Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K10: Faktorisierung am Quantencomputer

Stichworte: Ordnungsbestimmung und Faktorisierung, Quantencomputer, Qubit, Quanten-Fourier-transformation (QFT), Shor-Algorithmus zur Ordnungsbestimmung

---

10.1. **Def.:** Sei $x, N \in \mathbb{N}$, $1 < x < N$, $(x,N)=1$. Die (multiplikative) Ordnung von x mod N ist
$\operatorname{ord}_N(x) := \min\{r \in \mathbb{N};\ x^r \equiv 1\ (N)\}$.

10.2. **Vereinbarung:** In diesem Kapitel sei $N \in \mathbb{N}$ "groß" und ungerade. Schreibe $\operatorname{ord}(x) = \operatorname{ord}_N(x)$.

Wir zeigen zunächst, dass das Faktorisierungsproblem schnell lösbar ist, wenn man Ordnungen von Elementen x in $\mathbb{Z}_N^\times$, d.h. $\operatorname{ord}_N(x)$, schnell berechnen könnte.

10.3. **Satz:** Das Faktorisierungsproblem 9.1 (für N) ist (schnell) lösbar, falls die Bestimmung der Ordnung von x mod N, wo $x, N \in \mathbb{N}$, $1 < x < N$, $(x,N)=1$, möglich ist.

Bew.: Man gehe vor wie folgt: Wähle x zufällig, garantiere $(x,N)=1$ mit eukl. Algo (ansonsten wird damit ein nichttriv. Teiler von N gefunden). Bestimme $r = \operatorname{ord}(x)$.
Ist $2 \nmid r$ oder $2 \mid r$ & $x^{r/2} \equiv -1\ (N)$, wähle neues solches x.
(Die W., dass dies klappt ist hoch, vgl. Beh. 10.4.)
Somit nimm OE an: $2 \mid r$ und $x^{r/2} \not\equiv -1\ (N)$. (*)
Beh. $0 \equiv x^r - 1 = \underbrace{(x^{r/2}-1)}_{\not\equiv 0\ (N)\ \text{da } r=\operatorname{ord}(x)} \cdot \underbrace{(x^{r/2}+1)}_{\not\equiv 0\ (N)\ \text{nach (*)}}\ (N)$, d.h. $p \mid N \Rightarrow p \mid x^{r/2}-1$ oder $p \mid x^{r/2}+1$.
Nicht jeder Primteiler p von N mit $p^e \| N$ erfüllt $p \nmid x^{r/2}+1$, da sonst $p^e \mid x^{r/2}+1$ ($\Leftrightarrow x^{r/2} \equiv -1\ (N)$), $\lightning$. (PFZ von N)
Also ex. Primteiler p von N, für die $p \mid x^{r/2}-1$ gilt.
Mit $(x^{r/2}-1, N)$ kann über den eukl. Algo somit ein nichttriv. Teiler von N bestimmt werden. □

Die Bedingung (*) trifft oft genug ein:

10.4 **Beh.:** Die W., ein $x \bmod N$, $1 < x < N$, $2 \mid \operatorname{ord}(x)$, $x^{\frac{\operatorname{ord}(x)}{2}} \not\equiv -1 \ (N)$, zu finden ist $\geq 1 - \frac{\hat{1}}{2^{k-1}}$.
Also: Bei zufälliger Wahl von $x \bmod N$ trifft man mit hoher Wahrsch. auf ein passendes x.
Hat man Pech, wiederholt man die Wahl solange bis x passend ist. Hier: $k = \omega(N)$.

