Quantum Computation:
Zusammenfassung der 11. Vorlesung (23.01.09)

2.3 *Ordnungsbestimmung*

2.3.1 *Die Ordnung einer Restklasse modulo M*

Die ganzen Zahlen $z \in \mathbf{Z}$, für die bei Division durch eine natürliche Zahl $M \in \mathbf{N}$ derselbe positibe Rest $0 \leq r < M$ bleibt, bilden eine Restklasse modulo M. Eine nicht negative Zahl z gehört zur Restklasse $[r]_M$ genau dann, wenn $z = kM + r$ mit $k \in \mathbf{N}$ ist. Eine negative Zahl z' gehört zur Restklasse $[r]_M$ genau dann, wenn $z' = -k'(M+1)+r$, $k' \in \mathbf{N}$, ist. $x, y \in \mathbf{Z}$ gehören derselben Restklasse an, wenn ihre Differenz durch M (ohne Rest) teilbar ist d.h. $|x - y| = kM$ gilt. Für

$$x \in [z]_M \text{ schreibt man auch } x = z\,(\mathrm{mod} M).$$

Wie man leicht zeigen kann, bilden die Restklassen modulo M mit $[x]_M + [y]_M := [x + y]_M$ und $[x]_M[y]_M := [xy]_M$ einen Ring. $[x]_M$ ist genau dann invertierbar, wenn x,M teilerfremd sind, d.h. der größte gemeinsame Teiler $(x, M) = 1$ ist. Mithin ist der Restklassenring modulo M genau dann ein Körper, wenn M eine Primzahl ist. Wir beweisen einige allgemeinere Sätze, wobei wir die Eindeutigkeit der Primzahlzerlegung und den ersten Satz von Euklid, dass für eine Primzahl p und $a, b \in \mathbf{N}$

$$\frac{ab}{p} \in \mathbf{Z} \quad . \Leftrightarrow . \quad \frac{a}{p} \in \mathbf{Z} \vee \frac{b}{p} \in \mathbf{Z}$$

gilt, ohne Beweis Gebrauch machen. Eine hier wichtige Folgerung ist, 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.

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

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

weil $(k, K) = 1$ (*Erster Satz von Euklid*).

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

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

Anders ausgedrückt ist für $(x, M) = 1$ die Abbildung $[z]_M \mapsto [xz]_M$ eine Bijektion der Restklassen auf sich.

Um den nächsten Satz beweisen zu können, benötigen wir den Begriff eines Moduls ganzer Zahlen: Eine Teilmenge $\mathcal{S} \subseteq \mathbf{Z}$ heisst Modul, wenn mit $x, y \in \mathcal{S}$ auch $(x+y), (y-x) \in \mathcal{S}$ gilt. Somit sind auch alle ganzen Vielfachen eines Elementes von $\mathcal{S}$ in $\mathcal{S}$ enthalten.

Satz: Sei $\mathcal{S} \subseteq \mathbf{Z}$ ein Modul und $\mathcal{S} \neq \{0\}$. Dann gibt es eine Zahl $d \in \mathbf{N}$, so dass

$$\mathcal{S} = \{x | x = zd, z \in \mathbf{Z}\} =: \mathcal{S}_d.$$

Beweis: $d = \min(\mathcal{S} \cap \mathbf{N})$ leistet dies: Sei $c \in \mathcal{S}$ und $c = zd + r$, $0 \leq r < d$. Da $r = c - zd \in S$ ist, gilt $r = 0$, denn d ist minimal.

Aus diesem Satz folgert man leicht:

Satz: Seien $a, b \in \mathbf{N}$, und $\mathcal{S} = \{x | x = z_a a + z_b b, z_a, z_b \in \mathbf{Z}\} = \mathcal{S}_d$, dann ist d der größte gemeinsame Teiler von a und b, d.h. $d = (a, b)$.

Beweis: d teilt jedes Element von S, also auch a und b. Also ist $d \leq (a, b)$. Nun folgt aus $(a, b)|a$ und $(a, b)|b$, dass $(a, b)|(z_a a + z_b b)$. Also ist

jedes Element von $\mathcal{S}$ ein Vielfaches von (a, b), d.h. $\mathcal{S} = \mathcal{S}_{(a,b)}$ und damit ist $d = (a, b)$.

Es gilt also stets

$$\{x | x = z_a a + z_b b, z_a, z_b \in \mathbf{Z}\} = \mathcal{S}_{(a,b)}.$$

Zwei Folgerungen dieses Satzes sind:

Satz: Die Gleichung

$$ax + by = c$$

hat genau dann ganzzahlige Lösungen x, y, wenn mit $d = (a, b)$ auch $d|c$ gilt. Insbesondere hat $ax + by = z$ ganzzahlige Lösungen, denn $d = 1$ ist-

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

Die erste dieser Folgerungen liefert den Beweis für den folgenden Satz, der den Anlass für die Betrachtung der Moduln gegeben hat.

