Quantenalgorithmen
(ab Vorlesung 09)

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 2011/12

Problem von Simon (1994)

Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow y = x + s$
Gesucht: $s \in \mathbb{F}_2^n$

Anmerkungen:

- Je zwei Urbilder x und $x + s$ werden auf dasselbe Bild abgebildet.
- Damit ist f eine (2:1)-Abbildung.

Klassischer Algorithmus:

- Werte paarweise verschiedene $x_1, \ldots, x_k$ aus, bis eine Kollision $f(x_i) = f(x_j)$ gefunden wird.
- Nach Schubfachprinzip genügen $k \leq 2^{n-1} + 1$ Auswertung von f.
- Probabilistisch genügen $k = \Theta(2^{\frac{n}{2}})$ mit hoher Ws.
- Definiere eine Indikatorvariable mit $X_{i,j} = 1$ gdw $f(x_i) = f(x_j)$.
- Die erwartete Anzahl von Kollisionen ist damit
$$E(\mathit{Kollisionen}) = \sum_{1 \leq i < j \leq k} \mathrm{Ws}[X_{i,j} = 1] = \frac{k^2}{2^n - 1}.$$
- Das heißt, wir benötigen $k = \Theta(2^{\frac{n}{2}})$, um Kollisionen zu erhalten.

Ermittle Vektor orthogonal zu s.

Quantenschaltkreis Q_S:

- Sei U_f die reversible Einbettung der Funktion f.
- Anwendung von $H_n \otimes I_n$ und U_f auf $0^n 0^n$ liefert
$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle.$$
- Messung der letzten n Register liefert für ein festes $f(x_0)$
$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 + s\rangle) \otimes f(x_0).$$
- Anwendung von $H_n \otimes I_n$ führt zu
$$\begin{aligned} & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} ((-1)^{x_0 y} + (-1)^{(x_0+s)\cdot y}) |y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} (-1)^{x_0 y} (1 + (-1)^{sy}) |y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{2^{\frac{n-1}{2}}} \left(\sum_{y \in \{0,1\}^n, ys=0} (-1)^{x_0 y} |y\rangle \right) \otimes f(x_0). \end{aligned}$$
- Messung der ersten n Register liefert gleichverteiltes y mit $ys = 0$.

Quantenalgorithmus für Simons Problem

Algorithmus Simon

EINGABE: Quantenschaltkreis Q_S

1. Konstruiere leere $(n \times n)$-Matrix Y.
2. Wiederhole bis $\mathrm{rang}(Y) = n$:
   1. Konstruiere mittels Q_S gleichverteiltes $y \in \{0,1\}^n$ mit $ys = 0$.
   2. Falls y linear unabhängig zu Vektoren aus Y, füge y zu Y hinzu.
3. Löse das Gleichungssystem $Y \cdot s = \mathbf{0}$ über $\mathbb{F}_2$.

AUSGABE: $s \in \mathbb{F}_2^n$ mit $f(x) = f(x+s)$ für alle $x \in \mathbb{F}_2^n$

- Korrektheit: Für $\mathrm{rang}(Y) = n$ ist s eindeutig bestimmt.
- Laufzeit: $\mathcal{O}(n)$ Gatteranwendungen ($+\mathcal{O}(n^3)$ für lineare Algebra).
- Exponentieller Speedup gegenüber der klassischen Lösung.

Verallgemeinertes Problem von Simon

Verallgemeinertes Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow x \oplus y \in S$ für einen Untervektorraum $S \subset \mathbb{F}_2^n$.

Gesucht: Basis für S

- Verwenden gleichen Quantenschaltkreis wie bei Simon's Problem.
- D.h. wir führen $H_n \otimes I_n$, U_f und wieder $H_n \otimes I_n$ durch.
- Durchführung von Hadamard und U_f auf $|0^n\rangle|0^n\rangle$ führt zu
$$\frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.$$
- Messung der letzten n Register liefert ein $f(x_0)$, d.h.
$$\frac{1}{|S|^{\frac{1}{2}}} \sum_{s \in S} |x_0 + s\rangle \otimes |f(x_0\rangle.$$
- Anwendung von Hadamard liefert
$$\frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{s \in S} (-1)^{(x_0+s)y} |y\rangle$$
$$= \frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} (-1)^{x_0 y} \sum_{s \in S} (-1)^{sy} |y\rangle.$$

