Quantum Computation:
Zusammenfassung der 12. Vorlesung (06.02.09)

2.3,2 *Auswertung durch Kettenbruchentwicklung*

Wie am Schluß des letzten Abschnitts angedeutet wurde, lässt sich dass Ergebnis eines Laufs des Quantgenalgorithmus zur Ordnungsbestimmung durch Kettenbruchentwicklung des Messergebnisses erhalten. Um dies zu verstehen, müssen wir die Kettenbrüche etwas geneuer betrachten.

Kettenbrüche lassen sich mit reellen Zahlfolgen belibiger Länge bilden. Hier genügt es jedoch, Kettenbrüche endlicher Länge

$$x = [a_0 a_1 a_2 \dots a_N] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\cdots\cdots\cdots}{a_{N-1} + \cfrac{1}{a_N}}}}}$$

mit positiven Nennern, d.h. $a_o \in \mathbf{R}$, und $a_1, a_2 \dots, a_N \in \mathbf{R}_+$, sowie die spezielleren einfachen Kettenbrüche, d.h. $a_o \in \mathbf{Z}$, und $a_1, a_2 \dots, a_N \in \mathbf{N}$ zu betrachten.. Kettenbrüche kann man abkürzen, indem man

$$\begin{aligned} [a_o a_1 a_2 \dots a_N] &= [a_o a_1 a_2 \dots a_{n-1} [a_n, \dots a_N]] \\ &= a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\cdots\cdots\cdots}{a_{n-1} + \cfrac{1}{[a_n \dots a_N]}}}}} \end{aligned}$$

schreibt. Kettenbrüche mit positiven Nennern gehen dabei in ebensolche über. Der Kettenbruch

$$a'_n := [a_n \dots a_N]$$

heisst dann der n-te vollständige Nenner. Der Kettenbruch

$$\frac{p_n}{q_n} := [a_0 a_1 a_2 \dots a_n]$$

heisst der n-te Näherungsbruch von $x = [a_0 a_1 a_2 \ldots a_N]$. Die vorstehend definierten Begriffe verknüpft der im folgenden Satz behauptete Algorithmus, der auch als Euklidischer Algothmus bekannt ist:

Satz: Für Kettenbrüche gilt allgemein mit den vorstehenden Bezeichnungen

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \quad p_0 = a_0, \quad p{-}1 = 1, \quad p_{-2} = 0; \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_{-1} = 0, \quad q_{-2} = 0. \end{aligned}$$

Beweis : Es gilt

$$\begin{aligned} [a_0] &= \frac{a_0}{1} = \frac{p_0}{q_0}, \\ [a_0 a_1] &= a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{a_1 p_0 + p_{-1}}{a_1 q_0 + q_{-1}} = \frac{p_1}{q_1}, \\ [a_0 a_1 a_2] &= a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} \\ &= \frac{(a_0 a_1 + 1)a_2 + a_0}{a_1 a_2 + 1} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{p_2}{q_2}. \end{aligned}$$

Wir machen nun die Induktionsannahme

$$[a_0 a_1 a_2 \ldots a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

Dann folgt

$$\begin{aligned} [a_0 a_1 a_2 \ldots a_n a_{n+1}] &= [a_0 a_1 a_2 \ldots a_{n-1}(a_n + \frac{1}{a_{n+1}})] \\ \frac{(a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}})q_{n-1} + q_{n-2}} &= \frac{(a_n a_{n+1} + 1) + a_{n+1} p_{n-2}}{(a_n a_{n+1} + 1)q_{n-1} + a_{n+1} q_{n-2}} \\ \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} &= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}, \end{aligned}$$

was die Induktionsannnahme bestätigt. Folgerungen aus diesem zentralen Satz sind:

Satz: Es gilt mit den vorstehenden Bezeichnungen

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$

oder auch

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_{n-1} q_n}.$$

Beweis : Für $n = 0$ gilt

$$p_0 q_{-1} - p_{-1} q_0 = (-1)^{0+1},$$

und für $n = 1$ gilt

$$p_1 q_0 - p_0 q_1 = (a_1 a_0 + 1)1 - a_0 a_1 = (-1)^{1+1}.$$

Aus der Induktionsannaahme

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$

folgt

$$\begin{aligned} p_{n+1} q_n - p_n q_{n+1} &= (a_{n+1} p_n + p_{n-1}) q_n - p_n (a_{n+1} q_n + q_{n-1}) \\ &= p_{n-1} q_n - p_n q_{n-1} = -(-1)^{n+1} = (-1)^{(n+1)+1}, \end{aligned}$$

was die Annahme bestätigt.

