Complexity of Some Elementary Operations on Continued Fractions

Marek Teichmann

Abstract

We consider the simple continued fractions representations of real numbers. Continued fractions are assumed to be streams of integers that represent the partial quotients. We analyze some unary and binary operations including homography, addition and multiplication, implemented as 'filters'. These take as input one or two streams and produce a stream of partial quotients of the continued fraction of the result. We prove some bounds on the number of terms that are necessary to input to provide one term of output for the homography operation.

1 Introduction

The form

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots \frac{}{+\frac{1}{a_n}}}}$$

with $a_i \in \mathbf{Z}$ and $a_i \geq 1$ for $i > 0$ is a *regular continued fraction.* We will denote its value by

$$[a_0, a_1, a_2, \ldots, a_n].$$

We call $a_0, a_1, a_2, \ldots, a_n$ the *partial quotients* or *terms* of the continued fractions.

Continued fractions offer an interesting way to represent real numbers, and have many nice properties. It is possible to do basic operations, like addition, multiplication, etc. directly using the partial quotients.

Finite continued fractions like above represent rational numbers (uniquely if we assume that $a_n \geq 2$), and infinite continued fractions of the form $[a_0, a_1, \ldots]$ uniquely represent irrational numbers.

Here we assume that we are given the continued fractions as streams of numbers.

Knuth [K81] describes an algorithm to compute the continued fraction of a homography in terms of an input continued fraction.

Gosper [G72] generalizes this to include two inputs and allows the computation of the sum, difference, product and ratio of two continued fractions.

Filter type algorithms can be viewed in the following general framework. A similar one is described by Vuillemin [V90]:

They take as input terms of the input contined fraction, and output terms of the output contined fraction. We start out with no output and the continued fraction of x as input. Say we wish to compute the continued fraction of $f(x)$, where $x = [a_0, a_1, \ldots]$.

We cannot produce a term of the continued fraction of $f([a_0, a_1, \ldots])$ since generally $\lfloor f(x) \rfloor$ varies with x, as x ranges over all possible values. So we must input a term (a_0) and consider

$$f_1(x) = f(a_0 + \frac{1}{x}) = f([a_0, x])$$

to see if $\lfloor f(x) \rfloor$ remains constant. If it is not, we must input another term. In general, we consider $f_i(x) = f([a_0, a_1, \ldots, x])$.

So at each step we maintain a function f_i, initially f, whose role is to compute the continued fraction of the remaining input. At any time, the range of the input to f_i is $[1, \infty]$ since we still haven't seen the next term which could be anywhere in that range. Let $R_i = f_i([1, \infty])$ be the range of f_i. If no integer is contained in R_i, we know the value of $c = \lfloor f_i(1) \rfloor$ and we can output one term c of the continued fraction of $f(x)$, and let

$$f_{i+1}(x) = \frac{1}{f_i(x) - c}.$$

Otherwise we need to input a new term a, and we let

$$f_{i+1}(x) = f_i(a + \frac{1}{x}).$$

Note: If f is monotone on $[1, \infty]$ then it remains monotone after each transformation. Proof: Assume f_i is monotone on $[1, \infty]$. This is certainly true of f_0. Now the function $t_e(x) = e + \frac{1}{x}$ is monotone has a range of $[e, e+1] \subset [1, \infty)$ for $e \in [1, \infty)$ and $x \in [1, \infty]$ hence $f_{i+1}(x) = f_i(a + \frac{1}{x})$ is also monotone. In the other case, $f_{i+1}(x) = 1/(f_i(x) - c)$, is also monotone on $[1, \infty]$ since $c \leq f_i(x)$. Hence by induction f_i is monotone on $[1, \infty]$ for all i. ∎

For a two argument function $f(x, y)$ the situation is analoguous. Say we wish to compute the terms of the continued fraction of $f([a_0, a_1, \ldots], [b_0, b_1, \ldots])$. We maintain $f_{ij}(x, y)$, with $f_{00} = f$. As before, we can output a term of $f(x, y)$ when $\lfloor f_{ij}(x, y) \rfloor$ is constant for all $x, y \in [1, \infty]$. Otherwise a term of x of y or both must be input. Input of a term a_k of x is done using the transformation

$$f_{i+1,j}(x, y) = f_{i,j}(a_k + \frac{1}{x}, y).$$

Input of term of y is similar. Here however we will input a term of both input continued fractions for simplicity of analysis, but other algorithms are possible. Thus we drop one index, the transformation becomes

$$f_{i+1}(x, y) = f_i(a_k + \frac{1}{x}, b_k + \frac{1}{y})$$

upon input of a_k and b_k.

