Quantum Information & Quantum Computing

Problems Set X
Due

Continuous fraction expansion:

If \( 0 < \alpha < 1 \) then let \( a_1 = a(\alpha) \) denote the integer part of \( 1/\alpha \) and let \( \alpha_1 = G(\alpha) \) denote the fractional part of \( 1/\alpha \). \( G : (0, 1) \rightarrow [0, 1] \) is called the Gauss map. Then \( G^n \) will denote the \( n \)th iterated of \( G \), defined recursively by \( G^n(\alpha) = G^{n-1}(G(\alpha)) \). Moreover, \( a_n \) will denote the integer part of \( 1/G^{n-1}(\alpha) \) namely, \( a_n = a(G^{n-1}(\alpha)) \).

1. Draw the graph of the Gauss map.
2. Show that if \( \alpha_n = G^n(\alpha) \), then

\[
\alpha = a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n + a_{n+1}}}.
\]  

Remark: The previous formula (1) is called the continuous fraction expansion of \( \alpha \) and it is denoted by \( \alpha = [a_1, a_2, \cdots, a_n, \cdots] \). Setting \( \alpha_n = 0 \) gives a fraction denoted by \( p_n/q_n \) and called a convergent of \( \alpha \).

3. Use a handpocket calculator to solve this question
   (a) Compute the continuous fraction expansion of \( \alpha = 271/391 \) (Remark: this is a convergent of \( \ln 2 \)).
   (b) Make the algorithm explicit.
   (c) If \( \alpha \) is rational, does an ordinary handpocket calculator give the exact result? If not explain why?

4. The golden mean is the number \( 0 < \sigma = (\sqrt{5} - 1)/2 < 1 \).
   (a) Show that \( 1 + \sigma = 1/\sigma \).
   (b) Deduce its continuous fraction expansion.
   (c) It will be shown later (see question (7e)) that its convergent are given by \( F_{n-1}/F_n \) where \( F_0 = F_1 = 1 \) and \( F_{n+1} = F_n + F_{n-1} \). The \( F_n \)'s are called the Fibonacci numbers.
   Give the explicit values of the \( F_n \)'s for \( n \leq 11 \).
   (d) Prove, by recursion, that \( F_n \geq (1/\sigma)^{n-1} \).
   (e) The result proved in question (7e) show that if \( p_n/q_n \) is the \( n \)-th convergent of \( \alpha \), then \( q_n \geq F_n \). Conclude that the algorithm giving the continuous fraction expansion of \( p/q \) terminates after \( n = O(\ln q) \) steps.

Remark: It can be proved that each such step requires \( O((\ln q)^2) \) gates of elementary arithmetic.
5. Show that \( \alpha = \frac{p}{q} \) is a fraction if and only if there is an \( n \) such that \( \alpha_n = 0 \) (Hint: show that if \( \alpha \) is a fraction, so is \( G(\alpha) \)).

6. A map \( F : \mathbb{R} \to \mathbb{R} \) is called \textit{harmonic}, whenever it is of the form

\[
F(x) = F_A(x) = \frac{p + rx}{q + sx}, \quad rq - sp = \pm 1 \quad A = \begin{bmatrix} q & s \\ p & r \end{bmatrix},
\]

for some real numbers \( p, q, r, s \).

(a) Show that the composition of \( F_A \) and \( F_B \) is the map \( F_{AB} \). In particular the composition of two harmonic maps is harmonic.

(b) If \( A \) and \( B \) have integral entries, show that so does \( AB \).

(c) What values are taken on by \( \det A ? \)

7. If \( a \) is an integer larger than or equal to 1, let \( f_a \) be the map \( f_a : x \in [0, 1] \mapsto 1/(a + x) \in [0, 1] \).

(a) Show that \( f_a \) is harmonic and give the expression of the corresponding matrix that will be denoted by \( T_a \).

(b) Show that the continuous fraction decomposition of \( \alpha \) can be expressed as

\[
\alpha = f_{a_1} \circ f_{a_2} \circ \cdots \circ f_{a_n}(\alpha_n)
\]

(2)

(c) Conclude that there are integers \( p_n, q_n, r_n, s_n \) such that

\[
\alpha = \frac{p_n + r_n\alpha_n}{q_n + s_n\alpha_n},
\]

(3)

and gives the corresponding matrix \( A_n \) in term of a product of the \( T_{a_k} \)’s.

(d) Compute \( p_0, q_0, r_0, s_0 \).

(e) Show recursively that

\[
r_n = p_{n-1}, \quad s_n = q_{n-1}, \quad p_{n+1} = a_n p_n + p_{n-1}, \quad q_{n+1} = a_n q_n + q_{n-1}.
\]

(f) Show that \( q_n p_{n-1} - q_{n-1} p_n = (-1)^n \). In particular show that \( p_n \) and \( q_n \) are prime to each other.

(g) Prove from eq. (2) that \( \alpha \) is an increasing function of \( \alpha_n \) if \( n \) is even, and is decreasing if \( n \) is odd.

(h) Conclude that

\[
\frac{p_{2m}}{q_{2m}} \leq \frac{p_{2m+2}}{q_{2m+2}} \leq \alpha \leq \frac{p_{2m+1}}{q_{2m+1}} \leq \frac{p_{2m-1}}{q_{2m-1}}.
\]

(i) Show that

\[
|\alpha - \frac{p_n}{q_n}| \leq \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2}.
\]
8. Let now $p$ and $q$ be coprime integers such that $p < q$. Using the continuous fraction expansion of $p/q$, prove the Bezout theorem, namely, that there are $p', q' \in \mathbb{Z}$ such that $pq' + qp' = 1$ integers.

9. Let now $p$ and $q$ be coprime integers such that $|\alpha - p/q| < 1/2q^2$. In this question it will be proved that $p/q$ is a convergent of $\alpha$.

(a) Show that $|\alpha - p/q| < 1/(2q^2 - q)$ and that $|\alpha - p/q| < 1/2$.

(b) If $p/q = 1$, show that there is $\alpha' \in (0, 1)$ such that

$$\alpha = \frac{1}{1 + \alpha'}.$$ 

Conclude then that $1$ is a convergent for $\alpha$.

(c) Assume now that $p = 1$ and $q \geq 2$. Using the question (9a), show that one of the two possibilities occurs:

\[(i) \quad q \leq \frac{1}{\alpha} < \frac{q}{1 - 1/2q - 1}, \quad \text{and} \quad (ii) \quad \frac{q}{1 + 1/2q - 1} < \frac{1}{\alpha} < q.\]

Then show that there is $0 \leq \alpha' < 1$ such that

in case $(i) \quad \alpha = \frac{1}{q + \alpha'}, \quad \text{in case (ii)} \quad \alpha = \frac{1}{q - 1 + 1/\alpha'}.$

Then conclude that in both cases, $1/q$ is a convergent of $\alpha$.

(d) Assume now that $2 \leq p < q$. Then let $a \geq 1$ and $0 \leq r \leq p - 1$ be the ratio and the rest in the Euclidean division of $q$ by $p$, namely $q = ap + r$. Since $p$ and $q$ are coprime, conclude that $1 \leq r \leq p - 1$. Using the question (9a), show that there is $\alpha' \in (0, 1)$ such that

$$\alpha = \frac{1}{a + \alpha'}, \quad \text{with} \quad |\alpha' - \frac{r}{p}| < \frac{1}{2p^2 - p}.$$ 

(e) Using the previous argument recursively, conclude that $p/q$ is a convergent of $\alpha$. 