Satz: Es gilt mit den vorstehenden Bezeichnungen

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

oder auch

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

Beweis :

$$\begin{aligned} p_{nn} q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2} (a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1} = (-1)^n a_n. \end{aligned}$$

Die folgenden zwei Sätze gelten für Kettenbrüche mit positiven Nennern. In diesem Fall gilt auch $p_n, q_n > 0$, $n = 1, 2, \ldots, N$. Für

$$x = [a_o a_1 a_2 \ldots a_N] \quad \text{sei} \quad x_n = \frac{p_n}{q_n} \quad \text{so dass} \quad x = x_N.$$

Eine unmittelbare Folgerung aus dem oben zuerst bewiesenen Satz ist:

Satz: Mit den vorstehenden Bezeichnungen gilt für $2 < n < N$

$$x = [a_o a_1 a_2 \ldots a_N] = \frac{a'_n p_{n-1} + p_{n-2}}{a'_n q_{n-1} + q_{n-2}}.$$

Mittelbar über die beiden Sätze danach erhält man für die Näherungsbrüche x_n:

Satz: Für natürliche Zahlen k gilt $x_{2(k-1)} < x_{2k} < x$ so lange $2k < N$ ist, und $x < x_{2k+1} < x_{2(k-1)+1}$ so lange $2k + 1 < N$ ist. Je nacchdem, ob N gerade oder ungerade ist, ist x das größte bzw. kleinste Element einer dieser Folgen.

Für einfache Kettenbrüche ist $p_n, q_n \in \mathbf{N}$, $n = 1, 2, \ldots, N$, und es gelten überdies die folgenden drei Sätze.

Satz: Es gilt

$$q_0 \leq q_1 < q_2 \cdots < q_{N-1} < q_N$$

Beweis : Da $a_n \in \mathbf{N}$ für $n \geq 1$ und $q_0 = 1$ ist, gilt $q_0 \leq a_1 q_0 \leq q_1$ und für $n \geq 2$ gilt

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} > q_{n-1}.$$

Satz: Es gilt

$$n \leq q_n, \quad \text{und} \quad n < q_n \quad \text{für} \quad 4 \leq n \leq N.$$

Beweis : Die Behauptung gilt für $n = 0, 1$ und ferner ist $q_2 = a_2 q_1 + q_0 \geq a_2 + 1 \geq 2$ und $q_3 = a_3 q_2 + q_1 \geq a_2 + 1 \geq 2 \geq 2 + 1 = 3$. Schließlich ist

$$q_n = a_n q_{n-1} + q_{n-2} \geq n - 1 + n - 2 = 2n - 3 > n \quad \text{für} \quad n \geq 4.$$

Satz: Für einfache Kettenbrüche gilt $(p_n, q_n) = 1$.

Beweis: Wgen

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$

enthält der von p_n und q_n erzeugte Modul ganzer Zahlen die 1 und ist deshalb $\mathcal{S}_1$. Damit sind p_n und q_n teilerfremd.

Der Wert eines einfachen Kettenbruuches endlicher Länge ist offenbar stets eine rationale Zahl. Es gilt aber auch die Umkehrung dieser Implikation, wie der folgende Satz zeigt.

Satz: Sei $x \in \mathbf{Q}$. Dann gibt es eine natürliche Zahl N, eine ganze Zahl a_0 und natürliche Zahlen a_n, $n = 1, 2, \ldots, N$, so dass $x = [a_o a_1 a_2 \ldots a_N]$ ist.