1.1 Homography of a Continued Fraction

An important function to study is the homography or linear fractional transformation. A property of homographies is that they retain their linear fractional form under the transformations described above. Here the function f is $h(x) = \frac{ax+b}{cx+d}$ where $a, b, c, d \in \mathbf{Z}$.

We maintain a homography h, initially $h(x) = \frac{ax+b}{cx+d}$ whose role is to compute the homography of the remaining input. (We will drop the indices in the following.) Input terms are absorbed if $h(x)$ has a pole for $x \geq 1$ or when $\lfloor \frac{a}{c} \rfloor \neq \lfloor \frac{a+b}{c+d} \rfloor$.

When an input term u is absorbed, the homography becomes $h(u + \frac{1}{x})$, that is

$$(a, b, c, d) \leftarrow (au + b, a, cu + d, c),$$

otherwise if we output $v = \lfloor \frac{a}{c} \rfloor = \lfloor \frac{a+b}{c+d} \rfloor$ we set

$$(a, b, c, d) \leftarrow (c, d, a - vc, b - vd).$$

1.2 Addition, Multiplication, etc ...

Gosper presents a unified way to compute the sum, difference, product and ratio of two continued fractions. The function $f(x)$ becomes a function of two variables $f(x, y)$ defined by

$$f(x, y) = \frac{Axy + Bx + Cy + D}{Exy + Fx + Gy + H}.$$

The four basic operations can be expressed by letting

$$(A, B, C, D; E, F, G, H) = (0, 1, +/-1, 0; 0, 0, 0, 1) \text{ for } + \text{ and } -,$$

$$(A, B, C, D; E, F, G, H) = (1, 0, 0, 0; 0, 0, 0, 1) \text{ for } \times \text{ and}$$

$$(A, B, C, D; E, F, G, H) = (0, 1, 0, 0; 0, 0, 1, 0) \text{ for } /.$$

Upon input of a term a of x, f changes as follows:

$$(A, B, C, D; E, F, G, H) \leftarrow (aA + C, aB + D, A, B; aE + G, aF + H, E, F),$$

and upon input of a term b of y, f changes as follows:

$$(A, B, C, D; E, F, G, H) \leftarrow (bA + B, A, bC + D, C; bE + F, E, bG + H, G).$$

When x runs out of terms $f(x, y)$ becomes f', univariate, with $f'(y) = f(\infty, y)$, and when y runs out of terms, $f'(x) = f(x, \infty)$.

We have

$$f(x, \infty) = \frac{Ax + C}{Ex + G}, \quad f(\infty, y) = \frac{Ay + B}{Ey + F}.$$

To output a term z, we proceed to transform f by

$$(A, B, C, D; E, F, G, H) \leftarrow (E, F, G, H; A - zE, B - zF, C - zG, D - zH).$$

If we hold one of the variables fixed, and examine the range of f, we obtain an interval on the projective line. Letting the other variable be 1, then ∞, we obtain four intervals, two for each variable. Because of the basically monotone behaviour of f, the range of f is the union of the four intervals.

If $\lfloor f(x,y) \rfloor$ is fixed for $(x,y) \in [1,\infty]^2$, we can output a term, otherwise it is necessary to input one term of x or y. Gosper suggests inputting the term associated with the largest interval. However it is not clear what this means when the intervals are infinite at the beginning. For instance, it is not enough to input only terms of one continued fraction while the intervals are infinite, since in that case the range of f remains infinite and we make no progress.

Note that it may happen that we may never be able to output a term. For example, in the continued fraction of $(\sqrt{2}+1)-(\sqrt{2}-1)$, the first term is 2, the second is infinite, but we never know since we would have to look at all the terms of both continued fractions. A similar situation arises if we are trying to calculate, say, the first output term of the continued fraction of $[a_0, a_1, \ldots] - [a_0, a_1, \ldots, a_{i-1}, b_i, \ldots]$ for some pair of continued fractions with identical initial terms. However, if the minimal polynomials of the two input numbers are known, it can be shown that for sufficiently large i, we must have $a_i = b_i$, and hence the first term of the difference is 0.

