z must be a threshhold value and a fixed point. We can also consider the continued fraction of length n+2 and final coefficient 1 (now we are at the even case). We pick an irrational x slightly larger than z which has the same first n+2 coefficients as z, say $x = [a_0, \ldots, a_{n-1}, a_n - 1, 1, b'_{n+2}]$ for some irrational b'_{n+2} (much) greater than 1. Then $X_{n+1}(x) = z$.

So every irrational number with continued fraction expansions of lengths n+1 and n+2 is a threshhold value (hence a fixed point) of R_n and R_{n+1}. For reasons that will soon become apparent, these fixed points are somewhat special. We also want to show that if z has continued fractions of lengths n+1 and n+2

then it is a fixed point of R_m for any $m \geq n+2$. To this end we will show that $R_m(y) \to z$ as $y \to z$, y irrational (from either side).

Let $z = [a_0, \ldots, a_n]$, $a_n \neq 1$. Suppose n is even. Pick an irrational y a little larger than z such that $y = [a_0, \ldots, a_n, b_{n+1}, \ldots, b_m, b'_{m+1}]$, with b'_{m+1} irrational greater than 1. We have $R_m(y) = [a_0, \ldots, a_n, b_{n+1}, \ldots, b_m(+1)]$, where the $(+1)$ is used if m is odd. As y continuously approaches z, the first $n+1$ coefficients of y cannot change, but the tail end $b'_{n+1} = [b_{n+1}, \ldots]$ will go to infinity, since

$$\lim_{y \to z^+} y = \lim_{b'_{n+1} \to \infty} [a_0, \ldots, a_n + \tfrac{1}{b'_{n+1}}] = \lim_{b'_{n+1} \to \infty} [a_0, \ldots, a_n, b'_{n+1}].$$

Therefore, with $b = [b_{n+1}, \ldots, b_m(+1)]$, $y \to z^+$ will imply that $b \to \infty$ (note that the $(+1)$ cannot have any fundamental effect on the entire tail end going to infinity), and we will have

$$\begin{aligned} \lim_{y \to z^+} R_m(y) &= lim_{b \to \infty} [a_0, \ldots, a_n, b] \\ &= \lim_{b \to \infty} [a_0, \ldots, a_n + \tfrac{1}{b}] \\ &= [a_0, \ldots, a_n] \\ &= z. \end{aligned} \tag{60}$$

We can also look at the limit from the left. In this case, we pick y a little less than z, of the form $y = [a_0, \ldots, a_n - 1, b'_{n+1}]$ so that the irrational tail end b'_{n+1} is very close to 1^+. This is the same as writing $y = [a_0, \ldots, a_n - 1, 1, b'_{n+2}]$ with b'_{n+2} irrational and tending to infinity. We will have $R_m(y) = [a_0, \ldots, a_n - 1, 1, \ldots, b_m(+1)]$ and

$$\begin{aligned} y \to z^- &\Rightarrow b'_{n+2} \to \infty \\ &\Rightarrow [b_{n+2}, \ldots, b_m(+1)] \to \infty \ ^{15} \\ &\Rightarrow R_m(y) \to [a_0, \ldots, a_n - 1, 1] \\ &\quad = z. \end{aligned}$$

We can also quickly consider the case of n odd, $z = [a_0, \ldots, a_n]$ with $a_n \neq 1$. If we take y a little larger than z, we have $y = [a_0, \ldots, a_n - 1, 1, b'_{n+2}]$ with b_{n+2} large irrational. Then $R_m(y) = [a_0, \ldots, a_n - 1, 1, b_{n+2}, \ldots, b_m(+1)]$ (where perhaps $m = n+2$). Since $b'_{n+2} = [b_{n+2}, \ldots] \to \infty$ implies $b = [b_{n+2}, \ldots, b_m(+1)] \to \infty$ and the former occurs when $y \to z^+$,

$$\begin{aligned} \lim_{y \to z^+} R_m(y) &= \lim_{b \to \infty} [a_0, \ldots, a_n - 1, 1, b] \\ &= \lim_{b \to \infty} [a_0, \ldots, a_n - 1, 1 + \frac{1}{b}] \\ &= [a_0, \ldots, a_n - 1, 1] \\ &= [a_0, \ldots, a_n] = z. \end{aligned} \tag{61}$$

Likewise, we can take y a little less than z, say $y = [a_0, \ldots, a_n, b'_{n+1}]$, with $b'_{n+1} = [b_{n+1}, \ldots]$ large and irrational. Then $y \to z^-$ corresponds to $b'_{n+1} \to \infty$,

which implies $b = [b_{n+1}, \ldots, b_m(+1)] \to \infty$, and

$$\begin{aligned} \lim_{y \to z^-} R_m(y) &= \lim_{b \to \infty} [a_0, \ldots, a_n, b] \\ &= \lim_{b \to \infty} [a_0, \ldots, a_n + \frac{1}{b}] \\ &= [a_0, \ldots, a_n] = z. \end{aligned} \tag{62}$$

Combined with previous results, this establishes that z is a fixed point of R_n whenever its continued fraction can be written to have at most $n+1$ coefficients. One direction of the proposition is finished. Conversely, we would like to show that (given n) all the fixed points of R_n are rational numbers whose continued fractions can be written to have at most $n+1$ coefficients. This is much easier. For suppose $z = [a_0, \ldots, a'_{n+1}]$ with a'_{n+1} some real number strictly greater than 1 (so z is either irrational or rational with a continued fraction of at least $n+2$ coefficients). Then we know that $R_n(z) = [a_0, \ldots, a_n(+1)]$, a continued fraction of length $n+1$. And the only way this could equal z, a continued fraction of length $\geq n+2$, is if we have $a'_{n+1} = 1$, which is not true. So z cannot be a fixed point of R_n. $\diamondsuit$

Now consider Figure 3 in light of this proof (in fact this discussion is concerned with the plot in which $R_n(x)$ is drawn for *all* n, but Figure 3 will do for a visual aid). We have essentially derived its entire structure. We showed that every threshhold value, as defined in the cases that were discussed,[16] is also a fixed point. Since the fixed points of R_n are all the rational numbers whose continued fractions can be of length $\leq n+1$, these are the only numbers that can be threshhold values. But we also showed that if z has a continued fraction of length $\leq n$-1 then $\lim_{y \to z} R_n(y) = z$. So R_n is continuous at such fixed points and they are not threshhold values. Therefore,

