Quantum Computation:
Zusammenfassung der 11. Vorlesung (08. u. 15.07.2011)

2.3 *Ordnungsbestimmung*

2.3.1 *Die Ordnung einer Restklasse modulo M*

Sei M eine natürliche Zahl und $x \in \mathbf{Z}$, dann gibt es eine ganze Zahl, $k \in \mathbf{Z}$, so dass

$$kM \leq x < (k+1)M \quad \text{bzw.} \quad x = kM + r, \quad 0 \leq r < M.$$

Bei Division von x durch M bleibt ein **positiver** Rest r. Als eine *Restklasse modulo* M bezeichnet man die Menge derjenigen $x \in \mathbf{Z}$, für die bei Division durch M der gleiche positive Rest r übrig bleibt. Die Restklassen modulo M sind durch die Relation

$$x \sim_M y \quad :\Leftrightarrow \quad (\exists k \in \mathbf{Z})\; x - y = kM,$$

die offenbar reflexiv, symmetrisch uns transitiv ist, also eine Äquivalenzrelation bildet. Für jede natürliche Zahl M zerfällt $\mathbf{Z}$ deshalb in die Vereinigung disjunkter Restklassen modulo M, $[x]_M$. Da jede Restklasse genau ein Element r mit $0 \leq r < M$ enthält, das die Klasse repräsentiert, $[x]_M = [r]_M$, gibt es genau M Restklassen modulo M.

Algebraisch bilden die Restklassen modulo M einen Ring. Die Addition

$$[x]_M + [y]_M; = [x+y]_M$$

definiert eine Klassenoperation, d,h, es ist gleichgültig, mit welchen Elementen $z \in [x]_M$ und $z' \in [y]_M$ die Summe gebildet wird, sie ist stets die Klasse $[x+y]_M$. Die Addition ist offenbar assoziativ, kommutativ, das netrale Element ist $[0]_M$ und das Inverse von $[x]_M$ ist $[-x]_M$. Die Multiplikation

$$[x]_M[y]_M := [xy]_M$$

definiert ebenfalls eine Klassenoperation, denn mit $z \in [x]_M$, $z' \in [y]_M$ gelten

$$xy = (k_x M + r_x)(k_y M + r_y) = (k_x k_y M + r_x k_y + k_x r_y)M + r_x r_y$$

und

$$zz' = (k_z M + r_x)(k_{z'} M + r_y) = (k_z k_{z'} M + r_x k_{z'} + k_z r_y)M + r_x r_y,$$

so dass die Differenz $xy - zz'$ (ohne Rest) durch M teilbar ist. Offenbar ist die Multiplikation auch assoziativ, kommutativ, und $[1]_M$ ist das neutrale Element. Offenbar gilt auch das Distributivgesetz

$$[x]_M([y]_M + [z]_M) = [x]_M[y]_M + [x]_M[z]_M.$$

Damit bilden die Restklassen modulo M algebraisch einen Ring. Der Bequemlichkeit halber wird auch

$$x = z \,\mathrm{mod} M \quad \text{anstelle von} \quad [x]_M = [z]_M$$

geschrieben.

Um die Frage nach der Existenz von inversen Elementen für die multiplikative Halbgruppe eines Restklassenringes zu beantworten, führen wir den Begriff eines *Moduls ganzer Zahlen* ein: Eine Teilmenge

$$\mathcal{S} \subseteq \mathbf{Z} \quad \text{heißt Modul, falls} \quad x, y \in \mathcal{S} \Rightarrow x \pm y \in \mathcal{S}$$

gilt. Speziell ist die Menge $\{0\}$ ein Modul, der *Nullmodul*. Die Null ist in einem Modul wegen $x - x \in \mathcal{S}$ stets enthalten. Mit $k \in \mathbf{Z}$ und $x \in \mathcal{S}$ ist auch $kx \in \mathcal{S}$. Sind $k, l \in \mathbf{Z}$ und $x, y \in \mathcal{S}$, dann sind auch $kx + ly \in \mathcal{S}$. Ist $\mathcal{S} \neq \{0\}$, dann gilt $\mathcal{S} \cap \mathbf{N} \neq \emptyset$, und diese Menge enthält ein kleinstes Element:

$$(\exists\, d \in \mathcal{S} \cap \mathbf{N})(\forall a \in \mathcal{S})\ 0 \leq a < d \Rightarrow a = 0.$$