Hence we find it interesting to study the above algorithms when applied to algebraic numbers of bounded degree.

2 Some Definitions and Facts

2.1 ... about Continued Fractions

Given the continued fraction $[a_0, a_1, \ldots]$, define the sequences p_n and q_n as follows:

$$\begin{aligned}
p_0 &= a_0, \quad q_0 = 1, \\
p_1 &= a_1 a_0, \quad q_1 = a_1, \\
p_n &= a_n p_{n-1} + p_{n-2} \quad (2 \leq n), \\
q_n &= a_n q_{n-1} + q_{n-2} \quad (2 \leq n).
\end{aligned}$$

Then we have the nth *partial quotient* $[a_0, a_1, \ldots, a_{n-1}, a_n] = \frac{p_n}{q_n}$. Furthermore, it can be shown that ([K64])

$$\frac{1}{q_n(q_n + q_{n+1})} \leq \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} \leq \frac{1}{F_{n+1} F_{n+2}} < \phi^{1-2n}.$$

2.2 ... about Polynomials

Let $P(x) = c_0 + c_1 x + \cdots + c_n x^n$. We define

$$\|P\|_\infty = \max_i \{c_i\}$$

and [M91]

$$M(P) = |c_n| \prod_{j=1}^{n} \max\{1, |z_j|\}.$$

The discriminant of P is defined by

$$\mathrm{disc}(P) = c_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Also F_n is the n-th Fibonnaci number and $\phi^{n-2} \le F_n \le \phi^{n-1}$, where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

3 Properties of polynomials and homographies

Let $P \in \mathbf{Z}[x]$ of degree n and α a root of P.

The continued fraction algorithm

$$\begin{aligned} \alpha_0 &= \alpha \\ \alpha_{i+1} &= \frac{1}{\alpha_i - a_i}, \quad a_i = \lfloor \alpha_i \rfloor \end{aligned}$$

produces a list of algebraic numbers α_i, roots of polynomials $P_i \in \mathbf{Z}[x]$ of degree n. These are defined by

$$\begin{aligned} P_0 &= P \\ P_{i+1}(x) &= x^n P(a_i + \tfrac{1}{x}) \end{aligned}$$

Since $|\alpha_i| \le 1 + \frac{\|P_i\|_\infty}{|\mathrm{lead}\, P_i|} \le 1 + \|P_i\|_\infty$ certainly $|a_i| = |\lfloor \alpha_i \rfloor| \le 2 + \|P_i\|_\infty$.

The operation $P_{i+1}(x) = x^n P(a_i + \frac{1}{x})$ can be decomposed into a translation $Q(x) = P(x + a_i)$, and a reciprocal $R(x) = Q(1/x)$. We analyze both separatly.

3.1 Polynomial Translation

Let $P(x) = c_0 + c_1 x + \cdots + c_n x^n$. We have by Taylor's theorem

$$T(x) = P(x+a) = P(a) + xP'(a) + \frac{x^2}{2} P''(a) + \cdots + \frac{x^i}{i!} P^{(i)}(a) + \cdots + x^n c_n$$

We assume that the translation amount a is such that $|a - \chi| < 1$ for some root χ of P.

This is the case when a is the first term of the continued fraction of a root of P. Using the root bound $|\chi| \le 1 + \|P\|_\infty$ we get that $|a| \le 2 + \|P\|_\infty$, and

$$|P^{(i)}(a)| \;\le\; i! \binom{n}{i} \|P\|_\infty \sum_{j=0}^{n-i} |a|^j$$

$$\begin{aligned}
& \leq & i!\binom{n}{i}\|P\|_\infty \frac{(2+\|P\|_\infty)^{n-i+1}}{1+\|P\|_\infty} \\
|P^{(i)}(a)| & < & i!\binom{n}{i}(2+\|P\|_\infty)^{n-i+1} \qquad (1)
\end{aligned}$$

When we use the root bound $|\chi| \leq M(P)$, $|a| \leq 1+M(P)$. Using the fact that $M(P) \leq (n+1)\|P\|_\infty$ if P is not a monomial ([M91, p152]) a similar calculation yields

$$|P^{(i)}(a)| < i!\binom{n}{i}\frac{(1+M(P))^{n-i+1}}{n+1} \qquad (2)$$

So

$$\|T\|_\infty = \|P(x+a)\|_\infty \leq \max_{i=0\ldots n}\left\{\binom{n}{i}(2+\|P\|_\infty)^{n-i+1}\right\}$$