Bew.: O.E. sei N ungerade und keine Primpotenz (dafür greifen andere Tests).
Ist $N = \prod_{i=1}^{s} p_i^{a_i}$, $r_i := \operatorname{ord}_{p_i^{a_i}}(x)$ und $r = \operatorname{ord}_N(x)$, ist $r = \operatorname{kgV}(r_1, \dots, r_k)$.
Betr. $2^{e_i} \parallel r_i$, $1 \leq i \leq s$. • Sind alle $e_i = 0$, ist $2 \nmid r$, $\frac{r}{2}$ ex. nicht.
• Sind alle $e_i > 0$ und $e_1 = \dots = e_k$, gilt $x^{r_i/2} \equiv -1 \ (p_i^{a_i})$ für $1 \leq i \leq k$.
Dann ist $x^{r/2} \equiv -1 \ (p_i^{a_i})$, $1 \leq i \leq k$, also $x^{r/2} \equiv -1 \ (N)$.
• Die W., ein x_i mit $x_i^{r_i/2} \equiv -1 \ (p_i^{a_i})$ zu finden, wo $r_i := \operatorname{ord}_{p_i^{a_i}}(x_i)$ exakt durch eine bestimmte 2er Potenz 2^e geteilt wird, d.h. $2^e \parallel r_i$, ist $\leq \frac{\hat{1}}{2}$, (ii)
weil die Gruppe $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ zyklisch ist. [Ist g Erzeuger, gilt $\operatorname{ord}(g^j) = \frac{\operatorname{ord}(g)}{(\operatorname{ord}(g), j)}$, was für maximal die Hälfte aller j durch eine bestimmte Potenz 2^e exakt teilbar ist.]
• Für jedes $i = 2, \dots, k$ stimmt die exakte 2er-Potenz in r_i mit der von r_1 überein, die W. dafür beträgt also $\leq \frac{\hat{1}}{2^{k-1}}$. □

10.5 **Bem.:** P. Shor zeigte 1996, dass die Ordnung $\operatorname{ord}(x)$ von zufällig gewählten $x \bmod N$ auf einem Quantencomputer polynomiell schnell berechnet werden kann – also auch das Faktorisierungsproblem (Satz 10.3), auf dem die Sicherheit von RSA u.a. Kryptosysteme beruht! Dabei ist ein Quantencomputer ein Computer, der die physikalischen Gesetze der Quantenmechanik (zusätzlich zu den klassischen) benutzen kann. Sobald solche Quantencomputer gebaut werden, die leistungsfähig genug sind, sind die auf Faktorisierung beruhenden Kryptosysteme damit (für aktuell benutzte Schlüssellängen) in wenigen Minuten "geknackt". Wir möchten in diesem § diesen Algo von P. Shor vorstellen, da er auch z.T. auf der Theorie der KBe beruht (und in einigen Jahrzehnten unser digitales Leben wie z.B. online-Banking, Datenschutz etc., komplett verändern könnte). An Krypto-Alternativen, die Angriffen eines Quantencomputers standhalten würden, wird derzeit geforscht.

10.6. **Quantencomputer:** Ein Quantenregister besteht aus L vielen miteinander gekoppelten Quantensystemen (etwa L vielen NH_3-Molekülen), jedes kann 2 beobachtbare Zustände haben (etwa Spin "up" oder "down" nach der bzw. durch die Messung am NH_3-Molekül, auf welcher Seite des H_3-Dreiecks das N-Atom sitzt).
Diese einzelnen Quantensysteme heißen Qubits.
Schreibe $|j\rangle$, $j \in \mathbb{N}$, wo $j = j_0 + j_1 \cdot 2 + \ldots + j_{L-1} \cdot 2^{L-1}$, $j_0, \ldots, j_{L-1} \in \{0,1\}$, für ein Quantenregister mit den $q := 2^L$ vielen möglichen beobachtbaren Zuständen $|j_0 \ldots j_{L-1}\rangle$ (L Qubits).
$\hookrightarrow 0 \le j \le 2^L - 1$.