Beweis: Es gilt

$$\begin{aligned}
x \in \mathbf{Q} \quad &\Rightarrow \quad x = a_0 + \xi_0,\ a_0 \in \mathbf{Z},\ 0 \le \xi_0 < 1 \quad \text{und falls} \\
\xi_0 \neq 0 \quad &\Rightarrow \quad \frac{1}{\xi_0} = a_1 + \xi_1,\ a_1 \in \mathbf{N},\ 0 \le \xi_1 < 1 \quad \text{und falls} \\
\xi_1 \neq 0 \quad &\Rightarrow \quad \frac{1}{\xi_1} = a_2 + \xi_2,\ a_2 \in \mathbf{N},\ 0 \le \xi_2 < 1 \quad \text{und falls} \\
\xi_2 \neq 0 \quad &\Rightarrow \quad \frac{1}{\xi_2} = a_3 + \xi_3,\ a_3 \in \mathbf{N},\ 0 \le \xi_3 < 1 \quad \ldots
\end{aligned}$$

Dieser "Kettenbruchalgorithmus" kann fortgesetzt werden, solange $\xi_n \neq 0$ ist und erzeugt offenbar die Nenner für den n-ten Näherungsbruch x_n von x, wenn er mit dem n-ten Schritt abgebrochen wird. Ist $\xi_{N+1} = 0$, dann ist $x = [a_o a_1 a_2 \ldots a_N]$. - Es bleibt zu zeigen, dass dieser Fall für $x \in \mathbf{Q}$ nach endlich vielen Schritten eintreten muss. Dazu schreiben wir $x = \frac{a}{k}$ mit $a \in \mathbf{Z}$, $k \in \mathbf{N}$ und $(a, k) = 1$, dann ist

$$a = a_0 k + \xi_0 k.$$

Falls $\xi_0 \neq 0$ ist, dann folgt wegen $a - a_o k \in \mathbf{N}$ auch $k_1 := \xi_0 k \in \mathbf{N}$, so dass mit $\frac{1}{\xi_0} = \frac{k}{k_1}$

$$k = a_1 k_1 + \xi_1 k_1 \quad \wedge \quad a = a_0 k + k_1$$

folgen. Falls $\xi_1 \neq 0$, dann verfährt man analog und erhält

$$k_1 = a_2 k_2 + \xi_2 k_2 \quad \wedge \quad k = a_1 k_1 + k_2 -$$

Falls $\xi_2 \neq 0$ ist, dann verfährt man analog und erhält

$$k_2 = a_3 k_3 + \xi_3 k_3 \quad \wedge \quad k_1 = a_2 k_2 + k_3.$$

Solange $\xi_{n-1} \neq 0$ ist, hat man also

$$k_{n-1} = a_n k_n + \xi_n k_n \quad \wedge \quad k_{n-2} = a_n k_n + k_{n+1}$$

und es folgt

$$k > k_1 > k_2 > k_2 > \cdots > k_n \quad \wedge \quad k, k_i \in \mathbf{N}.$$

Nach N Schritten, wobei $N \leq k$ gilt, muß also der Fall $\xi_{N+1} = 0$ eintreten und die Nenner eines einfachen Kettenbruchs endlicher Länge mit dem Wert $x = [a_o a_1 a_2 \ldots a_N]$ sind bestimmt.

Nun gilt für den letzten Nenner entweder $a_N = 1$ oder $a_N \geq 2$. Im ersten Fall ist

$$\frac{1}{a_{N-1} + \dfrac{1}{a_N}} = \frac{1}{a_{N-1} + \dfrac{1}{1}} = \frac{1}{a_{N-1} + 1},$$

und man kann den Kettenbruch um einen Nenner verkürzen. Der letzte Nenner ist dann größer oder gleich 2:

$$x = [a_o a_1 a_2 \ldots a_{N-1} 1] = [a_o a_1 a_2 \ldots (a_{N-1} + 1)].$$

Im zweiten Fall ist

$$\frac{1}{a_N} = \frac{1}{(a_N - 1) + \dfrac{1}{1}},$$

und man kann den Kettenbruch um einen Nenner verlängern. Der letzte Nenner ist dann gleich 1:

$$x = [a_o a_1 a_2 \ldots a_N] = [a_o a_1 a_2 \ldots (a_N - 1) 1].$$

Es gilt also:

Satz: Sei $x \in \mathbf{Q}$. Dann hat man entweder die Wahl, x durch einen einfachen Kettenbruch mit gerader oder Ungerader Länge N darzustellen, oder die Wahl, x durch einen einfachen Kettenbruch mit dem letzten Nenner gleich 1 oder größer als 1 darzustellen.