Hence our bounds can be summarized by

$$\|T\|_\infty < 2^n(2+\|P\|_\infty)^{n+1} \qquad (3)$$

$$M(T) < 2^n M(P)^{n+1} \qquad (4)$$

Furthermore the definition of the discriminant gives

$$\mathrm{disc}(T) = \mathrm{disc}(P).$$

3.2 Reciprocal Polynomial

Let $R(x) = x^n P(\frac{1}{x})$. Then $M(R) = M(P)$ (see [M91]) and $\|R\|_\infty = \|P\|_\infty$, $\|R\|_2 = \|P\|_2$. As for the discriminant a simple calculation using the fact c_0/c_n is up to sign, the product of all roots of P, we also have

$$\mathrm{disc}(R) = \mathrm{disc}(P).$$

3.3 Size of terms of a continued fraction of a root

From the above, at each step of the continued fraction algorithm we have

$$\begin{aligned}
\|P_{i+1}\|_\infty & < & 2^n(2+\|P_i\|_\infty)^{n+1} \\
& < & 2^n 2^{n+1}\|P_i\|_\infty^{n+1} \\
& < & (4\|P_i\|_\infty)^{n+1} \\
& < & (4(4\|P_{i-1}\|_\infty)^{n+1})^{n+1} = 4^{(n+1)+(n+1)^2}\|P_{i-1}\|_\infty^{(n+1)^2} \\
& & \ldots \\
& < & 4^{\sum_{j=1}^{i+1}(n+1)^j}\|P_0\|_\infty^{(n+1)^{i+1}} \\
& \text{hence} & \\
\|P_i\|_\infty & < & 4^{\frac{(n+1)^{i+1}}{n}}\|P\|_\infty^{(n+1)^i}
\end{aligned}$$

So we have a bound on the terms a_i of the continued fraction of a root of P:

$$|a_i| < 1 + 4^{\frac{(n+1)^{i+1}}{n}} \|P\|_\infty^{(n+1)^i}$$

and a_i has at most $O((n+1)^i \log \|P\|_\infty)$ bits. However this should be a constant independent of i if $n \leq 2$ if it were tight. This looseness is probably due to the fact that we don't use that a_i is close to a root of $P_i(x)$, and that we are not following a particular root.

We will need the following

Lemma 3.1 *For an algebraic number α with $P(\alpha) = 0$, $P(x) \in \mathbf{Z}[x]$, $\deg(P) = n$, and a rational number p/q with $P(p/q) \neq 0$,*

$$|\alpha - \frac{p}{q}| > |q|^{-n} n^{-1} (2 + \|P\|_\infty)^{-n},$$

$$|\alpha - \frac{p}{q}| > |q|^{-n} (1 + M(P))^{-n}.$$

Proof

$$|P(\frac{p}{q})| = \frac{|c_n p^n + c_{n-1} q p^{n-1} + \cdots + c_0 q^n|}{|q|^n} \geq \frac{1}{|q|^n}$$

since the numerator is an integer. Also

$$P(\frac{p}{q}) = P(\frac{p}{q}) - P(\alpha) = (\frac{p}{q} - \alpha) P'(x)$$

for some x between α and $\frac{p}{q}$. But then for $|\alpha - \frac{p}{q}| < 1$ we have

$$\begin{aligned} |\alpha - \frac{p}{q}| &= \frac{|P(\frac{p}{q})|}{|P'(x)|} \\ &> \frac{1}{|q|^n \max_x \{P'(x)\}} =: A \end{aligned}$$

but by (1)

$$A > \frac{1}{|q|^n n (2 + \|P\|_\infty)^n}$$

and by (2) we get

$$A > \frac{1}{|q|^n (1 + M(P))^n} \quad \blacksquare$$

Note: using $Q(x) = P(x)(qx - p)$ gives a worse bound, but doesn't require $P(p/q) \neq 0$.

