Continued fractions and the geometry of numbers

Burton Rosenberg

November 26, 2003

Introduction

A continued fraction is an expansion of a number with certain relationship to the euclidean algorithm. For a rational, it is exactly the euclidean algorithm.

This is a work in progress: the theory is not developed completely to my liking. I will indicate, as much for my own future reference, where the theory doesn't seem to hold together well.

Take a real $\alpha \geq 1$. Express it as integer and fractional part, $\alpha = \lfloor \alpha \rfloor + \alpha'$. If α' is not zero, its inverse is greater than one. Write it $1/\alpha' = \lfloor \alpha \rfloor + \alpha''$, and so on. If the first integer part is a_0, the second is a_1, and so on, then,

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}}$$

which we will write $\alpha = [a_0, a_1, a_2, \ldots]$.

For a rational α the continued fraction expansion is finite. The expansion of p/q follows the euclidean algorithm for $\gcd(p, q)$. From $p = a_0 q + r$ we have $p/q = a_0 + r/q$, where a_0 is the integer part of p/q and r/q is the fractional part. The next step of the algorithm gives $q/r = a_1 + r'/r$, where $r'/r < 1$.

For a expansion $[a_0, a_1, a_2, \ldots]$, the prefix expansions $p_i/q_i = [a_0, a_1, \ldots, a_i]$ are the convergents of the expansion.

Fundamentals

At some point here there has to be a definition. The fractional linear transform representation is not unique, and we talk about numbers resulting from a particular computation. There needs to be "computation invariant" statements about these numbers.

Lemma 1 *Let* $[a_0, a_1, \ldots, a_{i-1}, \alpha]$ *be a continued fraction, with the last entry a formal. Then,*

$$[a_0, a_1, \ldots, a_{i-1}, \alpha] = \frac{a\alpha + b}{c\alpha + d}$$

with $a, b, c, d \in \mathbb{Z}$*, non-negative, and* $ad - bc = (-1)^i$*.*

Proof: By induction. For $i = 0$ verify $(1 \cdot \alpha + 0)/(0 \cdot \alpha + 1)$ satisfies the lemma. For $i > 0$ we use the induction hypothesis on the tail of the expansion.

$$a_0 + 1/[a_1, \ldots, a_{i-1}, \alpha] = a_0 + \left(\frac{a\alpha + b}{c\alpha + d}\right)^{-1} = \frac{(a_0 a + c)\alpha + a_0 b + d}{a\alpha + b}$$

By various laws of determinates and the induction hypothesis,

$$\det \begin{bmatrix} a_0 a + c & a_0 b + d \\ a & b \end{bmatrix} = -\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = -(-1)^{i-1}$$

Note that the modular determinate implies that a and b are relatively prime, as are c and d, as are a and c, as well as b and d.

Lemma 2 *For the continued fraction expansion,*

$$[a_0, \ldots, a_{i-1}, \alpha] = \frac{p_{i-1}\alpha + p_{i-2}}{q_{i-1}\alpha + q_{i-2}}$$

and,

$$\begin{aligned} p_i &= p_{i-1} a_i + p_{i-2} \\ q_i &= q_{i-1} a_i + q_{i-2} \end{aligned}$$

where p_i/q_i *is the* i*-th convergent (reduced to lowest terms).*

Proof: Evaluate the form $(a\alpha + b)/(c\alpha + d)$ at $\alpha = 0$. On the one hand this gives the convergent $p_{i-2}/q_{i-2} = [a_0, \ldots, a_{i-2}]$ and on the other hand, the fraction b/d. Since b and d are relatively prime, $b = p_{i-2}$ and $d = q_{i-2}$. Likewise, evaluation at $\alpha = \infty$ and consideration of relative primality give $a = p_{i-1}$ and $b = q_{i-1}$.