Wir zeigen im übernächsten Satz, dass die Darstellung von $x \in \mathbf{Q}$ durch einen einfachen Kettenbruch bis auf diese Alternativen eindeutig ist. Die Aussage des nächsten Satzes wird im Beweis des Eindeutigkeitssatzes verwendet.

Satz: Mit Ausnahme des Falles $n = N-1 \ \wedge \ a_N = 1$, in dem für den $(N-1)$-ten vollständigen Nenner $[a'_{N-1}] = a_{N-1} + 1$ gilt, ist für einfache Kettenbrüche $[a'_n] = a_n$.

Beweis: Für $x \notin \mathbf{Z}$ gilt $a_0 = [x] < x$

$$x = a'_0 = a_0 + \frac{1}{a'_1} \quad \wedge \quad a'_1 > a_1 \in \mathbf{N} \quad . \Rightarrow . \quad [a'_0] = a_0.$$

Für $1 \leq n \leq N-2$ gilt

$$a'_n = a_n + \frac{1}{a'_{n+1}} \quad \wedge \quad a'_{n+1} > a_{n+1} \in \mathbf{N} \quad . \Rightarrow . \quad [a'_n] = a_n.$$

Wegen

$$a'_{N-1} = a_{N-1} + \frac{1}{a_N}$$

sind zwei Fälle zu unterscheiden. Falls $a_N > 1$, dann gilt auch $[a'_{N-1}] = a_{N-1}$, aber falls $a_N = 1$, dann gilt $[a'_{N-1}] = a_{N-1} + 1$.

Satz: Für einfache Kettenbrüche folgt aus

$$x = [a_o a_1 a_2 \ldots a_N] = [b_o b_1 b_2 \ldots b_M], \quad a_N > 1, \ b_M > 1,$$

dass $N = M$ und $a_n = b_n$, $n = 0, 2, 3, \ldots, N$.

Beweis: Es gilt $[x] = a_0 = b_0$. Dann gilt auch $x = a_0 + \frac{1}{a'_1} = a_0 + \frac{1}{b'_1}$ und damit $a'_1 = b'_1$ und $[a'_1] = [b'_1]$, so dass nach dem vorstehenden Satz $a_1 = b_1$ folgt. Aus der Induktionsannahme $a_k = b_k$ für $k = 3, 4, \ldots, n$ folgt

$$x = [a_o a_1 dots a_{n-1 a'_n}] = [b_o a_1 a_2 \ldots a_{n-1} b'_n],$$

d.h.

$$x = \frac{a'_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{b'_n p_{n-1} + p_{n-2}}{b'_n q_{n-1} + q_{n-2}}.$$

Der Zähler der Differenz dieser Ausdrücke verschwindet also, d.h.

$$\begin{aligned} 0 &= (a'_n p_{n-1} + p_{n-2})(b'_n q_{n-1} + q_{n-2}) - (b'_n p_{n-1} + p_{n-2})(a'_n q_{n-1} + q_{n-2}) \\ &= a'_n p_{n-1} q_{n-2} + p_{n-2} b'_n q_{n-1} - (b'_n p_{n-1} q_{n-2} + p_{n-2} a'_n q_{n-1}) \\ &= (a'_n - b'_n)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = (a'_n - b'_n)(-1)^n. \end{aligned}$$

Damit ist $a'_n = b'_n$ und auf Grund des vorstehenden Satzes folgt $a_n = b_n$, was die Induktionsannahme bestätigt. Man bemerke, dass ie Voraussetzng $a_n, b_n > 1$ den Ausnahmefall für $n = N - 1$ ausschliet. Die Gleichheit der Nenner gilt also für $n \leq N$, falls o.B.d.A. f$N \leq M$ angenommen wird. - Die Annahme $N < M$ führt zum Widerspruch, denn aus

$$x = \frac{p_N}{q_N} = \frac{b'_{N+1} p_N + p_{N-1}}{b'_{N+1} q_N + q_{N-1}}$$

folgt

$$0 = q_N(b'_{N+1} p_N + p_{N-1}) - p_N(b'_{N+1} q_N + q_{N-1}) = q_N p_{N-1} - q_{N-1} P_N = (-1)^N.$$