Corrolary 7 *Summary of threshhold values:*

- *The threshhold values of R_n are precisely the rational numbers that have continued fractions of minimum lengths n or $n+1$.*
- *A rational number whose continued fraction has minimum length $n+1$ is a threshhold value for R_n and R_{n+1}.*
- *If a number is a threshhold value for R_n but not for R_{n-1} then its continued fraction has minimum length $n+1$.*

Figure 3 is entirely characterized by the threshhold values of the R_n and the magnitudes of the jump discontinuities that occur, since the R_n are otherwise constant functions. Let an n-triangle refer to a triangle drawn by R_n. Note how the last case discussed in the section on threshholds, n odd and

[16] essentially a point where R_n has a jump discontinuity

$X = [a_0, \ldots, a_{n-1}, 1]$, corresponds to R_n approaching[17] the diagonal as it moves leftwards towards the lower corner of an (n-1)-triangle and then jumping down at the beginning of the next (n-1)-triangle. We can also see that the case n even, $X = [a_0, \ldots, a_{n-1}, 1]$, corresponds to R_n smoothly approaching the diagonal as it moves rightwards towards the upper corner of an (n-1)-triangle and then being constant in the next (n-1)-triangle.[18] The other two cases, where $X = [a_0, \ldots, a_n]$ and $a_n \neq 1$ for n even or odd, correspond to R_n being constant (leftwards) up to the diagonal and then jumping to another constant value.

That each rational number is also a threshhold value for exactly two R_k can also be seen in Figure 3 for a few threshold values with short continued fractions. If $X = [a_0, \ldots, a_n] = [a_0, \ldots, a_n - 1, 1]$ and n is even, then going leftwards R_n jumps from $[a_0, \ldots, a_n]$ to $[a_0, \ldots, a_n - 1]$ and R_{n+1} approaches horizontally and leaves in infinitesimally small triangles. Note that in this case we can also see that moving rightwards from the threshhold R_n will jump to $[a_0, \ldots, a_n + 1]$ at $[a_0, \ldots, a_n + 1]$ while R_{n+1} will jump much sooner, to $[[a_0, \ldots, a_n - 1, 2]$ at $[a_0, \ldots, a_n - 1, 2]$. If n is odd then the situation is essentially reversed. Moving leftwards, R_n approaches horizontally and jumps from $[a_0, \ldots, a_n]$ down to $[a_0, \ldots, a_n + 1]$, while R_{n+1} approaches in infinitesimally small triangles and jumps much less to $[a_0, \ldots, a_n - 1, 2]$.

This should explain much of what is going on in the plot. And now Figure 3 itself can tell us about the location of rational numbers with continued fractions of certain minumum lengths. By considering the third part of Corrolary 7, we immediately see that the only numbers that have minimum continued fractions of length 2 are of the form $1/n$,[19] with m an integer. To actually prove this, we can use the fact that the right threshhold of the 0-triangle (the entire section below the diagonal) is $[1] = [0, 1]$. To get the first "1-threshhold", we add 1 to the last continued fraction digit to get $[0, 2] = 1/2$. We continue in this way and get that $[0, n] = 1/n$ is a threshhold of R_1 (but not of "R_0", the outline of the 0-triangle) for all $n \geq 2$. Since these are the only numbers generated and cover the entire interval they are the only numbers with continued fractions of minimum length 2 (yes, this is a rather obvious conclusion).

We can then find the numbers with continued fractions of minimum length 3 simply by looking at R_2. To actually find their formulas, we note that 2 is even[20] and that the left threshholds of all the 1-triangles are of the form $[0, n] = [0, n-1, 1]$, $n \geq 2$. So we move rightwards from each of these threshholds and find numbers with continued fractions of minimum length 3 are of the form

$$[0, n-1, m] = \frac{m}{(n-1)m + 1} \tag{63}$$

[17] "approaching" as in not being a horizontal line up to the diagonal but actually approaching it through infinitely many infinitesimally small triangles

[18] If we define threshholds as jump discontinuities, this isn't technically a threshhold; but it makes sense to call it one and inner consistency is preserved if we do.

[19] We are of course looking at everything (mod 1). By now it should be more than clear why we can do this.

[20] surprise!

for $n, m \geq 2$. Continuing this way, we get that all numbers with continued fractions of minimum length $k+1$ are of the form

$$[0, n_1, n_2, \ldots, n_k], \tag{64}$$

with $n_k \geq 2$ and $n_i \geq 1 \ \forall i \neq k$. This is of course entirely obvious, just by a consideration of what the continued fraction coefficients could be. But it is very nice that we got this conclusion from the graph. And it is even more exciting that we can now visualize the locations of the numbers with continued fractions of a certain minimum length–we can think of their coefficients as indices describing which 1-triangle, 2-triangle, etc they belong to! For example, [0,2,3,1,5] is in the 2nd 1-triangle from the right, the 3rd 2-triangle from the left inside that 1-triangle, and the 1st 3-triangle from the right inside that 2-triangle. Inside the 3-triangle, it is the 4th 4-threshhold from the left.

Now let's return to probabilities.

2.3.2 Improved probability bounds

Proposition 3 *Given a point $(\xi - \lfloor \xi \rfloor, r - \lfloor \xi \rfloor)$ randomly distributed below the diagonal of the unit square, the probability that the algorithm will fail is bounded by*

$$0.7101 \leq P(failure) \leq 0.7609.$$

This of course implies that the probability of success is bounded by

$$0.2391 \leq P(success) \leq 0.2899.$$

Proof. For the *exact* probabilities, we would consider $R_n(x)$ for all n. Recall that if n is odd than points (x, y) below $R_n(x)$ but above any other $R_m(x)$ with $m < n$ correspond to definite failure of the algorithm with $\xi - \lfloor \xi \rfloor = x$ and $r - \lfloor \xi \rfloor = r$ (as usual, we consider everything (mod 1)). Likewise, if n is even, such points correspond to definite success of the algorithm. Note that defining $R_0(x) \equiv 0$ goes along with this–if a point is below R_0 than $(3'')$ is no longer violated. Looking at the interval (0,1), i.e. a plot such as Figure 3, the probability of failure is 2 times the area of the regions of definite failure and the probability of success is 2 times the area of the regions of definite success. We multiply by two because we are for the moment ignoring the top half (triangle) of the graph; we assumes that the root r violates $(3'')$, so it is definitely located on the bottom half of the graph.