Für diese Zahl d gilt nun die folgende

Behauptung: $x \in \mathcal{S} \cap \mathbf{N} \Rightarrow (\exists\, n \in \mathbf{N})\ x = nd.$

Beweis:

$$\left.\begin{array}{r} x = nd + c,\ 0 \leq c < d \\ \Rightarrow\ c = x - nd \in \mathcal{S} \end{array}\right\} \Rightarrow\ c = 0.$$

Damit haben wir gezeigt

Satz: Sei $\mathcal{S} \neq \{0\}$, dann gibt es ein $d \in \mathcal{S} \cap \mathbf{N}$, so dass für jedes Element $x \in \mathcal{S}$ ein $k \in \mathbf{Z}$ existiert mit $x = kd$, also $\mathcal{S} = \{kd | k \in \mathbf{Z}\}$. Insbesondere ist jedes Element von $\mathcal{S}$ (ohne Rest) durch d teilbar.

Im Folgenden werden wir für die Teilbarkeit (ohne Rest) ein Symbol verwenden. Sei $c \in \mathbf{N}$ und $a \in \mathbf{Z}$, wir schreiben

$$c|a \quad :\Leftrightarrow \quad (\exists k \in \mathbf{Z})\ a = kc$$

und nennen a durch c teilbar.

Definition: Sei $d \in \mathbf{N}$, $a, b \in \mathbf{Z}$. Wir schreiben

$$(a, b) = d \quad :\Leftrightarrow \quad d|a \wedge d|b \wedge .(\forall c > d)\ c \not| a \vee c \not| b.$$

und nennen d den größten gemeinsamen Teiler (ggT) von a und b.

Offenbar ist $\mathcal{S}(a, b) := \{ka + lb | k, l \in \mathbf{Z}\}$ ein Modul und damit existiert ein $d' \in \mathbf{N}$ mit $\mathcal{S}(a, b) := \{kd' | k \in \mathbf{Z}\}$. Jedes Element von $\mathcal{S}(a, b)$ ist durch d' teilbar, also auch a und b. Somit gilt $d' \leq d = (a, b)$. Andererseits gilt $d|a$ und $d|b$ und damit $d|ka + lb$ für $k, l \in \mathbf{Z}$, also gilt $d|x$ für alle $x \in \mathcal{S}(a, b)$, insbesondere gilt $d|d'$. Damit ist auch $d \leq d'$, also $d = d'$. Damit haben wir den folgenden Satz bewiesen.

Satz: $\mathcal{S}(a, b) := \{kd | d = (a, b), k \in \mathbf{Z}\}$.

Aus diesem Satz folgen unmittelbar:

Satz: Seien $a, b, c \in \mathbf{Z}$, $(a, b) = d$ dann gilt

$$(\exists\, x, y \in \mathbf{Z})\ xa + yb = c \quad \Leftrightarrow \quad d|c.$$

Insbesondere gilt $(a, b) = d = x'a + y'b,\ x', y' \in \mathbf{Z}$.

Satz: Jeder gemeinsame Teiler von a und b ist ein Teiler von $d = (a, b)$.

Wir können nun die Frage beantworten, welche Elemente $[x]_M$ des Restklassenringes modulo M invertierbar sind. Es gilt

$$[x]_M[y]_M = [1]_M \ \Leftrightarrow\ (\exists k \in \mathbf{N})\, yx + kM = 1 \ \Leftrightarrow\ .1 = ld,\, l \in \mathbf{Z}. \ \Leftrightarrow\ d = 1,$$

wobei $d = (x, M)$ ist. Damit gilt:

Satz: $[x]_M$ ist genau dann invertierbar, wenn $(x, M) = 1$ ist. Insbesondere ist der Restklassenring modulo M ein Körper genau dann, wenn M eine Primzahl ist.