Evaluation at $\alpha = a_i$ gives $p_i/q_i = (p_{i-1}a_i + p_{i-2})/(q_{i-1}a_i + q_{i-2})$. To conclude that equality of ratios give actual equality of numerators and denominators separately we need to show relative primality of the values given by the linear forms in numerator and denominator. From the previous lemma,

$$p_{i-1}q_{i-2} - p_{i-2}q_{i-1} = \det \begin{bmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{bmatrix} = \pm 1$$

If numerator and denominator were not relatively prime then there would be a prime p such that a_i is a solution to,

$$\begin{bmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p}$$

which is impossible, since the matrix is invertible over $\mathbb{Z}_p$.

Lemma 3 *The even convergents of x are smaller then x; the odd convergents are greater than x. The error of a convergent $|x - p/q|$ is bound by $1/q^2$.*

Proof: Consider the continued fraction expansion and its fractional linear form as a function of α,

$$f(\alpha) = [a_0, a_1, \ldots, a_i, \alpha] = \frac{p_i\alpha + p_{i-1}}{q_i\alpha + q_{i-1}}$$

Then,

$$df(\alpha)/d\alpha = \frac{p_i q_{i-1} - p_{i-1}q_i}{(q_i\alpha + q_{i-1})^2}$$

Hence f is monotonic in α, increasing or decreasing depending on the sign of $p_i q_{i-1} - p_{i-1}q_i$.

Treating f as a function, there is an x' such that $x = f(x')$. In fact, it will be the residual amount we are continuing each step in the evaluation of the a_i So $f(0) = p_{i-1}/q_{i-1}$ and $f(\infty) = p_i/q_i$ will be on opposites sides of x. Note that the 0-th covergent is simple $\lfloor x \rfloor$, so the even convergents bound x from below.

Furthermore the error of a convergent is bound by the difference between it and its following convergent,

$$\left| x - \frac{p_i}{q_i} \right| < \left| \frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}} \right| = \left| \frac{p_i q_{i+1} - p_{i+1}q_i}{q_i q_{i+1}} \right| = \frac{1}{q_i q_{i+1}} < \frac{1}{{q_i}^2}$$

This might be a proper place to establish the uniqueness of the continued fraction representation, i.e. that distinct sequences of integers, when placed as quotients in the continued fraction, give distinct reals.

The geometry of numbers

Consider the lattice $\mathbb{Z} \times \mathbb{Z}$ in the real plane, that is, all points (a, b) for integer a and b. The ratio p/q is represented by the vector (q, p), this vector has slope p/q. To any number α the line through the origin with slope α. The process of continued fractions give a series of vectors with slope converging towards α. And they are constructed this way.

$$v_{i+1} = (q_{i+1}, p_{i+1}) = (q_i a_{i+1} + q_{i-1}, p_i a_{i+1} + p_{i-1}) = a_{i+1}v_i + v_{i-1}$$

Geometrically speaking, recalling the alternation of approximations, beginning from v_{i-1} which w.l.o.g. underestimates α, we add multiples of v_i, which consequently overestimates α, until just before we pass through the line of slope α. This is the new convergent, v_{i+1}.

Approximation to any real

We take this proof from Mika's book.

Theorem 1 *Let α be a real, and p/q a rational. If $0 < |\alpha - p/q| \leq 1/(2q^2)$ then p/q is a convergent of the continued fraction expansion of α.*

We first show a lemma:

Lemma 4 *Let P, Q, P' and Q' be integers such htat $Q > Q' > 0$ and $PQ' - QP' = \pm 1$. We call this last equality the determinate condition. If there exists an $\alpha' \geq 1$ such that,*

$$\alpha = \frac{\alpha' P + P'}{\alpha' Q + Q'}$$

then P'/Q' and P/Q are consecutive convergents in the continued fraction expansion of α.