Though at the moment we are not going to find exact probabilities, we can imagine how we would go about doing so. We can find a lower bound on probability of failure from the R_1, a lower bound on probability of success from R_2, and so on. Since lower bounds for success correspond to upper bounds for failure, we would get two sequences, $\{P_n(failure)\}$ and $\{1 - P_n(success)\}$, that converge monotonically to the same limit from below and above. This limit is of course the exact probability of failure.

For the first probability of failure, we can subdivide the are under R_1 (see Figure 1) into rectangles. Since we know the fixed points are at $1/n$, n is an integer, the area we want is

$$\begin{aligned}
P_1(failure) &= 2\left[\sum base \times height\right] \\
&= 2\left[\frac{1}{2}\left(\frac{1}{2}\right) + \left(\frac{1}{2}-\frac{1}{3}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}-\frac{1}{4}\right)\left(\frac{1}{4}\right) + \cdots\right] \\
&= 2\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)\left(\frac{1}{n+1}\right) \\
&= 2\left[\sum_{n=1}^{\infty}\frac{1}{n(n+1)} - \sum_{n=1}^{\infty}\frac{1}{(n+1)^2}\right] \\
&= 2\left[\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right) - \left(\frac{\pi^2}{6}-1\right)\right] \\
&= 2\left(2-\frac{\pi^2}{6}\right) = 4-\frac{\pi^2}{3} \qquad (65) \\
&\approx 0.7101\ .
\end{aligned}$$

Now we want the first bound on the probability of success, twice the area between R_2 and R_1. We know the fixed points are $m/((n-1)m+1)$ for integral m, n. In the (n-1)st 1-triangle, the area is

$$\begin{aligned}
A_n^2 &= \sum[base \times height] \\
&= \sum_{m=2}^{\infty}\left(\frac{m+1}{(n-1)(m+1)+1} - \frac{m}{(n-1)m+1}\right)\left(\frac{m}{(n-1)m+1} - \frac{1}{n}\right) \\
&= \sum_{m=2}^{\infty}\frac{m-1}{n((n-1)m+1)^2(m(n-1)+n)}, \qquad (66)
\end{aligned}$$

so that

$$P_2(success) = 2\sum_{n=1}^{\infty} A_n^2.$$

Since we know what the area under R_1 is, we could also just calculate the are under R_2 and subtract that under R_1:

$$\begin{aligned}
Area\ under\ R_2 &= \sum_{n=2}^{\infty}\sum_{m=1}^{\infty}\left(\frac{m+1}{(n-1)(m+1)+1} - \frac{m}{(n-1)m+1}\right)\left(\frac{m}{(n-1)m+1}\right) \\
&= \sum_{n=2}^{\infty}\sum_{m=2}^{\infty}\frac{m}{((n-1)m+1)^2(m(n-1)+n)}, \\
P_2(success) &= 2\left[\sum_{n=2}^{\infty}\sum_{m=2}^{\infty}\frac{m}{((n-1)m+1)^2(m(n-1)+n)} - \left(2-\frac{\pi^2}{6}\right)\right].
\end{aligned}$$

Unfortunately, there seems to be no easy way to explicitly evaluate this sum. Looking at what the terms refer to in the plot, we might expect the sum to converge fairly quickly. Unfortunately, this is not the case. A glance at the summand shows it is on the order of $1/m$. And if we call the summand in (66) $C(n,m)$, we have

$$\begin{aligned}
\sum_{n=2}^{25}\sum_{m=2}^{25} C(m,n) &\approx 0.1008 \\
\sum_{n=2}^{50}\sum_{m=2}^{25} C(m,n) &\approx 0.1102 \\
\sum_{n=2}^{100}\sum_{m=2}^{100} C(m,n) &\approx 0.1153 \\
\sum_{n=2}^{200}\sum_{m=2}^{200} C(m,n) &\approx 0.1179,
\end{aligned}$$

which shows that the tail end is still contributing significantly. *Mathematica* will not evaluate the infinite sum numerically. (Though we do know that the sum must *somehow* converge, since it is bounded from above–it can only be a finite area.) The best result that could be achieved in a reasonable calculating time[21] was

$$\sum_{n=2}^{500}\sum_{m=2}^{500} C(m,n) \approx 0.1196.$$

We might try to integrate $R_2(x)$ using *Mathematica*'s numerical integration algorithms, which give

$$\int_0^1 R_2(x)\,dx - \left(2 - \frac{\pi^2}{6}\right) \approx 0.1207,$$

but which also produced quite a few integral convergence errors.[22]

Using the sum from 2 to 500, we know that $P_2(\text{success}) \geq 2{*}0.1196 = 0.2392$, which, combined with the result from R_1, gives us the bounds

$$0.7101 \leq P(failure) \leq 1 - 0.2392 = 0.7609, \tag{67}$$

the assertion of the Proposition. $\diamondsuit$

Achieving better bounds is on one hand straightforward–we can always write out the sum–and on the other hand very difficult because the resulting sums cannot be easily evaluated. By using *Mathematica* to integrate the first ten R_n,

[21] about 2 hours on my PC

[22] Though I believe the integration route is in fact decently accurate, and certainly a better way to go than approximating the sums.

we obtained the following *estimate*[23]:

$$0.7498 < P(failure) < 0.7499 \quad or \quad P(failure) \approx 0.750 \tag{68}$$
$$0.2500 < P(success) < 0.2502 \quad or \quad P(success) \approx 0.250 \tag{69}$$

These numbers are tantalizingly close to 1/4 and 3/4, so we might say that

Conjecture 1 *$P(failure) = 3/4$ and $P(success) = 1/4$.*

It would be great if this were actually proven.[24]

Note that all these calculations can be found and rerun at the bottom of the notebook rless.nb.