Die im vorletzten Absatz aus den Eigenschaften eines Moduls ganzer Zahlen gefolgerten Sätze erlauben den Beweis zweier grundlegender Theoreme. Als Primzahlen werden bekanntlich die von 1 verschiedenen natürlichen

Zahlen bezeichnet, die keinen von 1 verschiedenen Teiler haben. Das folgende Theorem wird auch der "erste Euklidische Satz" genannt.

Satz (Euklid): Sei p eine Primzahl und $a, b \in \mathbf{Z}$, dann gilt

$$p|ab \quad \Leftrightarrow \quad .p|a \vee p|b.$$

Beweis: Sei $p|ab$ und etwa $p \not| a$, dann gilt $(a, p) = 1$ und damit gibt es ganze Zahlen x und y mit $xa + yp = 1$. Folglich gilt $xab + ypb = b$. $p|ab$ und $p|pb$ führen sofort auf $p|b$.

Jede von 1 verschiedne natürliche Zahl n ist trivialerweise ein Produkt von von Primzahlen. Schreibt maan

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_N^{a_N}, \quad p_1 < p_2 < p_3 < \dots < p_N, \quad a_i > 0,$$

dann heißt dies die Standarddarstellung der Primfaktorzerlegung. Aus dem ersten Euklidischen Satz folgern wir nun:

Satz: Die Primfaktorzerlegung einer Zahl $1 < n \in \mathbf{N}$ ist eindeutig.

Beweis: Seien

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_N^{a_N} = q_1^{b_1} q_2^{b_2} q_3^{b_3} \dots q_M^{b_M}$$

Standarddarstellungen. Da $q_j|n$ muss nach dem Satz von Euklid mindestens einer der $\sum_1^N a_i$ "p"-Primfaktoren durch q_j teilbar und damit gleich q_j sein. Damit folgt $\{q_j\}_{j=1,2,\dots,q_M} \subseteq \{p_i\}_{i=1,2,\dots,q_N}$. Analog zeigt man $\{p_i\}_{i=1,2,\dots,q_N} \subseteq \{q_j\}_{j=1,2,\dots,q_M}$. Aus der Gleichheit der Mengen folgt $M = N$ und aus der Stadardanordnung $p_i = q_i$. Nehmen wir an $a_i < b_i$, dann folgt für $n/p_i^{a_i}$ sowohl $p_1|(n/p_i^{a_i})$ als auch $p_1 \not|(n/p_i^{a_i})$, ein Widerspruch. Ebenso ist $ab_i < a_i$ nicht möglich, also gilt $a_i = b_i$.

Wir beweisen weitere für uns nützliche allgemeine Sätze. Im Beweis des ersten Satzes von Euklid haben wir gezeigt, dass für $k \in \mathbf{N}$

$$\frac{ab}{k} \in \mathbf{Z} \wedge (a, k) = 1 \quad . \Rightarrow . \quad \frac{b}{k} \in \mathbf{Z}$$

ist, wobei k nicht notwendig eine Primzahl sein muß. Diese Aussage findet auch im folgenden Theorem Anwendung.

Satz: Sei $(x, M) = d$, dann gilt

$$xy = xz \,\mathrm{mod} M \quad \Leftrightarrow \quad y = z \,\mathrm{mod} \frac{M}{d}.$$

Beweis: Es gilt

$$x = kd, \quad M = Kd, \quad (k, K) = 1,$$

letzteres, weil andernfalls d nicht der größte gemeinsame Teiler wäre, was vorausgesetzt wurde. Es folgt

$$\mathbf{Z} \ni \frac{xy - xz}{M} = \frac{kd(y-z)}{Kd} = \frac{k(y-z)}{K} \quad \Leftrightarrow \quad \frac{(y-z)}{K} \in \mathbf{Z},$$

weil $(k, K) = 1$. Aus $K = M/d$ folgt die Behauptung.

Satz: Sei $(x, M) = 1$ und $\{[y_m]_M\}_{m=0,1,\ldots,M-1}$ ein vollständiges System von Restklasssen modulo M. Dann ist auch $\{[xy_m]_M\}_{m=0,1,\ldots,M-1}$ ein vollständiges System von Restklasssen modulo M.

