Problem

Given input a/b and Q,

where a, b, Q are n bit integers

$(|a|, |b|, |Q| \leq 2^n)$

want to find $p, q \in \mathbb{Z}$ s.t.

(1) $q \leq Q$.

(2) $\left|\frac{a}{b} - \frac{p}{q}\right|$ is minimized subject to the above.

Goal: find the answer in poly(n) time.

Continued Fractions

Given $\alpha \in \mathbb{R}$, $\alpha > 1$

Do the following process:

$$\alpha = a_0 + \frac{1}{\alpha_1} \qquad a_0 \in \{1, 2, 3, \cdots\}, \ \alpha_1 > 1$$

$$\alpha_1 = a_1 + \frac{1}{\alpha_2} \qquad a_1 \in \{1, 2, 3, \cdots\}, \ \alpha_2 > 1$$

.

$\alpha_N = a_N$ | or forever.

If N exists:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_N}}}$$

Otherwise, it is an infinite expansion.

Run this for a/b.

$$\frac{a}{b} = a_0 + \left(\frac{r_0}{b}\right)$$
$$= q_0$$

$$\frac{b}{r_0} = a_1 + \left(\frac{r_1}{r_0}\right)$$
$$= q_1$$

$$\vdots$$

GCD:

$$a = q_0 b + r_0$$

$$\frac{a}{b} = q_0 + \left(\frac{r_0}{b}\right) \in [0, 1)$$

$$b = q_1 r_0 + r_1$$

$$\vdots$$

$$1$$

$$\frac{r_{N-1}}{r_{N-2}} = q_N + 0 \qquad \Big| \quad r_{N-1} = q_N r_{N-2}$$

Continued fraction expansion of $\frac{a}{b}$

$$= q_0 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_N}}$$

$\downarrow$

Quotients in GCD computation.

(In particular $N \leq 2n$)

Notation:

$$[a_0, a_1, \cdots, a_m] = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_m}}$$

$$= a_0 + \frac{1}{[a_1, a_2, \cdots, a_m]}$$

Convergents of $[a_0, a_1, \ldots, a_m, \ldots]$

$\frac{p_m}{q_m} = [a_0, \ldots, a_m]$ in lowest terms

Formula for p_m, q_m in terms of a_i's.

$$a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \rightarrow \frac{p_1}{q_1}$$

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{q_2}{a_1 a_2 + 1}$$

$$= \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{p_2}{q_2}$$

Lemma

$$p_m = a_m \cdot p_{m-1} + p_{m-2}$$

$$q_m = a_m \cdot q_{m-1} + q_{m-2}$$

$p_0 = a_0$ $\quad p_1 = a_0 a_1 + 1$

$q_0 = 1$ $\quad q_1 = a_1$

Proof

We will show for the sequence p_n, q_n defined in Lemma:

(1) $\forall z \in \mathbb{R}^{>0}. [a_0, a_1, \dots, a_{m-1} + \frac{1}{z}]$

$$= \frac{p_{m-1} z + p_{m-2}}{q_{m-1} z + q_{m-2}} \quad \cdots (*)$$

(2) p_m, q_m are relatively prime

If we showed this,

$$[a_0, \dots, a_m] = [a_0, \dots, a_{m-1} + \frac{1}{a_m}]$$

$$= \frac{p_{m-1} a_m + p_{m-2}}{q_{m-1} a_m + q_{m-2}} = \frac{p_m}{q_m}$$

which is in lowest terms by (2).

Suppose we know $(*)$ for a certain m.

Let us show

$$[a_0, a_1, \ldots, a_{m-1}, a_m + \tfrac{1}{2}] = \frac{p_m 2 + p_{m-1}}{q_m 2 + q_{m-1}}$$

$$\| \quad [a_0, \ldots, a_{m-1} + \frac{1}{a_m + \frac{1}{2}}]$$

by induction

$$= \frac{p_{m-1} \cdot (a_m + \frac{1}{2}) + p_{m-2}}{q_{m-1}(a_m + \frac{1}{2}) + q_{m-2}}$$

$$= \frac{(p_{m-1} a_m + p_{m-2}) \cdot 2 + p_{m-1}}{(q_{m-1} a_m + q_{m-2}) 2 + q_{m-2}}$$

$$= \frac{p_m 2 + p_{m-1}}{q_m 2 + q_{m-1}}$$

$$\begin{bmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{bmatrix} \begin{bmatrix} a_m & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{bmatrix}$$

$\uparrow$ $\qquad$ $\parallel$ $\qquad$ $\uparrow$

$$\begin{bmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{bmatrix} = \begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_2 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_m & 1 \\ 1 & 0 \end{bmatrix}$$

$$\left(p_m q_{m-1} - q_m p_{m-1} \right) = (-1)^{m+1}$$

So GCD $(p_m, q_m) = 1$.