Also note that we know now that the interiors of each (even or odd) triangle all have the same structure but no two are similar in the strict sense of the word. This was not actually proved explicitly, but when we consider the general form of threshhold values of R_n (i.e., the general form of a continued fraction of length n+1), we see that there are no factors of previous indices that can be factored out. (This answers a question asked right before section 2.3.1)

2.3.3 Other roots

We have spent a good deal of effort investigating success and failure of the algorithm as a function of a *single* root r of the polynomial less than the sought root ξ. The situation is not greatly complicated by multiple roots less than ξ which violate $(3'')$. Each one individually must satisfy all the conditions mentioned previously–i.e. each one must be in a region of success on the plot in order for the algorithm to succeed. Using the results of Proposition 3, we can say that for k roots that violate $(3'')$ we will have

$$(0.2391)^k \leq P^k(success) \leq (0.2899)^k \tag{70}$$
$$1 - (0.2899)^k \leq P^k(failure) \leq 1 - (0.2391)^k. \tag{71}$$

Of course we can also conjecture that

$$P^k(success) = (1/4)^k \tag{72}$$
$$P^k(failure) = 1 - (1/4)^k. \tag{73}$$

We have also not discussed roots greater than the sought root ξ, i.e. roots for which $(4'')$ is applicable. The calculations are almost identical to those used for roots that violate $(3'')$, so for the most part they will be suppressed and various results will be given without complete (or any) proof.

Let r be the only root of the polynomial greater than ξ. Let $x{=}\lfloor\xi\rfloor$ and define ξ_n, x_n, and r_n by equations 50 and 51; note that we have $x_n = \xi_n$ for $n \geq 1$. If $(4'')$ is satisfied, we have definite success, and to satisfy $(4'')$ we need

$$r_1 < \lfloor\xi_1\rfloor$$
$$\Rightarrow r > \tfrac{1}{\lfloor\xi_1\rfloor} + \lfloor\xi\rfloor = [\lfloor\xi\rfloor, \lfloor\xi_1\rfloor].$$

[23] *Mathematica*'s integration algorithms cannot actually prove anything!

[24] In fact, see Section 4.1 for a proof, done later.

Therefore, we can define $Q_1(\xi) = [\lfloor \xi \rfloor, \lfloor \xi_1 \rfloor]$ or

$$Q_1(x) = [\lfloor x \rfloor, \lfloor x_1 \rfloor] = [0, \lfloor x_1 \rfloor]$$

so that if $y = r - \lfloor \xi \rfloor$ and $y > Q_1(x)$ we will have definite success.

We continue like this. For any odd n we get

$$Q_n(x) = [\lfloor x \rfloor, \lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor]. \tag{74}$$

For any even n, we will have $r_n > x_n$. The condition for definite failure (given that all the previous conditions for definite success or failure have failed) will be $r_n > \lfloor x_n \rfloor + 1$. Therefore, we get

$$Q_n(x) = [\lfloor x \rfloor, \lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor + 1]. \tag{75}$$

For definite failure in the even case, we must have $y > Q_n x$. Notice that the exact opposite happens with the $(+1)$ compared to the situation when r was less than ξ. The resulting plot[25] for the first five conditions appears in Figure 4. The conditions for r less than ξ are included below the diagonal in the bottom part.

All the results concerning the continued fraction expansion of x and properties of the R_n still hold for the Q_n. The proofs are almost identical, the main exception being that $Q_n(x)$, x rational, is defined by $\lim_{y \to \underline{x^-}} Q_n(y)$. We have:

Proposition 4 *The following results hold for $Q_n(x)$:*

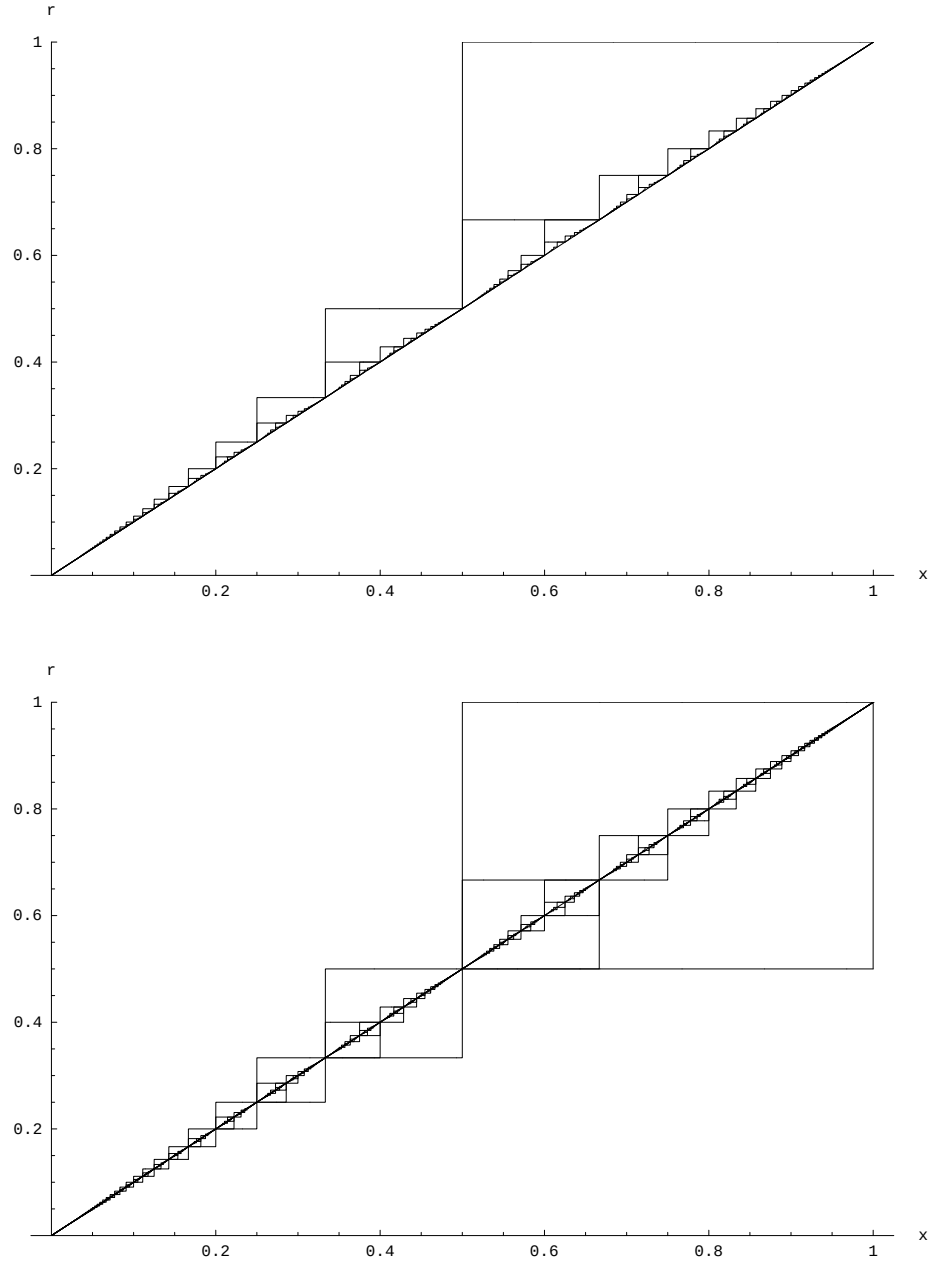
- *$Q_n(x) = x$ if and only if the continued fraction expansion of x has $\leq n+1$ coefficients*
- *The set of numbers x for which $Q_n(x) = x$ (for some n) is precisely the set of rational numbers*
- *The threshhold values of Q_n are precisely the rational numbers that have continued fractions of minimum lengths n or $n+1$.*
- *A rational number whose continued fraction has minimum length $n+1$ is a threshhold value for Q_n and Q_{n+1}.*
- *If a number is a threshhold value for Q_n but not for Q_{n-1} then its continued fraction has minimum length $n+1$.*