Haben so also die möglichen messbaren beobachtbaren Einzel-Zustände $|0\rangle, |1\rangle, \ldots, |q-1\rangle$ für ein Quantenregister. Nach den Gesetzen der Quantenmechanik sind nun beliebige (physikalisch möglichen) Zustände des Registers durch Superposition, d.h. durch bestimmte Linearkombinationen $\sum_{j=0}^{q-1} \alpha_j |j\rangle$ gegeben. (Unterscheidbar nur durch die Wahrscheinlichkeitstupel $(|\alpha_0|^2, |\alpha_1|^2, \ldots, |\alpha_{q-1}|^2) \in [0,1]^q$, wobei $|\alpha_j|^2$ die W. ist, mit der ein bestimmter Messzustand $|j\rangle$ gemessen wird. Haben also $\sum_{j=0}^{q-1} |\alpha_j|^2 = 1$.)
Fassen wir $|0\rangle, \ldots, |q-1\rangle$ als Standard-Basis auf, erlaubt die Quantenmechanik nur unitäre Transformationen, die Zustand $|j\rangle$ auf $\sum_{i=0}^{q-1} c_{ij} |i\rangle$ bringt, d.h. wo $(c_{ij})_{0 \le i,j < q} \in \mathbb{C}^{q \times q}$ eine unitäre Matrix ist (A unitär $:\Leftrightarrow A^{-1} = \bar{A}^T$).
Eine erlaubte und physikalisch durchführbare Transformation ist dabei die QFT:

10.7. **Quanten-Fourier-Transformation (QFT):**
Diese Transformation führt einen Einzel-Zustand $|a\rangle$ über in die Superposition

$$QFT(|a\rangle) = \frac{1}{q^{1/2}} \sum_{c=0}^{q-1} e\left(\frac{ac}{q}\right) |c\rangle$$

der Zustände $|0\rangle, \ldots, |q-1\rangle$.

Wir beschreiben nun den eigentlichen probabilistischen Algorithmus von Shor, der die Ordnung einer Zahl x mod N schnell berechnet:
Shor-Algorithmus: Sei N die (große) nat. Zahl und x mod N gegeben. Gesucht: $r = \mathrm{ord}_N(x)$.

Schritt 1. Ein Quantencomputer bestehe aus zwei Quantenregistern (eins für Input, eins für Output), jeweils der Länge L, wo $q = 2^L$ mit $N^2 < q \leq 2N^2$, die Anzahl der mögl. beobachtbaren Zustände sei. Das erste Register sei durch die Superposition aller Zustände a mod q initialisiert, das zweite mit der Superposition aller Zustände $x^a \bmod N$:

Schreiben dafür $\frac{1}{q^{1/2}} \sum_{a=0}^{q-1} \underbrace{|a\rangle}_{1.\text{Register}} \underbrace{|x^a \bmod N\rangle}_{2.\text{Register}}$.

unitär: $|a\rangle|0\rangle \mapsto |a\rangle|x^a \bmod N\rangle$

[z.B. so machbar: $|0\rangle|0\rangle \xrightarrow{\text{QFT 1.Reg.}} \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} e\left(\frac{a\cdot 0}{q}\right)|a\rangle|0\rangle = \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|0\rangle \mapsto \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle|x^a \bmod N\rangle$.]

Schritt 2. Führe auf dem ersten Register eine QFT durch, erhalten

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e\left(\frac{ac}{q}\right)|c\rangle|x^a \bmod N\rangle.$$

Schritt 3. Führe eine Messung an den Quantenregistern durch.

10.8. **Lemma:** Die Wahrsch., dabei $|c\rangle|x^k \bmod N\rangle$, $0 < k < r = \mathrm{ord}(x)$, zu messen, beträgt $\geq \frac{1}{3r^2}$, falls $|R| \leq \frac{r}{2}$ gilt, wo $R = R(c,r,q)$ der absolut kleinste Rest bei der Division von rc durch q sei, d.h. $rc \equiv R \bmod q$ mit $-\frac{q}{2} < R \leq \frac{q}{2}$ per Def.

[Bew.: s.u.; rc ist also nahe einem Vielfachen von q.]

Die Bed. $|R| \leq \frac{r}{2}$ gilt, wenn ein $d \in \mathbb{Z}$ ex. mit $|rc - dq| \leq \frac{r}{2} \overset{(:qr)}{\iff} \left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$.

Der Bruch $\frac{c}{q}$ darin ist bekannt (c wurde gemessen). Da $q > N^2$, folgt $\left|\frac{c}{q} - \frac{d}{r}\right| < \frac{1}{2N^2}$, $r < N$.