Beweis: Wegen $(x, M) = d = 1$ ist nach dem vorsthenden Satz $x(y_m - y_n) = 0 \,(\mathrm{mod} M)$ äquivalent zu $y_m - y_n = 0 \,\mathrm{mod} M$. Da letzteres mur für $m = n$ gelten kann, folgt die Behauptung.

Alternativ kann man auch argumentieren, dass für $(x, M) = 1$ die Abbildung $[z]_M \mapsto [xz]_M$ eine Bijektion der Restklassen modulo M auf sich ist, weil $[x]_M$ invertierbar ist.

Satz: Sei $(a, M) = d$, dann ist die Gleichung

$$ax = b \,\mathrm{mod} M$$

genau dann lösbar, wenn d Teiler von b ist. Sie hat genau d modulo M verschiedene Lösungen. Speziell ist sie eindeutig lösbar, wenn $d = 1$ ist und insbesondere ist in diesem Fall das Inverse von $a \,\mathrm{mod} M$ die Lösung von $ax = 1 \,\mathrm{mod} M$.

Beweis: Wir haben oben gezeigt

$$(a, M) = d \;\Rightarrow .(\exists\, x, y \in \mathbf{Z})\; ax + My = b \;\Leftrightarrow\; d|b. .$$

Wegen $b = ax + My = ax \,\mathrm{mod}\, M$ ist dies die erste Behauptung des Satzes. Für $d = 1$ ist $ax = b \,\mathrm{mod} M$ stets lösbar, und, da $[a]_M$ invertierbar und

$[a]_M^{-1}[b]_M = [x]_M$ ist, ist die Lösung modulo M eindeutig. Für $d > 1$ und $d|b$ seien $a = da'$, $M = dM'$ und $b = db'$. Dann gilt

$$ax = b \,\mathrm{mod} M \quad \Longleftrightarrow \quad a'x = b' \,\mathrm{mod} M',$$

und, weil $(a', M') = 1$ ist, hat die Gleichung mit den gestrichenen Koeffizienten eine eindeutige Lösung. Diese sei $x' \,\mathrm{mod} M'$. Modulo M sind aber

$$x' \,\mathrm{mod} M,\ (x' + M') \,\mathrm{mod} M,\ (x' + 2M') \,\mathrm{mod} M, \ldots$$
$$\ldots, (x' + (d-1)M') \,\mathrm{mod} M$$

d paarweise verschiedene Lösungen der ursprünglichen Gleichung.

Die *Eulersche Funktion* $\phi : \mathbf{Z} \to \mathbf{N}$ gibt tdie Anzahl der paaerweise verschiedenen Restklassen $[x]_M$ mit $(x, M) = 1$, d.h. die Anzahl der der invertierbaren Elemente des Restklassenringes modulo M an. Nstürlich gilt dafür auch der Satz:

Satz: Ist $\{x_i\}_{i=1,2,3,\ldots,\phi(M)}$ ein vollständiges System invertierbarer Restklassen und ist $(y, M) = 1$, dann ist auch $\{yx_i\}_{i?1,2,3,\ldots,\phi(M)}$ ein solches System.

Für die Eulersche Funktion gilt nun der Satz:

Satz: Wenn $(y, M) = 1$ ist, gilt

$$y^{\phi(M)} = 1 \,\mathrm{mod} M.$$

Beweis: Für ein vollständiges System invertierbarer Restklassen $\{[x_i]_M\}_{i=1,2,3,\ldots,\phi(M)}$ und $(y, M) = 1$, dann gilt

$$\prod_{i=1}^{\phi(M)} yx_i = \prod_{i=1}^{\phi(M)} x_i \,\mathrm{mod} M,$$

weil auf beiden Seiter der Gleichung das Produkt der invertierbaren Elemente des Restklassenringes steht. Somit gilt

$$y^{\phi} \prod_{i=1}^{\phi(M)} x_i = \prod_{i=1}^{\phi(M)} x_i \,\mathrm{mod} M,$$

und weil das Produkt invertierbarer Restklassen modulo M invertierbar ist folt die behauptete Gleichung

$$y^{\phi(M)} = 1 \,\mathrm{mod} M.$$

Definition: Sei $(x, M) = 1$, dann heißt $r_M(x) = \min\{l \in \mathbf{N} | x^l = 1 \,\mathrm{mod} M\}$ die Ordnung der Restklasse $[x]_M$, oder kurz die *Ordnung von* x modulo M.