And the Q_n can be used to visualize the continued fraction expansion of rational numbers the same way as the R_n.

The plot of the Q_n indicates that the Q_n are in a sense inverse functions of the R_n, their reflections across the diagonal. This in fact follows from the fact that Q_n and R_n have the same threshhold values and all the threshhold values are fixed points. In a given step, R_n must start at the diagonal (say the point (x_0, x_0)) and move (horizontally) to the right until it jumps up to the

[25] produced at the bottom of rless.nb

Figure 4: r greater than ξ



next step, which also starts at the diagonal. So the length of the jump is equal to the length of the step. But Q_n has a fixed point at the jump since it has the same fixed points as R_n; and from there Q_n moves horizontally to the left (note the different definition of $Q_n(x)$ for rational x) until it jumps down to its next step. But this jump must occur at the first threshhold value Q_n hits, and since its threshhold values are the same as those of R_n it must jump at x_0 and we are back where we started. Since all the threshhold values of Q_n are fixed points, the length of this jump must have been the length of the step–equal to the length of the step and jump of R_n. We have traced out a square and shown that Q_n must be the reflection or R_n.

As far as probabilities are concerned, there is definite success above every odd Q_n (but below all the others) and definite failure above every even Q_n (below all the others). In a sense we can say that success and failure invert when they are reflected across the diagonal. Therefore, given a point (x, y)=$(\xi - \lfloor\xi\rfloor, r - \lfloor\xi\rfloor)$ randomly distributed above the diagonal of the unit square, the bound on probability for success and failure of the algorithm are exactly the opposite of the bounds for a point below the diagonal. Hence we know

$$0.7101 \leq P(success) \leq 0.7609 \tag{76}$$

$$0.2391 \leq P(failure) \leq 0.2899 \tag{77}$$

and we can conjecture that

$$P(success) = 3/4, \quad P(failure) = 1/4. \tag{78}$$

Given k points randomly distributed in the unit square–essentially k roots distributed[26] in the interval $[\lfloor\xi\rfloor, \lfloor\xi\rfloor+1)$–we simply combine the results of R_n and Q_n to get bounds for probabilities of success and failure. For example, the conjectured probability values would predict[27]

$$\begin{aligned} P(success) &= \frac{1}{2^k}\left[\left(\frac{3}{4}\right)^k + \binom{k}{k-1}\left[\left(\frac{3}{4}\right)^{k-1} + \left(\frac{1}{4}\right)^1\right] + \cdots \right. \\ &\quad \left. + \binom{k}{0}\left(\frac{1}{4}\right)^k\right] \\ &\quad P(failure) = 1 - P(success). \end{aligned} \tag{79}$$

As a final remark, we now know there is no way to reformulate $(3'')$ and $(4'')$ to make them sufficient *and* necessary for success of the agorithm.

2.4 A possible practical fix

We have shown in quite some detail that the Lang-Trotter algorithm will not work on any given irrational root of a random polynomial–the other roots surrounding it are always a potential problem. But why, for practical purposes,

[26] Perhaps not entirely randomly? Not completely sure at the moment.

[27] check this...

could we not adjust the initial polynomial $p_0(x)$ so that it satisfied $(3'')$ and $(4'')$, which *are* sufficient for success?

Two solutions immediately come to mind. We might scale the polynomial $p_0(x)$ so that there are no other roots within an integer of the sought root ξ. To see how this would work, let $\{r_j\}$ be the roots of $p_0(x)$ not equal to ξ and take $\delta = \min |\xi - r_j|$. Since the roots of the polynomial $\tilde{p}_0(x) = p_0(\frac{x}{a})$ are a times the roots of $p_0(x)$, the spacings between the roots of this scaled polynomial will be a times the spacings of the roots of $p_0(x)$. If we take any $a > \frac{1}{\delta}$, the minimum spacing in $\tilde{p}_0(x)$ will be $a\delta > 1$, and the polynomial will satisfy $(3')$.