3.4 Transformation of a Polynomial by a Homography

Let $h(x)$ be the homography defined by $h(x) = \frac{ax+b}{cx+d}$ and $\|h\|_\infty = \max\{|a|, |b|, |c|, |d|\}$. We examine the polynomial $Q(x)$ whose roots are image under this homography of roots of a given polynomial P. Take $P(x) = \sum_{i=0}^{n} a_i x^i$, then we have

Lemma 3.2 *Let*

$$Q(x) = (cx+d)^n P\left(\frac{ax+b}{cx+d}\right) = \sum_{i=0}^{n} a_i (ax+b)^i (cx+d)^{n-i}$$

then

$$\|Q\|_\infty < n(n+1)2^n \|P\|_\infty \|h\|_\infty^n \tag{5}$$

Proof

$$(ax+b)^i = \sum_{j=0}^{i} \binom{i}{j} x^j a^j b^{i-j} \quad (cx+d)^{n-i} = \sum_{j=0}^{n-i} \binom{n-i}{j} x^j c^j d^{n-i-j}$$

Then for $i \neq 0, n$, the coefficient of x^l in $(ax+b)^i (cx+d)^{n-i}$ is[1]

$$e_l^{(i)} = \sum_{j+k=l} \binom{i}{j} a^j b^{i-j} \binom{n-i}{k} c^k d^{n-i-k}$$

$$e_l^{(0)} = \binom{n-i}{l} c^l d^{n-i-l} \qquad e_l^{(n)} = \binom{i}{l} a^l b^{i-l}$$

So

$$Q(x) = \sum_{i=0}^{n} a_i \sum_{l=0}^{n} e_l^{(i)} x^l = \sum_{l=0}^{n} \left[\sum_{i=0}^{n} a_i e_l^{(i)}\right] x^l$$

We have

$$\begin{aligned} e_l^{(i)} &= \sum_{j=0}^{l} \binom{i}{j} \binom{n-i}{l-j} a^j b^{i-j} c^{l-j} d^{n-i-(l-j)} \\ |e_l^{(i)}| &< l \binom{i}{\lfloor \frac{i}{2} \rfloor} \binom{n-i}{\lfloor \frac{n-i}{2} \rfloor} \max\{|a|, |b|, |c|, |d|\}^n \\ &< l 2^n \|h\|_\infty^n \leq n 2^n \|h\|_\infty^n \end{aligned}$$

hence the result. ∎

[1] We take $\binom{i}{j} = 0$ for $j < 0$ and $j > i$, and $\binom{0}{0} = 1$

4 Analysis of homography algorithm

Let α be an algebraic number with continued fraction $[a_0, a_1, \ldots]$ where $P(\alpha) = 0$, $P(x) \in \mathbf{Z}[x]$ of degree n. Let $h(x)$ be a homography with integer coefficients. We apply the homography algorithm to $[a_0, a_1, \ldots]$ and wish to see how many terms of $[a_i]$ we need to input in order to produce one term of output, that is in order to know $\lfloor h(\alpha) \rfloor$.

Define

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

where p_i/q_i is the i-th convergent of the continued fraction of α. We obtain an upper bound on the minimal i which guarantees that

$$\lfloor h(\alpha) \rfloor = \lfloor h(g_i(x)) \rfloor \text{ for all } x \in [1, \infty]$$

at which point the term $\lfloor h(\alpha) \rfloor$ can be output.

This is the case when $|h(\alpha) - h(g_i(x))| < |h(\alpha) - \lfloor h(\alpha) \rfloor|$ for all $x \in [1, \infty]$ or equivalently $|h(\alpha) - h(g_i(x))| < |h(\alpha) - \lfloor h(\alpha) \rfloor|$ for $x = 1, \infty$ and $h(g_i(x))$ has no pole on $[1, \infty]$, that is $|g_i(x) + d/c| > 0$ for $x \in [1, \infty]$.

The first condition will be replaced by $|h(\alpha) - h(g_i(x))| < |h(\alpha) - \lfloor h(\alpha) \rfloor|$.