Offenbar gilt $1 \leq r_M(x) \leq \phi(M)$. Offenbar ist

$$\mathcal{M}_M(x) := \{n \in \mathbf{Z} \,|\, x^n = 1 \,\mathrm{mod} M\} \neq \{0\}$$

ein Modul ganzer Zahlen, denn mit $m, n \in \mathcal{M}_M(x)$ ist $m \pm n \in \mathcal{M}_M(x)$, und es gibt ein $0 < d \in \mathcal{M}_M(x)$ mit $m \; \mathcal{M}_M(x) \to m = kd$, $k \in \mathbf{Z}$. Es ist also $r_M(x) = d$, das kleinste positive Element von $\mathcal{M}_M(x)$ und der größte gemeinsame Teiler aller Elemente von $\mathcal{M}_M(x)$. Insbeondere ist $\phi(M) \in \mathcal{M}_M(x)$ und damit gilt $r_M(x) | \phi(M)$. Für Primzahlen P ist $\phi(P) = P - 1$, denn alle von $[0]_P$ verschiedenen Restklassen modulo P sind invertierbar. Damit haben wir gezeigt:

Satz: Sei $(x, M) = 1$, dann ist die Ordnung $r_M(x)$ von x modulo M ein Teiler von $\phi(M)$, $r_M(x) | \phi(M)$. Für Primzahlen P gilt $r_P(x) | P - 1$.Es gilt $x^n = 1 \,\mathrm{mod} M$ je nach dem, ob $n = k r_M(x)$, $k \in \mathbf{Z}$, wahr ist oder nicht.

Einige Beispiele sollen das Vorstehende illustrieren:

$(2, 3) = 1$	$2^2 = 1 \,\mathrm{mod}\, 3$	$r_3(2) = 2$
$(2, 4) = 2$	$2^2 = 0 \,\mathrm{mod}\, 4$	$[2]_2$ ist "nilpotent"
$(2, 5) = 1$	$2^4 = 1 \,\mathrm{mod}\, 5$	$r_5(2) = 4$
$(2, 6) = 2$	$2^{2k+1} = 2 \,\mathrm{mod}\, 6$	
	$2^{2k} = 4 \,\mathrm{mod}\, 6$	
$(5, 21) = 1$	$5^6 = 1 \,\mathrm{mod}\, 21$	$r_{21}(5) = 6$

Klassische Algorithmen zur Ordnungsbestimmung sind von exponentieller Dauer.

2.3.2 *Ordnungsbestimmung und Phasenbestimmung*

Jede Restklasse modulo M, $[x]_M$, liegt durch Rest bei Division von x durch M, $0 \leq r_x < M$, $r_x \in [x]_M$, bzw. $r_x = x \,\mathrm{mod} M$, fest. Es gilt

$r_x = [0, M-1] \cap [x]_M$. Ist $\{|k)\}_{k=0,1,2,\ldots,(M-1)}$ eine Orthonormalbasis im $\mathbf{C}^M$, dann definiert jede Restklasse $[x]_M$ mit $x \bullet k := [0, M-1] \cap [xk]_M$ durch

$$|k) \longmapsto |x \bullet k)$$

eine lineare Transformation auf $\mathbf{C}^M$. Für $(x, M) = 1$ ist diese Transformation unitär.

Satz: Sei $(x, M) = 1$, dann ist die lineare Transformation

$$\begin{array}{rcl} U_x : \mathbf{C}^M & \longrightarrow & \mathbf{C}^M \\ |k) & \longmapsto & |x \bullet k) \end{array}$$

unitär. Ist $r := r_M(x)$ die Ordnung von x modulo M und gilt $(y, M) = 1$, dann sind

$$\chi_s(y) = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^l \bullet y)$$