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 dann d 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: Für eine beliebige ganze Zahl y gilt $ax = ax + My \,(\mathrm{mod} M)$, also liefert jede ganzzahlige Lösung von $ax + My = b$ eine solche von $ax = b \,(\mathrm{mod}\, M)$. Umgekehrt ist für jede Lösung von $ax = b \,(\mathrm{mod} M)$ die ganze Zahl $b - ax$ ein Vielfaches von M, also gibt es ein y' mit $ax + My' = b$. Mit $(a, M) = d$ ist $d|b$ also ein notwendiges und hinreichendes Kriterium für die Lösbarkeit von $ax = b \,(\mathrm{mod}\, M)$. Für $d = 1$ ist $ax = b \,(\mathrm{mod} M)$ stets lösbar, und, da die Abblidung $[x]_M \mapsto [ax]_M$ bijektiv ist, ist die Lösung in diesem Fall eindeutig. Für $d > 1$ und $d|b$ sei $a = da'$, $M = dM'$ und $b = db'$. Dann gilt

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

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

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

d paarweise verschiedene Lösungen der ursprünglichen Gleichung.

Satz: Sei $(x, M) = 1$, dann gibt es ein $n \in \mathbf{N}$, so dass $x^n = 1 \,(\mathrm{mod} M)$.

Beweis: Es gilt für alle $n \in \mathbf{N}$, dass $x^n \neq 0 \,(\mathrm{mod}\, M)$. Dis gilt für $n = 1$, denn sonst wäre M gemeinsamer Teiler von x und M. Nehmen wir an, dass $x^n = 0 \,(\mathrm{mod}\, M)$ und o.B.d.A. n minimal, dann gilt $x^n = kM$ und mithin $\mathbf{N} \ni x^{n-1} = \frac{kM}{x}$. Da nach Voraussetzung M nicht durch x geteilt wird, muss (*Erster Satz von Euklid*) $k_1 = \frac{k}{x} \in \mathbf{N}$ und damit schon $X^{n-1} = k_1 M$, d.h. $x^{n-1} = 0 \,(\mathrm{mod}\, M)$ gelten. Dies widerspricht der Minimalität von n.- Da es nur $M - 1$ Restklassen $[z]_M$ mit $z \neq 0 \,(\mathrm{mod}\, M)$ gibt, muss es natürliche Zahlen $n \neq m$, o.b.d.A. $m - n = l > 0$ geben. mit $x^{n+l} = x^n \,(\mathrm{mod}\, M)$ geben. Da aus $(x, M) = 1$ auch $(x^n, M) = 1$ folgt, hat $[x^n]_M$ ein Inverses, also gilt $x^l = 1 \,(\mathrm{mod}\, M)$.

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 Ordnung von x modulo M.

Da der Restklassenring modulo M nur $M - 1$ von Null verschiedene Elemente hat, ist $r_M \leq N$. Das eindeutige Inverse einer Restlasse $[x_M]$ mit $(x, M) = 1$ ist $[x^{r_M(x)-1}]_M$.

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"
$(2, 5) = 1$	$2^4 = 1 \,(\mathrm{mod}\, 5)$	$r_5(2) = 4 \,(\mathrm{mod}\, 5)$
$(2, 6) = 2$	$2^{2k+1} = 2 \,(\mathrm{mod}\, 6)$	
	$2^{2k} = 4 \,(\mathrm{mod}\, 6)$	
$(5, 21) = 1$	$5^6 = 1 \,(\mathrm{mod}\, 21)$	$r_{21}(5) = 6$

Klassische Algorithmen zur Ordnungsbestimmung sind von exponentieller Dauer.

2.3.2 *Ordnungsbestimmung und Phasenbestimmung*

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

$$U_x : \mathbf{C}^M \quad \longrightarrow \quad \mathbf{C}^M$$

die mit $x \bullet k := [0, M - 1] \cap [xk]_M$ für eine Basis $\{|k)\}_{k=0,1,2,\ldots,M-1}$ durch