Nach dem Satz Z2.2.6(ii) ← 2TI von Lagrange ist dann $\frac{d}{r}$ notwendig gleich einem NB in der KBt an $\frac{c}{q}$, wobei alle NBe (effektiv) berechnet werden können.

Bei den Zuständen c, die gemessen werden (sehr wahrscheinlich), ist unter den NBen von $\frac{c}{q}$ also ein NB $= \frac{d}{r}$ dabei, wo r die gesuchte Ordnung ist.

Dann erhalten wir einen (gekürzten) NB $\frac{u}{v}$ mit $\frac{d}{r} = \frac{u}{v}$, wo $v \leq N$, und $v \mid r$.

Fall 1): Ist dabei $v = r$, hat man r berechnet und ist fertig.

Fall 2): Ansonsten ist $r = \ell v$, wo ℓ eher klein sein dürfte. Ist v noch nicht die Ordnung, teste dann, ob $2v$, $3v$, ... die gesuchte Ordnung ist.

10.9. **Bem.:** • Fall 1.) tritt häufig genug auf: die Anz. der passenden c mod q, die auf gekürztes $\frac{d}{r}$ führen, ist die Anz. der d mod r mit $(d,r)=1$, also $\varphi(r)$. Die Anz. der dann passenden $|c\rangle|x^k\rangle$ ist dann $r\cdot\varphi(r)$, jeder ist mit W. $\geq \frac{1}{3r^2}$ messbar (laut Lemma 10.8), Erfolg haben wir also mit W. $\geq \frac{r\varphi(r)}{3r^2}$ s.o. $\frac{1}{\log\log(r)}$, vgl. ZT II, Bl. 11 A1(b). Man muss also das Experiment maximal $O(\log\log(r))$ oft wiederholen, bis r gefunden wird, was (in der Praxis) sehr klein ist,

• Die erwartete Gesamtlaufzeit ist nur $O((\log^2 N)(\log\log N)(\log\log\log N))$; vgl. Zahlkörpersieb (K9.4): $O(\exp(c(\log N)^{1/3}(\log\log N)^{2/3}))$. ← Wird mit der Anzahl glatter Zahlen gezeigt, vgl. K9.8/9

10.10. **Bew. von Lemma 10.8:** Die W., $|c\rangle|x^k\rangle$ zu messen, beträgt (laut Quantenmechanik)

$$W=\frac{1}{q^2}\Big|\sum_{\substack{a\\ x^a\equiv x^k (N)}} e\left(\frac{ac}{q}\right)\Big|^2.$$

Da $x^a\equiv x^k (N) \Leftrightarrow a\equiv k\ (r)$, schreibe $a=k+br$, $b\in\mathbb{Z}$.

$$\text{Also: } W=\frac{1}{q^2}\Big|\sum_{b=0}^{\lfloor\frac{q-1-k}{r}\rfloor} e\left(\frac{(br+k)c}{q}\right)\Big|^2=\frac{1}{q^2}\Big|\sum_{b=0}^{\lfloor\frac{q-1-k}{r}\rfloor} e\left(\frac{Rb}{q}\right)\Big|^2.$$

Nun ist nach der Eulerschen Summenformel a1.6 (ZT II) mit $x=\lfloor\frac{q-1-k}{r}\rfloor$, $c=0$, $f(t)=e(\frac{R}{q}t)$ also

$$\frac{1}{q}\sum_{b=0}^{\lfloor\frac{q-1-k}{r}\rfloor} e\left(\frac{Rb}{q}\right)=\frac{1}{q}\int_0^{\lfloor\frac{q-1-k}{r}\rfloor} e\left(\frac{Rt}{q}\right)dt+O\left(\frac{1}{q}\int_0^{\lfloor\frac{q-1-k}{r}\rfloor}(t-\lfloor t\rfloor-\tfrac{1}{2})\cdot 2\pi i\frac{R}{q}e\left(\frac{R}{q}t\right)dt\right)+O\left(\frac{1}{q}\right)$$