Upper bound for $|h(\alpha) - h(g_i(x))|$:

Note that g_i has no pole on $[1, \infty]$. We have by the mean value theorem

$$|h(\alpha) - h(g_i(x))| = |\alpha - g_i(x)| h'(z)$$

for some z between α and $g_i(x)$, and $x \in \{1, \infty\}$. But

$$|\alpha - g_i(x)| = |\alpha - [a_0, a_1, \ldots, a_i, x]| \leq \frac{1}{F_{i+1} F_{i+2}} < \frac{1}{\phi^{1-2i}}$$

also since this bound is true for any a_{i+1}. Now letting $\delta = ad - bc$ we have $h'(x) = \frac{\delta}{(cx+d)^2}$ and we need a lower bound on $(cz + d)^2$ where $|z - \alpha| \leq \phi^{1-2i} < 1$. We have by lemma 3.1

$$|\alpha - (-\frac{d}{c})| > \frac{1}{|c|^n n (2 + \|P\|_\infty)^n}$$

So when i is sufficiently large ($i > 1 + \log_\phi 2|c|^n n(2 + \|P\|_\infty)^n$)

$$|\alpha - g_i(x)| < \frac{1}{\phi^{1-2i}} < \frac{1}{2} \frac{1}{|c|^n n (2 + \|P\|_\infty)^n}$$

$$|x - (-\frac{d}{c})| > \frac{1}{|c|^n n (2 + \|P\|_\infty)^n} - \frac{1}{\phi^{1-2i}} > \frac{1}{2|c|^n n (2 + \|P\|_\infty)^n}$$

$$(cx + d)^2 > \frac{1}{(2|c|^n n (2 + \|P\|_\infty)^n)^2}$$

We have finally

$$|h(\alpha) - h(g_i(x))| < \frac{4\delta |c|^{2n-2} n^2 (2 + \|P\|_\infty)^{2n}}{\phi^{1-2i}}$$

Lower bound for $|h(\alpha) - \lfloor\alpha\rfloor|$:

Consider $Q(x) = P(h^{-1}(x))(a-cx)^n$, $(\alpha \neq a/c)$ be a polynomial with $Q(h(\alpha)) = 0$. Then $\|Q\|_\infty \leq n(n+1)\|P\|_\infty\|h\|_\infty^n$ by (5). Hence by lemma 3.1 with $q = 1$

$$\begin{aligned}|h(\alpha) - \lfloor\alpha\rfloor| &\geq \frac{1}{n(2+\|Q\|_\infty)^n} \\ &\geq \frac{1}{n(2+n(n+1)2^n\|P\|_\infty\|h\|_\infty^n)^n} \\ &> \frac{1}{(n+1)^{2n+1}2^{n^2}\|P\|_\infty^n\|h\|_\infty^{n^2}}\end{aligned}$$

So the number of terms to input that will certainly give a term of $h(\alpha)$ is the smallest i such that

$$|h(\alpha) - h(g_i(x))| < \frac{4\delta|c|^{2n-2}n^2(2+\|P\|_\infty)^{2n}}{\phi^{1-2i}}$$

$$< \frac{1}{(n+1)^{2n+1}2^{n^2}\|P\|_\infty^n\|h\|_\infty^{n^2}} < |h(\alpha) - \lfloor h(\alpha)\rfloor|$$

We get

$$\phi^{1-2i} > 2^{n^2+3n+2}\delta n^{2n+3}\|P\|_\infty^{3n}\|h\|_\infty^{n^2+2n-2}$$

That is

$$i > O(n\log\|P\|_\infty + n^2\log\|h\|_\infty)$$

5 Analysis of Addition Algorithm

Let α and β be two algebraic numbers of degree m and n respectively. We want to have a bound on the number of terms we need to input into the addition algorithm in order to be able to produce one term of output. Here we assume that one term of each of the continued fractions of α and of β are input at the same time.

Let $\gamma = \alpha + \beta$, $\alpha = [a_i]_{i\geq 0}$, $\beta = [b_i]_{i\geq 0}$, $\frac{p_i}{q_i} = [a_0, a_1, \ldots, a_i]$, $\frac{r_i}{s_i} = [b_0, b_1, \ldots, b_i]$. Also define

$$g_i(x) = \frac{p_i x + p_{i-1}}{q_i x + q_{i-1}} \text{ and } g_i'(x) = \frac{r_i x + r_{i-1}}{s_i x + s_{i-1}}.$$

It is easily seen that the two variable function $f(x,y)$ defined in section 1.2 is equal to $g_i(x) + g_i'(y)$.

We want i sufficiently large so that

$$|(\alpha+\beta) - (g_i(x) + g_i'(y))| < |(\alpha+\beta) - \lfloor\alpha+\beta\rfloor| \; \forall x, y \in [1, \infty].$$

Then we can output the term $\lfloor\alpha+\beta\rfloor$.