Observation

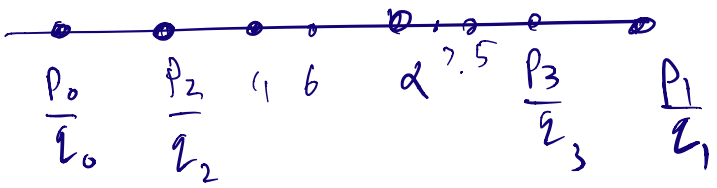
If m even,

$$\frac{p_m}{q_m} \leq \alpha$$

If m odd

$$\frac{p_m}{q_m} \geq \alpha.$$

Obvious



$$\frac{p_m}{q_m} = \frac{p_{m-1} a_m + p_{m-2}}{q_{m-1} a_m + q_{m-2}}$$

$$\in \left[\frac{p_{m-1}}{q_{m-1}} , \frac{p_{m-2}}{q_{m-2}} \right]$$

For $x > 0$,

$$\frac{p_{m-1} x + p_{m-2}}{q_{m-1} x + q_{m-2}} \in$$

$$\frac{a+c}{b+d} \in \left(\frac{a}{b} , \frac{c}{d} \right)$$

Thm Best rational approximation with bounded denominator

Let $\alpha \in \mathbb{R}$, $\alpha \geq 1$. Let $Q \in \mathbb{N}$.

Let $\alpha = [a_0, a_1, \ldots]$

Let q_m be the largest denominator of a convergent with $q_m \leq Q$.

Let t be the largest integer with $t \cdot q_m + q_{m-1} \leq Q$.

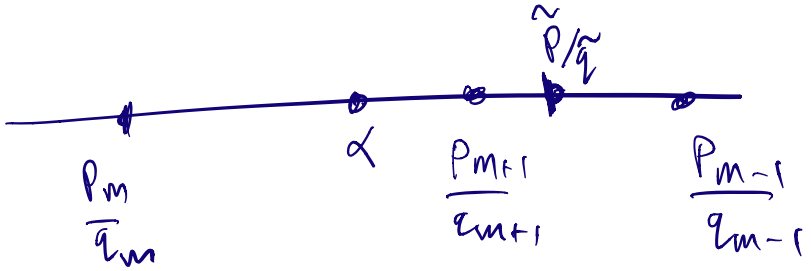
Then the best rational approx to α with denominator $\leq Q$ is either:

1. $\frac{p_m}{q_m}$

2. $\frac{t \cdot p_m + p_{m-1}}{t \cdot q_m + q_{m-1}} \rightarrow \frac{\tilde{p}}{\tilde{q}}$

Proof

Assume m even.



Suppose $\frac{p}{q}$ satisfies:

(1) $q \le Q$.

(2) $\frac{p}{q} \in \left(\frac{p_m}{q_m}, \frac{\tilde{p}}{\tilde{q}} \right)$

Want a contradiction.

Consider $\left| \frac{p}{q} - \frac{p_m}{q_m} \right|$

If is $\geq \frac{1}{q \cdot q_m}$

$$\left(\frac{\tilde{p}}{\tilde{q}} - \frac{p}{q} \right) \geq \frac{1}{q \cdot \tilde{q}}$$

$$\rightarrow \frac{\tilde{p}}{\tilde{q}} - \frac{p_m}{q_m} = \left(\frac{p}{q} - \frac{p_m}{q_m} \right) + \left(\frac{\tilde{p}}{\tilde{q}} - \frac{p}{q} \right)$$

$$\geq \frac{1}{q} \cdot \left(\frac{1}{q_m} + \frac{1}{\tilde{q}} \right)$$

$$\frac{p}{\tilde{q}} - \frac{p_m}{q_m} = \frac{t \cdot p_m + p_{m-1}}{t \cdot q_m + q_{m-1}} - \frac{p_m}{q_m}$$

$$= \frac{t \cdot p_m q_m + p_{m-1} q_m - t p_m q_m - p_m q_{m-1}}{(t \cdot q_m + q_{m-1}) \cdot q_m}$$

$$= \frac{p_{m-1} q_m - p_m q_{m-1}}{\tilde{q} \cdot q_m}$$

$$= \frac{(-1)^m}{\tilde{q} \cdot q_m} = \frac{1}{\tilde{q} \cdot q_m} \quad \text{small}$$

So $\frac{1}{q} \cdot \left(\frac{1}{q_m} + \frac{1}{\tilde{q}} \right) \leq \frac{1}{\tilde{q} \cdot q_m}$

$$\Downarrow$$

$$\frac{1}{q} \left(\frac{1}{q_m} + \frac{1}{t \cdot q_m + q_{m-1}} \right) \leq \frac{1}{q_m \cdot (t \cdot q_m + q_{m-1})}$$

$$\Updownarrow \qquad (\to Q \text{ by defn of } t)$$

$$\frac{1}{q} \quad \frac{(t+1)q_m + q_{m-1}}{q_m(t\cdot q_m + q_{m-1})} \leq \frac{1}{q_m(t\,q_m + q_{m-1})}$$

But $q \leq Q$

So contradiction.

Dirichlet.

Thm

$\alpha \in \mathbb{R}$, not rational.

$\exists$ infinitely many $\frac{p}{q}$ s.t.

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Thm

$\alpha \in \mathbb{R}$, $Q \in \mathbb{N}$

$\exists\, q \leq Q$ s.t. and p

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q\cdot Q}$$

$$|q\alpha - p| < \frac{1}{Q}.$$