Proof: Let $[a_0, \ldots, a_n]$ be the partial fraction expansion of P/Q. The determinate condition implies that this fraction is in lowest terms and therefore $P = p_n$ and $Q = q_n$. Therefore,

$$p_n Q' - q_n P' = \pm 1 = \pm(p_n q_{n-1} - q_n p_{n-1})$$

We can manipulate the partial fraction expansion to be one longer or one shorter, if necessary, to get the sign positive on the rightmost quantity.

$$p_n(Q' - q_{n-1}) = q_n(P' - p_{n-1})$$

Again using relative primality, we have that $q_n | (Q' - q_{n-1})$. Since $q_n > Q', q_{n-1} > 0$, the difference must be less than q_n and therefore zero. So $Q' - q_{n-1}$ and consequently $P' = p_{n-1}$. Hence we have,

$$\alpha = \frac{\alpha' p_n + p_{n-1}}{\alpha' q_n + q_{n-1}}$$

Continue the expansion with $\alpha' = [a_{n+1}, \ldots]$. The complete expansions of α therefore contains the desired convergents.

Proof (of theorem): Expand $p/q = [a_0, \ldots, a_n]$. We may assume $p = p_n$ and $q = q_n$. Define,

$$\alpha' = \frac{-\alpha q_{n-1} + p_{n-1}}{\alpha q_n - p_n}$$

The inverse of a fractional linear transformation is again a fractional linear transformation. In this case,

$$\alpha = \frac{\alpha' p_n + p_{n-1}}{\alpha' q_n + q_{n-1}}$$

So,

$$\left| \frac{p_n}{q_n} - \alpha \right| = \left| \frac{p_n(\alpha' q_n + q_{n-1}) - q_n(\alpha' p_n + p_{n-1})}{q_n(\alpha' q_n + q_{n-1})} \right| = \left| \frac{\pm 1}{q_n(\alpha' q_n + q_{n-1})} \right| \leq \frac{1}{2{q_n}^2}$$

which implies,

$$\alpha' \geq 2 - (q_{n-1}/q_n) > 1$$

So the lemma applies, and p/q is a convergent of the expansion of α.

Notes

Lemma 5 *Let $a, b \in \mathbb{Z}$ be relatively prime, and $s, t \in \mathbb{Z}$ be integers such at $sa - tb = 1$. Such integers are known to exist. Then all integer solutions to $xa - yb = 1$ are $\{ (s + kb, t + ka) \,|\, k \in \mathbb{Z} \}$.*

Proof: If $sa - tb = s'a - t'b$ then $a(s - s') = b(t - t')$. So $b|(s - s')$ and $a|(t - t')$. Writing $kb = s - s'$ and $k'a = t - t'$, we have $akb = bk'a$, so $k = k'$.

The notation $[a_0; a_1, \ldots]$ is preferable, since $a_i \in \mathbb{Z}^+$ for $i > 0$, and a_0 is zero only if the expansion is for a positive real less than one.

Lemma 6 *The continued fraction $[a_0; a_1, \ldots, a_i, \alpha]$, with $a_i \in \mathbb{Z}^+$ and α a formal is the fractional linear transformation,*

$$[a_0; a_1, \ldots, a_i, \alpha] = \frac{p_i \alpha + p_{i-1}}{q_i \alpha + q_{i-1}}$$

where $p_j/q_j = [a_0; a_1, \ldots, a_j]$, a ratio of positive integers expressed in lowest terms, and furthermore, $p_i q_{i-1} - p_{i-1} q_i = \pm 1$.

Lemma 7 *With $[a_0; a_1, \ldots, a_i, \alpha]$ as above, and $\alpha = [b_0; b_1, \ldots, b_j, \alpha']$. If $\alpha \geq 1$ then $b_0 \geq 1$ and $[a_0; a_1, \ldots, a_i, \alpha] = [a_0; a_1, \ldots, a_i, b_0, b_1, \ldots, b_j, \alpha']$.*

Lemma 8 (Construction lemma) *Suppose $x = [a_0; a_1, \ldots, a_i, \alpha]$ is a continued fraction expansion of x where α is not an integer. Let $a_{i+1} = \lfloor \alpha \rfloor$, and $\alpha' = (\alpha - a_{i+1})^{-1}$. Then $x = [a_0; a_1, \ldots, a_i, a_{i+1}, \alpha']$ is also a continue fraction expansion of x.*