Messung für Simons Schaltkreis

- **Fall 1:** Sei $y \in S^{\perp}$, d.h. $sy = 0$. Für jedes y ist die Amplitude $\frac{\pm|S|}{(2^n|S|)^{\frac{1}{2}}}$, d.h. wir messen jedes y mit Ws $\frac{|S|}{2^n}$.
- Wegen $\dim(S) + \dim(S^{\perp}) = n$, gilt $|S| \cdot |S^{\perp}| = 2^n$.
- Damit wird jedes $y \in S^{\perp}$ mit Ws $\frac{1}{|S^{\perp}|}$ gemessen.
- D.h. die Ws für alle $y \notin S^{\perp}$ müssen 0 sein. Wir rechnen kurz nach.
- **Fall 2:** Sei $y \notin S^{\perp}$. Damit existiert ein $s' \in S$ mit $s'y = 1$. Es gilt

$$\begin{aligned} \sum_{s \in S}(-1)^{sy} &= -(-1)^{s'y}\sum_{s \in S}(-1)^{sy} = -\sum_{s \in S}(-1)^{(s+s')y} \\ &= -\sum_{s \in S}(-1)^{sy}. \end{aligned}$$

- Damit verschwindet die Summe und alle Amplituden für $y \notin S^{\perp}$.

Bestimmung von S

- Messung liefert gleichverteilte $y_i \in S^{\perp}$.
- Da $\dim(S^{\perp})$ unbekannt ist, berechnen wir solange y_i bis die Anzahl der linear unabhängigen y_i stabil bleibt.
- Dazu genügen $\dim(S^{\perp}) + 4$ Werte mit hoher Ws.
- Wir berechnen aus den y_i eine Basis $B^{\perp}$ von $S^{\perp}$.
- Wir lösen das lineare Gleichungssystem $B^{\perp} s^T = \mathbf{0}$.
- Sei $B = \{s_1, \ldots, s_m\}$ eine Generatorenmenge des Lösungsraums.
- B ist die gesuchte Basis von S.

Speedup und Interpretation von Simons Problem

Speedup gegenüber klassischen Algorithmen:

- Jeder klassische Algorithmus für Simons Problem muss Kollisionen $f(x) = f(y)$ finden.
- Für zufällige x, y ist die Wahrscheinlichkeit einer Kollision $2^{\dim(S)-n}$.
- Geburtstagsparadoxon: Erwarten Kollision nach $2^{\frac{n-\dim(S)}{2}}$ Schritten.
- Quantenalgorithmus liefert Basis für ca. $\dim(S^{\perp}) = n - \dim(S)$ Auswertungen.
- Damit erhalten wir einen exponentiellen Speedup (Orakel-Modell).

Interpretation

- Simons Algorithmus findet versteckte Untergruppe S in $(\mathbb{F}_2^n, +)$.
- Interpretation als Algorithmus zum Finden einer Periode.
- $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ist periodisch: $f(x) = f(x \oplus s)$ mit Periode $s \in S$.
- Frage: Können wir $(\mathbb{F}_2, +)$ durch $(\mathbb{Z}, +)$ ersetzen?
  - $(r\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$ für $r \in \mathbb{N}$.
  - D.h. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = f(x + r\mathbb{Z})$ mit gesuchter Periode r.

RSA Verschlüsselung und Perioden

RSA Verschlüsselung

Sei $N = pq$ mit p, q prim und $\phi(N) = (p-1)(q-1)$. Ferner sei $e \in \mathbb{Z}^*_{\phi(N)}$. Die *RSA Funktion* ist die Abbildung $f_{RSA} : \mathbb{Z}_N \to \mathbb{Z}_N$ mit

$$m \mapsto m^e \bmod N.$$

Anmerkung:

- Sei $m \in \mathbb{Z}^*_N$. Wir definieren $\mathrm{ord}(m) = \min\{i \in \mathbb{N} \mid m^i = 1 \bmod N\}$.
- Betrachten die Exponentiations-Funktion $f : \mathbb{Z} \to \mathbb{Z}_N$ mit
$$i \mapsto m^i \bmod N.$$
- f ist für jedes $m \in \mathbb{Z}^*_N$ periodisch, denn
$$f(i) = f(i + \mathrm{ord}(m)k) \text{ für } k \in \mathbb{Z}.$$
- D.h. $\mathrm{ord}(m)$ ist die Periode für die Exponentiations-Funktion.
- Unser Ziel ist die effiziente Ermittlung dieser Periode $\mathrm{ord}(m)$.
- *Kleines Problem:* Angreifer kennt nur m^e und nicht m.