Another, slightly trickier, solution is to shift (translate) $p_0(x)$ by some number b. The roots of $\hat{p}_0(x) = p_0(x + b)$ are the roots of $p_0(x)$ minus b. If $(3'')$ and $(4'')$ are not satisfied, there is no way to pick a b to satisfy $(3')$; so the best we can hope for is a b that satisfies $(3'')$ and $(4'')$. Let r_1 and r_2, $r_1 < \xi < r_2$, be the roots of $p_0(x)$ closest to ξ. (Certainly one or the other may not exist, in which case they can be removed from the following argument.) Since we are essentially looking at things mod 1, we may assume that $\lfloor \xi \rfloor$ doesn't change; so

$$b < \xi - \lfloor \xi \rfloor. \tag{80}$$

To satisfy $(3'')$, we need $r_1 < \lfloor \xi \rfloor$. If $(3'')$ is already satisfied, there is no problem; but if not we want to pick a b such that

$$\begin{aligned} r_1 - b &< \lfloor \xi - b \rfloor = \lfloor \xi \rfloor \\ \Rightarrow b &> r_1 - \lfloor \xi \rfloor. \end{aligned} \tag{81}$$

We also want to satisfy $(4'')$, for which we need

$$\frac{1}{(r_2 - b) - \lfloor \xi \rfloor} < \lfloor \frac{1}{(\xi - b) - \lfloor \xi \rfloor} \rfloor. \tag{82}$$

As b approaches $\xi - \lfloor \xi \rfloor$, the RHS goes to infinity while the left hand side remains finite, so finding a b that satisfies (82) is always possible. Our problem, then, is finding the loosest possible constraint on b that will ensure (82); unfortunately, since b is inside the greatest integer function on the RHS, there is no simple solution. Three sufficient lower bounds on b will thus be given. Let $\rho = r_2 - \lfloor \xi \rfloor$ and $x = \xi - \lfloor \xi \rfloor$. If $b > 0$ (which will be the case if we need to satisfy $(3'')$) then $0 < \rho - b < 1$ and it will be sufficient to satisfy

$$\begin{aligned} \frac{1}{x - b} &> \frac{2}{\rho - b} \\ \Rightarrow \rho - b &> 2x - 2b \\ \Rightarrow b &> 2x - \rho \\ \Rightarrow b &> 2\xi - r_2 - \lfloor \xi \rfloor. \end{aligned} \tag{83}$$

For a better (though still not exact) bound we could also take

$$\begin{aligned} \frac{1}{x - b} &> \frac{1}{\rho - b} + 1 \\ \Rightarrow b^2 - (x + \rho)b + x\rho + x - \rho &< 0 \end{aligned}$$

Since the leading coefficient of this quadratic is positive, in the solution we must have b between the two roots, which are

$$b = \frac{\rho + x \pm \sqrt{(\rho - x)^2 + 4(\rho - x)}}{2}.$$

Taking into account the constraint in (80), this condition reduces to

$$\begin{aligned} b &> \frac{\rho + x - \sqrt{(\rho - x)^2 + 4(\rho - x)}}{2} \\ \Rightarrow b &> \frac{\xi + r_2 - 2\lfloor \xi \rfloor - \sqrt{(r_2 - \xi)^2 + 4(r_2 - \xi)}}{2} \end{aligned} \tag{84}$$

While this *is* a looser constraint on b, the first constraint is much nicer to work with.

As a final option, consider the fact that if $b > 0$ we will have $x - b < x$, so that $\lfloor \frac{1}{x} \rfloor \leq \lfloor \frac{1}{x-b} \rfloor$. Then to satisfy (82) it suffices to have

$$\begin{aligned} \frac{1}{\rho - b} &< \left\lfloor \frac{1}{x} \right\rfloor \\ \Rightarrow b &< \rho - \left\lfloor \frac{1}{x} \right\rfloor^{-1} \\ &= \rho - Q_1(x) \\ &= r_2 - \lfloor \xi \rfloor - \left\lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \right\rfloor^{-1}. \end{aligned} \tag{85}$$

Unfortunately, as can be seen from the definition in terms of Q_1, this condition may force b to be negative, thereby contradicting itself. We will therefore focus on the first two conditions for the time being.

To summarize our results for shifts by $-b$:

General constraint	$b < \xi - \lfloor \xi \rfloor$
$(3'')$ violated, $r_1 \geq \lfloor \xi \rfloor$	$b > r_1 - \lfloor \xi \rfloor$
$(4'')$ violated, $\frac{1}{r_2 - \lfloor \xi \rfloor} \geq \lfloor \frac{1}{\xi - \lfloor \xi \rfloor} \rfloor$	$b > \frac{1}{2}\left(\xi + r_2 - 2\lfloor \xi \rfloor - \sqrt{(r_2 - \xi)^2 + 4(r_2 - \xi)}\right)$
$(4'')$ violated and $b > 0$	$b > 2\xi - r_2 - \lfloor \xi \rfloor$

We should check that these constraints are always (jointly) attainable. If the only problematic roots are less than ξ, we can certainly have both (80) and (81), since we have $\lfloor \xi \rfloor < r_1 < \xi$. Now suppose the only problematic roots are greater than ξ and (80) holds. Then we have (with $r = r_2 - \lfloor \xi \rfloor$)

$$\begin{aligned} &(r - x)^2 + 4(r - x) > (r - x)^2 \\ \Rightarrow &\sqrt{(r - x)^2 + 4(r - x)} > r - x \\ \Rightarrow &r - \sqrt{(r - x)^2 + 4(r - x)} < x \\ \Rightarrow &x + r - \sqrt{(r - x)^2 + 4(r - x)} < 2x \\ \Rightarrow &1/2\big(x + r - \sqrt{(r - x)^2 + 4(r - x)}\big) < x, \end{aligned}$$

so we will always be able to apply (84) in conjunction with (80). And since we have $x > 0$ and $r > x \Rightarrow 2x - r < x$ we see that we will also be able to apply either $b > 0$ or (83), whichever is more restrictive, in conjunction with (80). Finally, suppose that there are problematic roots on both sides of ξ. Then the condition on b is simply a combination of (81) and either (83) or (84). Since all of these additional conditions bound b from below and we can apply all of them individually, we can apply all of them together.

2.4.1 Adding and multiplying continued fractions

Now we know that either scaling or a shift will "fix" a polynomial so that we can use the algorithm on an *adjusted* root $\tilde{\xi}$. But is this truly useful? The answer depend on what we need the continued fraction expansion of ξ for. If need to be able to write ξ to very high accuracy (i.e. the accuracy given by a great deal of continued fraction coefficients) than transforming the polynomial is not much of a problem. Scaling might be slightly awkward, since we would find the expansion of $\tilde{\xi} = a\xi$ and then have to divide by a; but a translation by a rational number would not be bad at all–we would just b to the accurate expression of $\tilde{\xi}$.