Eigenvektore n von U_x zum Eigenwert $e^{\frac{2\pi i}{r} s}$, (s=0,1,2,. . . ,r-1). Schließlich gilt

$$|y) = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \chi_s(y).$$

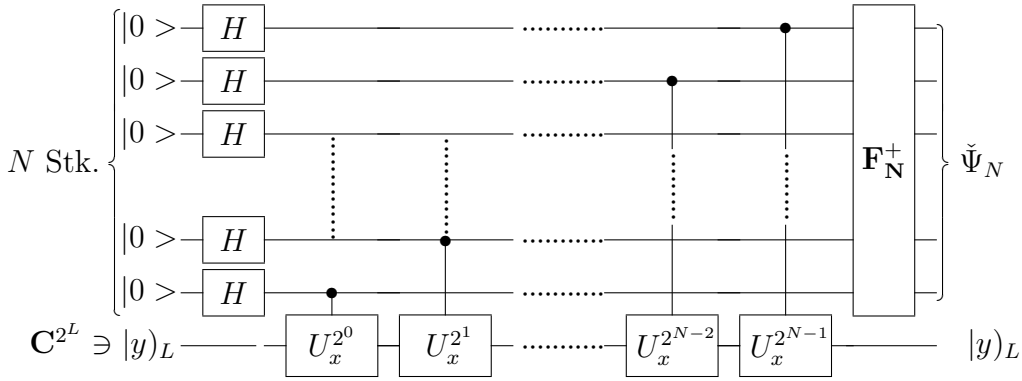
Beweis: U_x ist unitär, weil für $(x, M) = 1$ das vollständige System $[k]_M$, $(k = 0, 1, 2, \ldots, M-1)$ von Restklasssen modulo M auch $[xk]_M$ ein vollständigen System von Restklassen ist, so dass die Basisvektoren nur permutiert werden. Weiterhin ist

$$\begin{aligned} U_x \chi_s(y) &= \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^{l+1} \bullet y) \\ &= \frac{1}{\sqrt{r}} \sum_{l=1}^{r} e^{-\frac{2\pi i}{r} (l-1)s} |x^l \bullet y) \\ &= e^{\frac{2\pi i}{r} s} \frac{1}{\sqrt{r}} \left(\sum_{l=1}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^l \bullet y) + e^{-\frac{2\pi i}{r} rs} |x^r \bullet y) \right) \\ &= e^{\frac{2\pi i}{r} s} \frac{1}{\sqrt{r}} \left(\sum_{l=1}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^l \bullet y) + e^{-\frac{2\pi i}{r} 0s} |(1 \bullet y) \right) \\ &= e^{-\frac{2\pi i}{r} s} \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^l \bullet y) = e^{\frac{2\pi i}{r} s} \chi_s(y), \end{aligned}$$

damit sind die $\chi_s(y)$ Eigenvektoresn von U_x zum Eigenwert $e^{\frac{2\pi i}{r}s}$, (s=0,1,2,. . . ,r-1). Schließlich ist

$$\begin{aligned}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\chi_s(y) &= \frac{1}{r}\sum_{s=0}^{r-1}\sum_{t=0}^{r-1}e^{-\frac{2\pi i}{r}ts}|x^t \bullet y) \\ &= \sum_{t=0}^{r-1}\frac{1}{r}\sum_{s=0}^{r-1}e^{-\frac{2\pi i}{r}ts}|x^t \bullet y) \\ &= \sum_{t=0}^{r-1}\delta_{t0}|x^t \bullet y) = |1 \bullet y) = |y)\end{aligned}$$

Die Aussagen dieses Theorems erlauben nun, die Ordnungsbestimmung mit Hilfe der Phasenbestimmung zu erreichen. Um die Ordnung von x modulo M zu bestimmen, muss man zunächst $U_x : \mathbf{C}^M \to \mathbf{C}^M$ implementieren. Dazu benötigt man ein Register mit In $L = [\log_2 M]$ Qubits, $2^{L-1} < M \leq 2^L$. Die Quantenalgorithmen der Grundrechenarten reichen dann aus, um $x \bullet k$ zu berechnen und damit $U_x \oplus \mathbf{1}_{2^N-(M+1)}$ reversibel zu implementieren. Da r unbekannt ist , hat man jedoch nicht $\chi_s(y)$ als Eingabe im zweitn Register der Phasenbestimmung zur Verfügung, sondern nur $|y)_L \in \mathbf{C}^{2^L}$ mit $(y, M) = 1$, etwa $|1)_L = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\chi_s(1)$. Der Algorithmus



