Komplexität und Vergleich mit klassischen Algorithmen

Satz Komplexität von Shor's Algorithmus

Shor's Algorithmus benötigt $\tilde{\mathcal{O}}(\log^2 N)$ Gatter.

Beweis:

- Schritt 1 benötigt $n = \mathcal{O}(\log N)$ Hadamard-Gatter.
- Schritt 2 benötigt $\mathcal{O}(n^2 \log n \log\log n) = \tilde{\mathcal{O}}(\log^2 N)$ Gatter.
- QFT_{2^n} in Schritt 5 benötigt $\mathcal{O}(n^2)$ Gatter.
- Schritt 7 benötigt ebenfalls $\mathcal{O}(n^2)$ Gatter.

Klassisch:

- Bester beweisbarer Algorithmus $e^{\mathcal{O}(\sqrt{\log N \log\log N})}$.
- Bester heuristischer Algorithmus $e^{\mathcal{O}(\log^{\frac{1}{3}} N \log\log^{\frac{2}{3}} N)}$ (Number Field Sieve)

Finden der Ordnung und Faktorisieren

Satz Faktorisieren mittels Ordnung

Sei $N = pq$, p, q prim. Gegeben sei ein Algorithmus, der bei Eingabe $(a, N) \in \mathbb{Z}_N^* \times \mathbb{N}$ die Ordnung $\mathrm{ord}_{\mathbb{Z}_N *}(a)$ in Zeit $T(N)$ berechnet. Dann kann N in erwarteter Laufzeit $\mathcal{O}(\log^3 N \cdot T(N))$ faktorisiert werden.

Beweis: Übungsaufgabe.

- Hinweis: Sei $\mathrm{ord}(a) = 2^k t$ mit t ungerade.
- Falls $a^{2^i t} \neq \pm 1$ und $a^{2^{i+1} t} = 1$ für ein $i \in \mathbb{Z}_k$, berechne $\gcd(a^{2^i t}, N)$.

Finden einer Periode und Diskrete Logarithmen

Definition Diskretes Logarithmus Problem (DLP)

Gegeben: Abelsche Gruppe G, $a \in G$ und $\beta \in \langle a \rangle$
Gesucht: $k = \log_b a \in \mathbb{Z}_{\mathrm{ord}(a)}$ mit $a^k = b$

Lösung mittels Finden einer Periode:

- $\mathrm{ord}(a)$ kann mit Hilfe von Shors Algorithmus berechnet werden.
- Wir definieren die Funktion $f(x_1, x_2) = a^{x_1} b^{x_2} = a^{x_1 + k x_2}$.
- Es gilt $f(x_1 + k\ell, x_2 - \ell) = a^{x_1 + k\ell + k x_2 - k\ell} = f(x_1, x_2)$ für $\ell \in \mathbb{Z}_{\mathrm{ord}(a)}$.
- D.h. f ist periodisch mit Periode $(k, 1)$.
- Finden der Periode führt zur Lösung des DLPs.
- Der Quantenschaltkreis für DLP unterscheidet sich von Shor's Schaltkreis lediglich durch die beiden Eingaberegister für x_1, x_2.

Datenbanksuche

Definition Problem der Datenbanksuche

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für genau ein $a \in \mathbb{F}_2^n$
Gesucht: $a \in \mathbb{F}_2^n$

Klassisch:

- Sei $N = 2^n$. Wir benötigen $\Omega(N)$ Aufrufe, um a zu bestimmen.

Idee für einen Quantenschaltkreis:

- Erzeuge eine Superposition $|\psi\rangle$ aller möglichen Eingaben $x \in \mathbb{F}_2^n$.
- Drehe $|\psi\rangle$ sukzessive in Richtung des gesuchten $|a\rangle \in \mathbb{F}_2^n$.
- Bestimme die Anzahl der notwendigen Drehungen.
- Falls Vektor hinreichend nahe an $|a\rangle$ ist, messe a mit hoher Ws.

Aufwand dazu wird nur $\mathcal{O}(\sqrt{N})$ betragen.