Upper bound on $|(\alpha+\beta) - (g_i(x) + g_i'(y))|$:

We have $|\alpha - g_i(x)| < 1/F_{i+1}^2$, $|\beta - g_i'(x)| < 1/F_{i+1}^2$ so

$$|(\alpha+\beta) - (g_i(x) + g_i'(y))| < 2/F_{i+1}^2.$$

Lower bound on $|(\alpha+\beta)-\lfloor\alpha+\beta\rfloor|$:

Let $P(\alpha)=0$ of degree m and $Q(\beta)=0$ of degree n, $P,Q\in\mathbf{Z}[x]$. By computer algebra results, $\alpha+\beta$ is a root of $R(x)=\mathrm{res}_y(P(y),Q(x-y))$ which is of degree at most $m+n$ and

$$M(R)\leq 2^{mn}M(P)^nM(Q)^m \quad [\mathrm{M91}, p173]$$

Assume $R(x)$ satisfies the condition of lemma 3.1. Then, by lemma 3.1,

$$\begin{aligned}
|(\alpha+\beta)-\lfloor\alpha+\beta\rfloor| &> (1+M(R))^{-(m+n)}\\
&> (1+2^{mn}M(P)^nM(Q)^m)^{-(m+n)}\\
&> (1+2^{mn}(m+1)^n\|P\|_\infty^n(n+1)^m\|Q\|_\infty^m)^{-(m+n)}\\
&\text{since } M(P)<\|P\|_2<(m+1)\|P\|_\infty \text{ if } P \text{ not a monomial}\\
&> (2^{mn+m+n+1}m^nn^m\|P\|_\infty^n\|Q\|_\infty^m)^{-(m+n)}
\end{aligned}$$

for some positive constant K. So the number of terms to input that will certainly give a term of $\alpha+\beta$ is the smallest i such that

$$|(\alpha+\beta)-(g_i(x)+g_i'(y))|<\frac{2}{\phi^{2i-2}}$$

$$<\frac{1}{(2^{mn+m+n+1}m^nn^m\|P\|_\infty^n\|Q\|_\infty^m)^{m+n}}<|(\alpha+\beta)-\lfloor\alpha+\beta\rfloor|$$

That is

$$i>O((m+n)(mn+n\|P\|_\infty+m\|Q\|_\infty))$$

If $m=\theta(n)$, we have $i>O(n^2(n+\log\|P\|_\infty+\log\|Q\|_\infty))$.

6 Analysis of Multiplication Algorithm

In this section, we obtain a bound on the number of terms we need to input into the multiplication algorithm in order to be able to produce one term of output, using an analysis similar to that in the previous section. Again, we assume that one term of each of the continued fractions of α and of β are input at the same time.

Again let α and β be two algebraic numbers such that $P(\alpha)=0$, $Q(\beta)=0$ for some $P,Q\in\mathbf{Z}[x]$ with $\deg P=m$ and $\deg Q=n$. Using the same definitions as above, we want i sufficiently large so that

$$|\alpha\beta-g_i(x)g_i'(y)|<|\alpha\beta-\lfloor\alpha\beta\rfloor|\ \forall x,y\in[1,\infty].$$

Then we can output a term, we know $\lfloor\alpha\beta\rfloor$.

Again the two variable function $f(x,y)$ defined in section 1.2 is equal to $g_i(x)g_i'(y)$.

Upper bound on $|\alpha\beta-g_i(x)g_i'(y)|$:

Let $\epsilon_x = g(x) - \alpha$ and $\epsilon'_y = g'(y) - \beta$. Then

$$\begin{aligned}
|\alpha\beta - g_i(x)g'_i(y)| &= |\alpha\beta - (\alpha+\epsilon_x)(\beta+\epsilon'_y)| = |\alpha\epsilon'_y + \beta\epsilon_x + \epsilon_x\epsilon'_y| \\
&< \frac{1}{F_{i+1}^4} + \frac{|\alpha|+|\beta|}{F_{i+1}^2} < \frac{3+\|P\|_\infty + \|Q\|_\infty}{F_{i+1}^2} \\
&< \frac{3+\|P\|_\infty + \|Q\|_\infty}{\phi^{2i-2}}.
\end{aligned}$$

Lower bound on $|(\alpha\beta) - \lfloor\alpha\beta\rfloor|$:

By computer algebra results, $\alpha\beta$ is a root of $R(x) = \mathrm{res}_y(P(y), y^n Q(x/y))$ which is of degree at most $m+n$.