On the other hand, what if we actually need the exact continued fraction coefficients of ξ, say for a statistical analysis or some other test–can we get them back? Just how significantly will multiplying by or adding a constant affect a continued fraction? Multiplying or adding continued fractions is very difficult and entirely nontrivial; no general answer to the question is known. Multiplying or shifting by a rational number seems somewhat less disastrous than multiplying or shifting by an irrational, though both might cause irrepairable damage. In the case of a root of a quadratic, we can say that multiplying or translating by a rational will still give a root of a quadratic, so the resulting continued fraction will still be periodic; yet it is unclear how to directly get one continued fraction from the other or how the period will change. And what if we have a number like e, with a very nice linearly periodic continued fraction.[28] What will happen to the continued fraction of $e + 1/2$?

Thus arose the question of rational shifts or scaling of continued fractions, the topic which we shall pursue for the remainder of this paper now that we have put to rest most of the burning questions about the Lang-Trotter algorithm. In fact, we shall limit ourselves to the effects of rational multiplication and translation of linearly periodic continued fractions (and then primarily the latter) since such a nice family seems an excellent place to begin an investigation.

3 Linearly Periodic Continued Fractions

It turns out that $e + 1/2$ also has a linearly periodic continued fraction which is just slightly more complex than the one for e. In fact, it seems that any

[28] $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, ...] = [2, \overline{1, 2n, 1}]$

linearly periodic continued fraction retains its linear periodicity under a rational scaling or shift, though no proof of this has yet been found. In order to actually quantify effects observed, we shall need to say a bit more about linearly periodic continued fractions in general.

3.1 More terminology

Since we shall be discussing linearly periodic continued fractions a great deal and the name is quite lengthy, they shall be referred to as LPCF's from here on.

Recall equation 4, which defined an LPCF to be of the form

$$[a_0, \ldots, a_{l-1}, \overline{f_1(n), f_2(n), \ldots, f_j(n)}], \qquad n = 1, 2, 3, \ldots. \tag{86}$$

For each f_i we have $f_i(n) = b_i n + c_i$, with b_i and c_i integers and $c_i > -b_i$. If all the b_i are zero, than the continued fraction is an ordinary periodic one.

The **introductory sequence** of the LPCF in (86) is $(a_0, \ldots, a_{l-1})$ and has length l. In an LPCF, the introductory sequence is chosen to be as short as possible–it is the shortest possible sequence that cannot be included in the periodic rule.

The **period length** of the LPCF is j. Within the periodic sequence $(f_1(n), f_2(n), \ldots, f_j(n))$, we find two kinds of functions, f_i with $b_i = 0$ and f_i with $b_i \neq 0$. The former form the **base** or base sequence of the LPCF, which can simply be written as $(c_{i_1}, c_{i_2}, \ldots, c_{i_m})$, where m is the length of the base sequence. The latter form the **diagonals** of the LPCF. There is one diagonal for every unique value of $b_i \neq 0$, and b_i is called the slope of that diagonal (corresponding to how much the diagonal will increase per period). We can then talk about the length or number of points in a diagonal of slope b as the number of f_i with $b_i = b$. The **displacement** of these points is c_i. The diagonal with the lowest slope may often be referred to as the "first diagonal" or the "base diagonal."

Let's consider an example,

$$\begin{aligned}\tan(1) + 1/2 = [2, 17, 2, \overline{2, 1, 3n-2, 2, 12n-2,} \\ \overline{2, 3n-1, 1, 2, 1, 3n-1, 1, 48n+48, 1, 3n, 1}].\end{aligned}$$

The introductory sequence has length 3 and the period length is 16. The base sequence is$(2, 1, 2, 2, 1, 2, 1, 1, 1, 1)$. There are three diagonals, of slopes 3, 12, and 48. The first diagonal has four points (with displacements -2,-1,-1, and 0) and the other two have one point each.

3.2 A set of measure 0

By the results of the first section, we know that every LPCF is irrational, since every LPCF is infinite. So the LPCF's are a subset of the irrational numbers. But we also know that no LPCF will satisfy Kuzmin's Theorem, so in fact this set must have measure zero (is countably infinite). Here we give a much better proof that

Proposition 5 *The set of linearly periodic continued fractions has measure zero.*

Proof. First, note that the direct product of a finite number of countable infinite sets is also countable infinite. To see this, let $S_1, \ldots, S_n$ countable infinite sets and enumerate their elements: $S_i = \{s_1^i, s_2^i, \ldots\}$. Then there is a 1-1 correspondence between elements of $S = S_1 \times \cdots \times S_n$ and lattice points with positive coordinates of n-dimensional Euclidean space, namely

$$(s_{a_1}^1, s_{a_2}^2, \ldots, s_{a_n}^n) \longleftrightarrow (a_1, a_2, \ldots, a_n).$$

We can then count the elements s of S by first counting the finite number of elements with $|s| \leq 1$, then those with $1 < |s| \leq 2$, and so on. Thus, S is an infinitely countable set.

Also note that the union of finitely many countable sets is again countable. For if we set $S = \cup_{i=1}^n S_i$ with the S_i countable and enumerate the elements of the S_i as $\{a_1^i, a_2^i, \ldots\}$, we can count the elements of S by first counting the n $a_1^1, \ldots, a_1^n$ then the n $a_2^1, \ldots, a_2^n$, and so on.

Now, an LPCF of introductory length l and period j has at most $l + 2j$ parameters to be determined, namely $a_0, a_1, \ldots, a_{l-1}$, $b_1, \ldots, b_j$, and $c_1, \ldots, c_j$. Each of these parameters must be an integer, so the sets of possible a_0, etc, are all countably infinite, which implies that the set of continued fractions of introductory length l and period j is countable. Then if we pick an integer m and consider all LPCF's with $l + j = m$ we see that this must also be a countable set, since it is the finite union of countable sets (i.e. l=0 and j=m, l=1 and j=m-1,...,l=m and j=0). And the set of all LPCF's with $l + j \leq m$ is a finite union of the sets with $l + j = m$ so it must be a countably infinite set. Since this is valid for all m, we can say that the set of all possible LPCF's is countably infinite. If this argument seems questionable, consider the fact that the set with $l + j \leq m + 1$ has the same measure as the set with $l + j \leq m$. Of course we cannot extend this to $m = \infty$, and we wouldn't want to–we would then be proving that the real numbers are countable.