Die Drehung V

Definition der Drehung V:

- Starte mit Zustand $|0^n\rangle|1\rangle$. Sei $|\psi\rangle = H_n|0^n\rangle$.
- Anwendung von H_{n+1} auf $|0^n\rangle|1\rangle$ liefert die Superposition
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- Reversible Einbettung U_f führt zum Zustand
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- Effekt von U_f auf die ersten n Register entspricht der Abbildung
$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{für } x \neq a \\ -|x\rangle & \text{für } x = a. \end{cases}$$
- Sei $|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ ein beliebiger Quantenzustand.
- V flippt das Vorzeichen des zu $|a\rangle$ parallelen Anteils $\alpha_x|a\rangle$.
- Der Anteil orthogonal zu $|a\rangle$ bleibt unverändert.
- D.h. $V|z\rangle = |z\rangle - 2\alpha_x|a\rangle$ und $V|\psi\rangle = |\psi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle$.

Projektionen

Definition $a^{\perp}$

Wir betrachten die von $|a\rangle$, $|\psi\rangle$ aufgespannte 2-dimensionale Ebene.
Wir bezeichnen mit $|a^{\perp}\rangle$ den zu $|a\rangle$ orthogonalen Einheitsvektor.

Anmerkung:

- V spiegelt den Vektor $|\psi\rangle$ an $|a^{\perp}\rangle$.

Alternative Darstellung von V:

- Sei $|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.
- Anwendung von $\langle a|$ auf beiden Seiten liefert
$$\langle a|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \langle a|x\rangle = \alpha_x .$$
- D.h. die Projektion von $|z\rangle$ auf $|a\rangle$ ist
$$\alpha_x |a\rangle = \langle a|z\rangle |a\rangle = |a\rangle\langle a|z\rangle = |a\rangle\langle a||z\rangle .$$
- Wir können die Operation von V auf $|z\rangle$ schreiben als
$$V|z\rangle = |z\rangle - 2\cdot |a\rangle\langle a||z\rangle = \Big(I_n - 2|a\rangle\langle a|\Big)|z\rangle .$$

Die zweite Drehung W

Definition Projektionsoperator

Sei $|x\rangle \in \mathbb{C}^k$. Dann heißt $|x\rangle\langle x| \in \mathbb{C}^{k\times k}$ *Projektionsoperator* auf $|x\rangle$.