We have

$$M(R) \leq M(P)^n M(Q)^m$$

Assume $R(x)$ satisfies the condition of lemma 3.1. Then, by lemma 3.1,

$$\begin{aligned}
|\alpha\beta - \text{integer}| &> (1+M(R))^{-(m+n)} \\
&> (1+M(P)^n M(Q)^m)^{-(m+n)} \\
&> (1+(m+1)^n\|P\|_\infty^n(n+1)^m\|Q\|_\infty^m)^{-(m+n)} \\
&> (2^{m+n+1}m^n n^m\|P\|_\infty^n\|Q\|_\infty^m)^{-(m+n)}
\end{aligned}$$

for some constant K'. So the number of terms to input that will certainly give a term of $\alpha\beta$ is the smallest i such that

$$|\alpha\beta - g_i(x)g'_i(y)| < \frac{3+\|P\|_\infty + \|Q\|_\infty}{\phi^{2i-2}}$$

$$< \left(2^{m+n+1}m^n n^m\|P\|_\infty^n\|Q\|_\infty^m\right)^{-(m+n)} < |\alpha\beta - \lfloor\alpha\beta\rfloor|$$

That is

$$i > O((m+n)(n\log m + m\log n + n\log\|P\|_\infty + m\log\|Q\|_\infty))$$

If $m = \theta(n)$, we have $i > O(n^2(\log n + \log\|P\|_\infty + \log\|Q\|_\infty))$.

7 Conclusion

We have not analyzed the changes that occur when a term is output. Upon output of c, for addition and multiplication the functions

$$\frac{1}{(g_i(x)+g'_i(y)) - c} \text{ and } \frac{1}{(g_i(x)g'_i(y)) - c}$$

replace

$$(g_i(x)+g'_i(y)) \text{ and } (g_i(x)g'_i(y)).$$

Also the minimal polynomials P, Q of α and β change. Let $[c_1, c_2, \ldots, c_i]$, be the continued fraction of the output, and $h(x) = [c_1, c_2, \ldots, c_i, x]$. After i output steps P becomes $P(h(x))$ with $h^{-1}(\alpha)$ as a root, and similarly for Q.

Finally, the sizes of the numbers involved in the computation and the actual time involved need to be computed.

Of course the analysis of other operations still remains to be done.

I would like to thank prof. Chee Yap for introducing me to this subject and for many useful discussions on this topic.

References

[AN83] A. G. Akritas, K. H. Ng, *Exact Algorithms for Polynomial Real Root Approximation Using Continued Fractions.*, Computing 30, pp 63–76, 1983.

[LW92] L. Lorentzen, H. Waadeland, *Continued Fractions with Applications*, Studies in Computational Mathematics 3, C. Brezinski and L. Wuytack eds., North–Holland, 1992.

[G72] R.W. Gosper, Artificial Intelligence Memo No. 239, MIT, 1972.

[HW84] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Science publications, Fifth edition, 1984.

[K64] A. Ya. Khinchin, *Continued Fractions*, University of Chicago Press, Third Edition, 1964.

[K81] D. E. Knuth, *The Art of Computer Programming*, Vol 2, Addison Wesley, 1981.

[KM74] M. Mendes, *The Depth of a Rational Number.* Colloquia Mathematica Societatis János Bolyai, Topics in Number Theory, Hungary, 1974. Ed. P. Turán. North Holland, pp. 183–194.

[M91] M. Mignotte, *Mathematics for Computer Algebra.* Springer–Verlag, 1991.

[O63] C. D. Olds, *Continued Fractions*, Random House, 1963.

[U48] J. V. Uspensky, *Theory of Equations*, McGraw-Hill, New York, 1948.

[V36] A. J. H. Vincent, *Sur la Résolution des Equations numériques.* Journal de Mathématiques Pures et Appliquées I, pp 341–372, 1936.

[V90] Jean E. Vuillemin, *Exact Real Computer Arithmetic with Continued Fractions*, IEEE Trans. on Computers, Vol. 39, No. 8, Aug 90.