Ordnung von Plain- und Chiffretexten

Lemma

Seien N, e RSA Parameter und $m \in \mathbb{Z}_N^*$. Dann gilt $\mathrm{ord}(m) = \mathrm{ord}(m^e)$.

Beweis:

- Sei $\langle m \rangle = \{m, m^2, \ldots, m^{\mathrm{ord}(m)}\}$ die von m erzeugte Untergruppe.
- Es gilt $\mathrm{ord}(m) = |\langle m \rangle|$. Zeigen zunächst $\langle m^e \rangle \subseteq \langle m \rangle$.
- Sei $m^{ei} \in \langle m^e \rangle$. Dann gilt offenbar $m^{ei} \in \langle m \rangle$.
- Andererseits zeigen wir $\langle m \rangle \subseteq \langle m^e \rangle$.
- Nach Satz von Euler gilt $m^{|\mathbb{Z}_N^*|} = m^{\phi(N)} = 1$.
- Die Elementordnung teilt die Gruppenordnung, d.h. $\mathrm{ord}(m) \mid \phi(N)$.
- Wegen $\mathrm{ggT}(e, \phi(N)) = 1$ gilt damit ebenfalls $\mathrm{ggT}(e, \mathrm{ord}(m)) = 1$.
- Damit existieren $d, k \in \mathbb{Z}$ mit $ed + \mathrm{ord}(m)k = 1$.
- D.h. $m = m^{ed+\mathrm{ord}(m)k} = m^{ed} \cdot (m^{ord(m)})^k = (m^e)^d \bmod N$.
- Daraus folgt $m \in \langle m^e \rangle$ und damit auch $m^i \in \langle m^e \rangle$ für alle $i \in \mathbb{N}$.
- Insgesamt: $\langle m \rangle = \langle m^e \rangle$, d.h. $\mathrm{ord}(m) = |\langle m \rangle| = |\langle m^e \rangle| = \mathrm{ord}(m^e)$.

Brechen von RSA mit Hilfe der Ordnung von m

Satz

Seien N, e RSA-Parameter und $m^e \in \mathbb{Z}_N^*$. Mit Hilfe von $\mathrm{ord}(m^e)$ kann m in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

- Beweis zuvor liefert $\mathrm{ord}(m) = \mathrm{ord}(m^e)$ und $\mathrm{ggT}(e, \mathrm{ord}(m)) = 1$.
- Der Erweiterte Euklidische Algorithmus liefert bei Eingabe $e, \mathrm{ord}(m) \in \mathbb{Z}_N$ in Zeit $\mathcal{O}(\log^2 N)$ Zahlen d, k mit $ed + \mathrm{ord}(m)k = 1$.
- Wir berechnen $(m^e)^d = m^{1-ord(m)k} = m \cdot (m^{\mathrm{ord}(m)})^{-k} = m \bmod N$ in Zeit $\mathcal{O}(\log^3 N)$.

Motivation Phasenbestimmung

Problem Spezialfall der Phasenbestimmung

Gegeben: Zustand $|\mathbf{z}\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{y}} |\mathbf{y}\rangle$

Gesucht: $\mathbf{x} \in \mathbb{F}_2^n$

- Für $n = 1$ ist der Zustand $|\mathbf{z}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\mathbf{x}}|1\rangle) = H|\mathbf{x}\rangle$.
- Es gilt $H|\mathbf{z}\rangle = |\mathbf{x}\rangle$, d.h. H dekodiert die Phaseninformation $\mathbf{x}$.
- Für allgemeines n gilt $|\mathbf{z}\rangle = H_n|\mathbf{x}\rangle$ und damit $H_n|\mathbf{z}\rangle = |\mathbf{x}\rangle$.
- D.h. H_n dekodiert Phasen der speziellen Form $(-1)^{\mathbf{x}\cdot\mathbf{y}} = (e^{\pi i})^{\mathbf{x}\cdot\mathbf{y}}$.
- Gibt es ein Analog für Phasen der Form $e^{2\pi i\omega}$ für ein $\omega \in [0, 1)$?