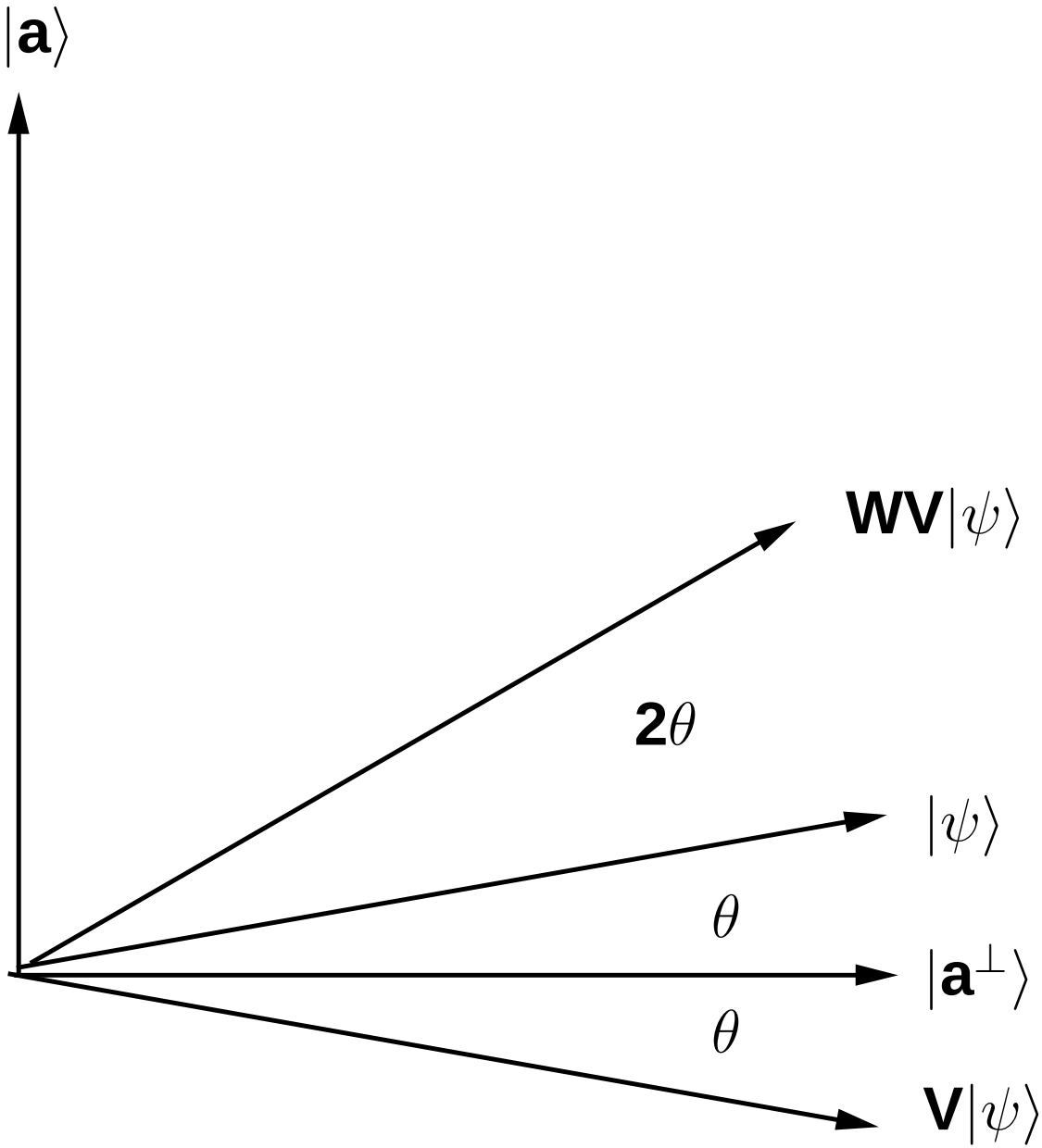
Definition der Drehung W:

- Sei $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ die Gleichverteilung.
- Wir definieren die zweite Drehung W wie folgt.
- Die Drehung W erhält den Anteil eines Vektors parallel zu $|\psi\rangle$.
- W flippt das Vorzeichen des Anteil orthogonal zu $|\psi\rangle$.
- Die Drehung W entspricht also einer Spiegelung an $|\psi\rangle$.
- Analog zu V definieren wir $W = (-I_n + 2|\psi\rangle\langle\psi\rangle)$.

Definition Grover-Iteration

Seien $V = (I_n - 2|a\rangle\langle a|)$ und $W = (-I_n + 2|\psi\rangle\langle\psi\rangle)$. Dann nennen wir die Abbildung WV eine *Grover-Iteration*.

Graphische Darstellung



Grover-Iteration ist Rotation in der Ebene

- Wir wenden WV sukzessive auf den Zustand $|\psi\rangle$ an.
- Die Definition von V und W hängt nur von $|a\rangle$ und $|\psi\rangle$ ab.
- Wir spiegeln abwechselnd an $|a^{\perp}\rangle$ und $|\psi\rangle$.
- Damit liefert die Grover-Iteration eine 2-dimensionale Rotation in der Ebene aufgespannt durch die Vektoren $|a\rangle$ und $|\psi\rangle$.
- D.h. wir können jeden durch Grover-Iteration erhaltenen Vektor als Linearkombination von $|a\rangle$ und $|\psi\rangle$ darstellen.
- Wegen $\langle a|\psi\rangle = \langle\psi|a\rangle = \frac{1}{\sqrt{2^n}}$ erhalten wir stets reelle Amplituden.