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

festliegt, 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

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

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. Weiterhin ist

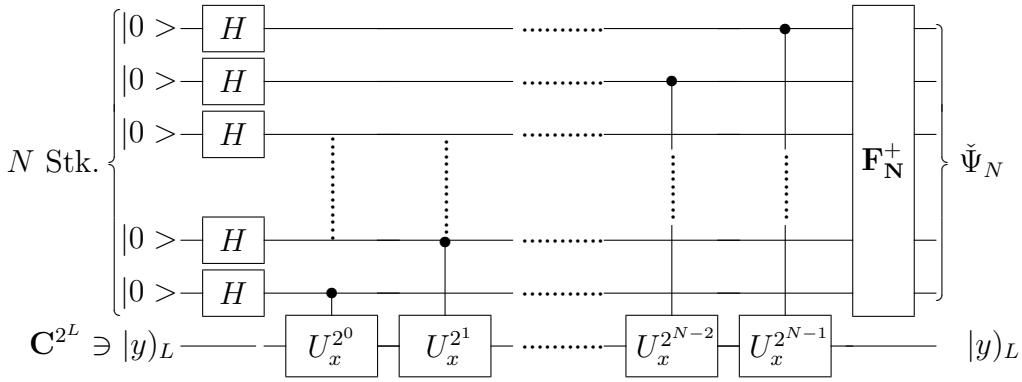
$$\begin{aligned}
U_x \chi_s(y) &= \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^{l+1} \bullet y) \\
&= \frac{1}{\sqrt{r}} \sum_{l=1}^{r} e^{-\frac{2\pi i}{r} (l-1)s} |x^l \bullet y) \\
&= e^{\frac{2\pi i}{r} s} \frac{1}{\sqrt{r}} \left(\sum_{l=1}^{r-1} e^{-\frac{2\pi i}{r} ls} |x^l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

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

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

Die Aussagen dieses Theorems erlauben nun, die Ordnungsbestimmung mit Hilfe der Phasenbestimmung zu erreichen. In einem Register mit $L = [\log_2 M]$ Qubits lässt sich $U_x \bigoplus_{M+1}^{2^L} \mathbf{1}$, wobei $\mathbf{1}$ der Einsoperator in $\mathbf{C}^2$ ist, mit Hilfe der Grundrechenarten reversibel implementieren. Da r unbekannt ist ,lässt sich jedoch $\chi_s(y)$ nicht präparieren. dafür aber $|y)$ mit $(y, M) = 1$, etwa $|1) = \sum_{s=0}^{r-1}\chi_s(1)$. 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 Eingrenzung des Fehlers durch Wahl von N kommen wir noch zurück. Da anstelle von $\chi_s(y)$ jedoch nur $|y)_L = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\chi_s(y)$ eingegeben werden kann, liefert der Algorithmus

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

Damit gilt für das Ergebnis κ der Messung von $A = \sum_k \frac{k}{2^N}|k)(k|$ am ersten Register unter der Hypothese $s = \sigma$, die mit der Wahrscheinlichkeit $\frac{1}{r}$ zutrifft, mit der Wahrscheinlichkeit $q_{|d|\leq\epsilon}(\delta)$

$$\kappa \in [\frac{\sigma}{r} - \epsilon, \frac{\sigma}{r} + \epsilon].$$

Anders ausgedrückt gilt für den gemessenen Wert κ mit der Wahrscheinlichkeitt $q_{|d|\leq\epsilon}(\delta)$

$$\kappa \in \mathcal{M}_r := \bigcup_{s=0}^{r-1} [\frac{s}{r} - \epsilon, \frac{s}{r} + \epsilon]$$

Der gemessene Wert κ ist wegen der endlichen Anzahl von Stellen hinter dem Komma stets eine rationale Zahl. Wie im nächsten Abschnitt gezeigt werden wird, kann κ deshalb in einen einfachen Kettenbruch endlicher Länge G entwickelt werden, etwa mit $G = 4$

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

wobei $a_0 = 0$ wegen $0 \leq \kappa < 1$ und $a_j \in \mathbf{N}$ für $j \geq 1$ gilt. Dadurch liegen G Näherungsbrüche $\kappa_1 = [0a_1] = \frac{1}{a_1}$, $\kappa_2 = [0a_1a_2] = \frac{p_2}{q_2}$, $\kappa_3 = [0a_1a_2a_3] = \frac{p_3}{q_3}, \ldots,$ $\kappa_{G-1} = [0a_1a_2a_3 \ldots a_{G-1}] = \frac{p_{G-1}}{q_{G-1}}$, $\kappa_G = [0a_1a_2a_3 \ldots a_G] = \frac{p_G}{q_G} = \kappa$, 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 von $\epsilon \leq \frac{1}{2M^2} < \frac{1}{2r^2}$ für ein $\frac{s}{r}$, $s = 1, 2, 3, ;N - 1$ erfüllt seein muss, wenn $\kappa \in \mathcal{M}$ gilt. 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. Es gilt allerdings $\kappa \in \mathcal{M}$ nur mit der Wahrscheinlichkeit $q_{|d|\leq\epsilon}(\delta)$. Man prüft nun 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.