würde bei Eingabe von $\chi_s(y)$ den Zustand $\sum_{k=0}^{2^N-1} a_k(\frac{s}{r})|k)_N$ liefern, mit $a_k(\frac{s}{r}) = \delta_{k\frac{s}{r}}$ falls $2^N\frac{s}{r} \in \mathbf{N}$. Letzteres ist jedoch nicht zu erwarten, so dass man mit einem Fehler gemäß Abschnitt 2.3.1 rechnen muss. Auf eine geeignete Eingrenzung des Fehlers durch Wahl von N kommen wir noch

zurück. Sie wird durch ein Theorem über die Approximation rationaler Zahlen durch Kettenbrüche festgelegt. Da anstelle von $\chi_s(y)$ nur $|y)_L = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \chi_s(y)$ eingegeben werden kann, liefert der Algorithmus

$$\check{\Psi}_N = \sum_{s=0}^{r-1} \sum_{k=0}^{2^N-1} a_k(\frac{s}{r})|k)_N.$$

Das Ergebnis κ der Messung von $A = \sum_k \frac{k}{2^N}|k)(k|$ am ersten Register ist eine rationale Zahl, da nur 2^N Stellen hinter dem Komma zur Verfügung stehen. Die zu bestimmende Zahl ist auch eine rationale Zahl, $\frac{s}{r}$, wobei der Nenner oder ein Vielfaches des Nenners die gesuchte Ordnung von x modulo M sein kann. Das Verfahren besteht nun darin, dass der Messwert κ in einen einfachen Kettenbruch endlicher Länge G entwickelt wird, der etwa mit $G = 4$ die Gestlt

$$\kappa = a_o + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_G}}}} =: [a_0 a_1 a_2 a_3 a_G],$$

hat, wobei $a_0 = 0$ wegen $0 \leq \kappa < 1$ und $a_j \in \mathbf{N}$ für $j \geq 1$ gilt. Dadurch liegen G Näherungsbrüche $\kappa_1 = [0a_1] = \frac{1}{a_1}$, $\kappa_2 = [0a_1a_2] = \frac{p_2}{q_2}$, $\kappa_3 = [0a_1a_2a_3] = \frac{p_3}{q_3}, \ldots,$ $\kappa_{G-1} = [0a_1a_2a_3 \ldots a_{G-1}] = \frac{p_{G-1}}{q_{G-1}}$, $\kappa_G = [0a_1a_2a_3 \ldots a_G] = \frac{p_G}{q_G}$, wobei $p_j, q_j \in \mathbf{N}$ und $(p_j, q_j) = 1$ gelten, fest. Diese Entwicklung und die Nenner der Näherungsbrüche lassen sich klassisch mit einem Algorithmus polynomialer Dauer erhalten. Erstaunlicher Weise lässt sich zeigen, dass $\frac{s}{r}$ mit einem dieser Näherungbrüche übereinstimmt, wenn nur der Messwert κ um weniger als $\frac{1}{2r^2}$ von $\frac{s}{r}$ abweicht, d.h. $|\kappa - \frac{s}{r}| < \frac{1}{2r^2}$ gilt. Nun ist $r < M$, so dass diese Voraussetzung bei Wahl der maximalen Abweichung $\epsilon \leq \frac{1}{2M^2} < \frac{1}{2r^2}$ für ein $\frac{s}{r}$, $s = 1, 2, 3, \dot{,} N - 1$ erfüllt sein muss. Die Ordnung r von x modulo M ist dann also der Nenner oder, wegen $(p_n, q_n) = 1$, ein ganzes Vielfaches des Nenners von einem der Näherungsbrüche des Messwertes κ. Dies gilt allerdings nur mit einer gewissen Wahrscheinlichkeit, die noch abzuschätzen ist. Man prüft mit einem klassischen Agorithmus mit polynomialer Dauer, ob eine der Zahlen mq_j, $m = 1, 2, 3, \ldots, \frac{M}{2}$, $j = 1, 2, 3, \ldots, G$ die Ordnung von x modulo M ist. Wenn man die Ordnung nicht findet, muss man κ verwerfen und neu beginnen.