3.3 Rational and quadratic numbers

Our observations (and a few provable results) begin with two subsets of the LPCF's. If we allow the period of an LPCF to be 0, then the rational numbers are the subset with 0 period. What happens when we shift or scale rational number? If we shift or scale by another rational, than the result will be rational and we will get a continued fraction of some finite length. Just *how* the length changes is quite another question. We would expect that if a rational r was shifted or scaled by m/n, the length of the ensuing continued fraction would (most of the time) be an increasing function of n. For a large n will produce a rational with a large denominator, necessitating a long continued fraction. Moreover, we might expect the ensuing length to be essentially independent of m, since it is the denominator that determines the "precision" of a continued fraction.

insert guesses & tests of the function

If the period of an LPCF is strictly positive but there are no diagonals, then the LPCF is an ordinary periodic continued fraction, hence an irrational root of a quadratic, say $f(x)$. And if we scale or shift this root by a rational, it will be the root of a new quadratic, $f(x - m/n)$ or $f(x/a)$. So the transformed number will again have a periodic continued fraction. Now we again want to ask: how will the period change? In the case of shifts, it seems that the period changes just like it did in the rational case: it is an increasing function of n. Some supporting data are shown in ———. The case of scaling has not been investigated but we might expect similar results.

3.4 Shifts of Tan(1)

all we had time to investigate in any depth; and even then not much depth

3.4.1 Effects on the period

varies roughly as $n^{5/14}$

3.4.2 Effects on the diagonals

primes: 3 diagonals, slopes 4, $4p^2$, $4p^4$

non-primes: much trickier, but get neat patterns that depend very directly on divisors

3.4.3 Effects on the base sequence

largest number is always $\leq n^2$ and almost always equal to n^2

tend to converge to Kuzmin probabilities (converge or fluctuate?)

3.5 Other LPCF's

- show a few things about e
- shifts and scaling in general: shifts in ptic probably act like those of tan(1); compare to effects on rational and quadratic numbers
- great way to visualize things quickly: log-log graphs; include notebook

There is much left to investigate & many questions unanswered!

4 Appendix

4.1 Proof of Conjecture 1

Consider the plot of the R_n, partially drawn in Figure 3. The total probability of failure is the area under R_1 plus the area between R_2 and R_3 plus.... Likewise, the total probability of success is the area between R_1 and R_2 plus the area between R_3 and R_4 plus.... But notice the apparent symmetry around $x = 1/2$. It seems that the structure of the graph for $x < 1/2$ is reflected into the first 1-triangle ($x > 1/2$). In the first 1-triangle, the lower boundary of this structure is R_2 while for $x < 1/2$ the lower boundary is R_1. So *if* the structure is reflected, all the success and failure regions are precisely inverted in the reflection. Therefore, we can imagine switching all the areas of success in the $x < 1/2$ region with the corresponding areas of failure in the first 1-triangle. Then the 1-triangle has *all* the areas of success and the remainder of the region below the diagonal has all the areas of failure. So certainly the total probability of failure is $3/4$ and the total probability of success is $1/4$.

For the proof, it is enough to establish the claimed symmetry. Considering the correlation between the R_n and the continued fraction coefficients of rational numbers described at the end of Section 2.3.1, it is sufficient to show that we have

$$1 - [0, 1, a_2, a_3, \ldots] = [0, 1 + a_2, a_3, a_4, \ldots] \tag{87}$$

for any continued fraction $[0, 1, a_2, \ldots]$, or, equivalently, that

$$1 - [0, a_1, a_2, \ldots] = [0, 1, a_1 - 1, a_2, \ldots] \tag{88}$$

for any continued fraction $[0, a_1, a_2, \ldots]$ with $a_1 \neq 1$. In the former, the LHS is the continued fraction representation of any number $1/2 < x < 1$ and the RHS is what we would like the continued fraction of its reflection about $1/2$ to be. The opposite is true in the latter. To establish (87), note that the LHS can be written as

$$\begin{aligned}
1 - [0, 1, a_2, a_3'] &= 1 - \frac{1}{1 + \frac{1}{a_2 + 1/a_3'}} \\
&= 1 - \frac{1}{1 + \frac{a_3'}{a_2 a_3' + 1}} \\
&= 1 - \frac{1}{\frac{a_2 a_3' + 1 + a_3'}{a_2 a_3' + 1}} \\
&= 1 - \frac{a_2 a_3' + 1}{a_2 a_3' + 1 + a_3'} \\
&= \frac{a_3'}{a_2 a_3' + 1 + a_3'},
\end{aligned}$$

and the RHS is

$$\begin{aligned}
[0, 1 + a_2, a_3'] &= \frac{1}{1 + a_2 + \frac{1}{a_3'}} \\
&= \frac{1}{\frac{a_3' + a_3' a_2 + 1}{a_3'}} \\
&= \frac{a_3'}{a_3' + a_3' a_2 + 1},
\end{aligned}$$

so the two sides are equal. Equation 88 can obviously be established in a similar way.

Therefore, we can in fact say

Theorem 7 *Given polynomial with a root ξ a single root $\lfloor \xi \rfloor \leq r < \xi$ (and no roots $\xi < \rho < \lfloor \xi \rfloor + 1$) such that the point $(\xi - \lfloor \xi \rfloor, r - \lfloor \xi \rfloor)$ is randomly distributed below the diagonal of the unit square, the probability of success of the Lang-Trotter algorithm is 1/4 and the probability of failure is 3/4.*

4.2 Complete data for shifts of Tan(1)

–

4.3 Explanation of *Mathematica* codes

–

References

[1] R. P. Brent, A. J. van der Poorten, and H. J. J. te Riele. "A Comparative Study of Algorithms for Computing Continued Fractions of Algebraic Numbers." *Proceedings of the Second International Symposium on Algorithmic Number Theory.* Talence, France 1996.

[2] A. Y. Khinchin, *Continued Fractions*, Third Edition, The University of Chicago Press, Chicago 1964.

[3] S. Lang and H. Trotter. "Continued fractions for some algebraic numbers." *J. reine angew. Math.*, 225. 1972. p. 112-134.

[4] R. Takloo-Bighash, S. J. Miller, H. Helfgott, and F. Spinu. Notes for Princeton Junior Seminar, Fall 2002: *Diophantine Analysis and Roth's Theorem.* Princeton University 2002.