für $|R|\leq\frac{r}{2}$

$$\text{Subst. } u=\frac{rt}{q}: \quad =\frac{1}{r}\int_0^{\frac{r}{q}\lfloor\frac{q-1-k}{r}\rfloor} e\left(\frac{R}{r}u\right)du \qquad +O\Big(\underbrace{\frac{1}{q}\cdot\lfloor\frac{q-1-k}{r}\rfloor\cdot\frac{r}{q}}_{\leq 1/q}\Big)+O\left(\frac{1}{q}\right),$$

der Gesamtfehler beträgt hier also nur $O(\frac{1}{q})$. Im $\int$ ersetzen wir die obere Schranke durch 1, dies ergibt weiter einen zusätzlichen Fehler

$$\Big|\frac{1}{r}\int_{\frac{r}{q}\lfloor\frac{q-1-k}{r}\rfloor}^{1} e\left(\frac{R}{r}u\right)du\Big|=\Big|\frac{1}{2\pi iR}e\left(\frac{R}{r}u\right)\Big|_{u=\frac{r}{q}\lfloor\frac{q-1-k}{r}\rfloor}^{u=1}\Big|=\frac{1}{2\pi R}\cdot\Big|e\left(\frac{R}{r}\right)-e\left(\frac{R}{r}\cdot\frac{r}{q}\lfloor\frac{q-1-k}{r}\rfloor\right)\Big|$$

MWS $= \frac{1}{2\pi R} \left| 2\pi i \frac{R}{r} \cdot e\left(\frac{R}{r}\cdot\xi\right) \right| \cdot \left| 1 - \frac{r}{q}\left\lfloor \frac{q-1-k}{r} \right\rfloor \right| \le \frac{1}{r}\cdot\left(1 - \frac{r}{q}\cdot\left(\frac{q-1-k}{r} - 1\right)\right)$

$\xi \in \left[\frac{r}{q}\left\lfloor\frac{q-1-k}{r}\right\rfloor, 1\right]$ $= \frac{1}{r}\left(1 - 1 + \frac{k+1}{q} + \frac{r}{q}\right) \ll \frac{1}{q}$, da $k<r$, also wieder $O(\frac{1}{q})$.

Das S ist $= \frac{1}{r}\int_0^1 e\left(\frac{R}{r}u\right)du = \frac{1}{2\pi i R} e\left(\frac{R}{r}u\right)\Big|_{u=0}^{u=1} = \frac{1}{2\pi R}\cdot\left(e\left(\frac{R}{r}\right) - 1\right)$

$= \frac{1}{2\pi R}\, e\left(\frac{R}{2r}\right)\cdot 2i \sin\left(\pi\frac{R}{r}\right)$, der Betrag davon ist $\frac{1}{\pi R}\left|\sin\left(\pi\frac{R}{r}\right)\right|$, wo $|R| \le \frac{r}{2}$, dieser Ausdruck wird minimal für $R = \pm\frac{r}{2}$ [$\sin(\pi x) \ge 2x$ für $|x| \le \frac{1}{2}$], der Wert dann: $\frac{2}{\pi r}$. Die W. ist dann also $\ge \frac{4}{\pi^2 r^2} + O\left(\frac{1}{q}\right) \ge \frac{1}{3r^2}$, da $q \ge N^2 \ge r^2$, wenn N groß genug ist. □

10.11. Bem.: • Mittlerweile haben erste Prototypen 20 Qubits und mehr. Solche Quantenregister würden also die Faktorisierung von Zahlen $N \le \sqrt{q} = 2^{10} = 1024$ zulassen. Es könnten mit ca. 100 Qubits aber auch schon $N \le \sqrt{2^{100}} = 2^{50} \approx 1{,}1\cdot 10^{15}$ sein. Mit ca. 50 Qubits sollte ein solcher Computer klassischen bereits überlegen sein.

• Weitere Quantenalgorithmen, die klassischen überlegen sind, werden bereits gefunden, z.B. die Auffindung der Minimallösung einer Pellschen G/g. in polynomieller Zeit [Hallgren 2007].

↳ vgl. ZT I, Z19/Z25, dort wird in Z25.8 auch der Satz Z22.6 (ii) von Lagrange benutzt!