Grover-Iteration rotiert in Richtung $|a\rangle$

- Wir betrachten die erste Grover-Iteration auf $|\psi\rangle$.
- Wegen $\langle a|\psi\rangle = \frac{1}{\sqrt{2^n}}$ sind $|a\rangle$ und $|\psi\rangle$ nahezu orthogonal.
- Sei θ der von $|\psi\rangle$ und $|a^\perp\rangle$ eingeschlossene Winkel.
- V spiegelt $|\psi\rangle$ an $|a^\perp\rangle$.
- D.h. V dreht den Vektor $|\psi\rangle$ um den Winkel 2θ in Richtung $|a^\perp\rangle$.
- W spiegelt an $|\psi\rangle$, d.h. dreht um den Winkel 4θ in Richtung $|a\rangle$.
- D.h. eine Iteration dreht $|\psi\rangle$ insgesamt um 2θ in Richtung $|a\rangle$.
- Da WV eine Rotation ist, wird $|\psi\rangle$ in jeder Iteration um 2θ in Richtung $|a\rangle$ gedreht.

Anzahl der benötigten Grover-Iterationen

Lemma Benötigte Grover-Iterationen

Der Vektor $|\psi\rangle$ ist parallel zum gesuchten $|a\rangle$ nach ca. $\frac{\pi}{4}\sqrt{N}$ Grover-Iterationen.

Beweis:

- Zu Beginn gilt $\cos\gamma = \langle a|\psi\rangle = \frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}}$.
- D.h. der von $|\psi\rangle$ und $|a^\perp\rangle$ eingeschlossene Winkel $\theta = \frac{\pi}{2} - \gamma$ erfüllt
$$\sin\theta = \cos\gamma = \frac{1}{2^{\frac{n}{2}}}.$$
- Wegen $sin(x) \approx x$ für kleine x gilt $\theta \approx 2^{-\frac{n}{2}}$ für große n.
- Jede Grover-Iteration vergrößert den Winkel um 2θ.
- D.h. nach k Iterationen ist der Winkel $(2k+1)\theta$.
- Damit ist nach ca. $\frac{\pi}{4}2^{\frac{n}{2}}$ Grover-Iterationen $|\psi\rangle$ orthogonal zu $|a^\perp\rangle$.

Grover-Algorithmus

Algorithmus von Grover

EINGABE: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für genau ein $a \in \mathbb{F}_2^n$

1. Berechne $|z\rangle = H_{n+1}|0^n 1\rangle$.
2. Führe auf den ersten n Registern $\frac{\pi}{4} \cdot 2^{\frac{n}{2}}$-mal WV aus.
3. Messe die ersten n Register. Sei $|a\rangle$ das Ergebnis.
4. Falls $f(a) \neq 1$, gehe zurück zu Schritt 1.

AUSGABE: $a \in \mathbb{F}_2^n$

Verallgemeinerung von Grover

Definition Verallgemeinertes Problem der Datenbanksuche

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für $a_1, \ldots, a_m \in \mathbb{F}_2^n$
Gesucht: $a_i \in \mathbb{F}_2^n$ mit $i \in [m]$

Modifikation im Grover-Algorithmus:

- Analog gilt
$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{für } x \notin \{a_1, \ldots, a_m\} \\ -|x\rangle & \text{für } x \in \{a_1, \ldots, a_m\}. \end{cases}$$
- Wir definieren $|\bar{a}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |a_i\rangle$.
- V und W rotieren ψ in der 2-dimensionalen Ebene aufgespannt durch die beiden Vektoren $|\bar{a}\rangle$ und $|\psi\rangle$.
- Der Winkel zwischen $|\bar{a}^{\perp}\rangle$ und $|\psi\rangle$ beträgt nun
$$\sin\theta = \langle \bar{a}^{\perp}|\psi\rangle = \sqrt{\frac{m}{2^n}}.$$
- D.h. für $m \ll 2^n$ benötigt der Grover-Algorithmus etwa $\frac{\pi}{4} \cdot \frac{2^{\frac{n}{2}}}{\sqrt{m}}$ Iterationen.

Unbekanntes m

Frage: Können wir Grover auch anwenden, falls m unbekannt ist?

- Die Grover-Iteration ist eine periodische Funktion.
- Der ursprüngliche Zustand $|\psi\rangle$ wird nach ca. $\pi \frac{2^{\frac{n}{2}}}{\sqrt{m}}$ vielen Grover-Iterationen wieder angenommen.
- D.h. wir können die Quanten-Fouriertransformation verwenden, um m zu bestimmen.