Problem der Phasenbestimmung

Problem Phasenbestimmung

Gegeben: Zustand $|z\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$ für $\omega \in [0,1)$

Gesucht: ω (bzw. eine gute Approximation von ω)

Notation:

- Wir bezeichnen mit $\mathbf{y} \in \mathbb{F}_2^n$ einen n-dimensionalen Vektor.
- Mit $y \in \mathbb{Z}_{2^n}$ bezeichnen wir eine Zahl zwischen 0 und $2^n - 1$.
- Z.B. schreiben wir für $n = 4$ den Zustand $|y\rangle = |3\rangle = |0011\rangle = |\mathbf{y}\rangle$.
- Für $\omega = \sum_k x_k 2^{-k}$ schreiben wir $\omega = 0.x_1 x_2 x_3 \ldots$
- Für $n = 1$ und $\omega = 0.x_1$ folgt

$$|z\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i (0.x_1) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i x_1 y} |y\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x_1 y} |y\rangle = H|x_1\rangle$$

- D.h. $H|z\rangle = |x_1\rangle$ liefert x_1 und damit ω.

Produktformel von Griffith-Nui (1996)

Satz Produktformel von Griffith-Nui

Für $\omega = 0.x_1x_2\ldots x_n$ gilt

$$|z\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle = \frac{|0\rangle+e^{2\pi i 0.x_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle+e^{2\pi i 0.x_1x_2\ldots x_n}|1\rangle}{\sqrt{2}}.$$

Beweis:

$$\begin{aligned}
|z\rangle &= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} e^{2\pi i\omega \sum_{\ell=0}^{n-1} y_\ell 2^\ell}|y_{n-1}\ldots y_0\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} \bigotimes_{\ell=1}^{n} e^{2\pi i\omega y_{n-\ell}2^{n-\ell}}|y_{n-\ell}\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=1}^{n} \left(\sum_{y_\ell=0}^{1} e^{2\pi i\omega y_{n-\ell}2^{n-\ell}}|y_{n-\ell}\rangle\right) = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2\pi i\omega 2^{n-\ell}}|1\rangle\right) \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\left(|0\rangle + e^{2\pi i x_1x_2\ldots x_{n-1}.x_n}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{2\pi i 0.x_1x_2\ldots x_n}|1\rangle\right)\right)
\end{aligned}$$

Bestimmen von zwei Nachkommastellen

Problem Phasenbestimmung mit $n = 2$ Bits

Gegeben: Zustand $|z\rangle = \frac{1}{2}\sum_{y=0}^{2^2-1} e^{2\pi i \omega y}|y\rangle$ für $\omega = 0.x_1x_2$

Gesucht: $\omega = 0.x_1x_2$

- Schreibe $|z\rangle = \left(\frac{|0\rangle + e^{2\pi i 0.x_2}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_1x_2}|1\rangle}{\sqrt{2}}\right)$.
- Bestimme x_2 durch Anwendung von Hadamard auf das 1. Qubit.
- Falls $x_2 = 0$, bestimme x_1 durch Hadamard auf das 2. Qubit.
- Falls $x_2 = 1$, dann eliminieren wir zunächst x_2 durch eine Rotation.
- Wir betrachten die Rotation $R_2 = F_{2\pi(0.01)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix}$.
- D.h. $R_2^{-1}\left(\frac{|0\rangle + e^{2\pi i 0.x_1 1}|1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + e^{2\pi i (0.x_1 1 - 0.01)}|1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + e^{2\pi i 0.x_1}|1\rangle}{\sqrt{2}}\right)$.
- Verwenden ein vom 1.Qubit kontrolliertes R_2^{-1}-Gatter auf Qubit 2.
- Anschließend bestimmen wir x_1 mittels eines Hadamard-Gatters.

Bestimmen von 3 Nachkommastellen

Problem Phasenbestimmung mit $n = 3$ Bits

Gegeben: Zustand $|z\rangle = \frac{1}{2^{\frac{3}{2}}} \sum_{y=0}^{2^3-1} e^{2\pi i \omega y} |y\rangle$ für $\omega = 0.x_1x_2x_3$

Gesucht: $\omega = 0.x_1x_2x_3$

- $|z\rangle = \left(\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_2x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_1x_2x_3}|1\rangle}{\sqrt{2}}\right)$
- Bestimme x_3 und x_2 wie zuvor.
- Definiere Rotation R_k zum Entfernen der k-ten Nachkommastelle

$$R_k = F_{2\pi 2^{-k}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}.$$

- Entferne x_3 in Qubit 3 durch R_3^{-1} kontrolliert durch Qubit 1.
- Entferne x_2 in Qubit 2 durch R_2^{-1} kontrolliert durch Qubit 2.
- Bestimme anschließend x_1 durch ein Hadamard-Gatter.

Die Quanten Fourier Transformation

- Verallgemeinerung auf beliebiges n führt zu einem Schaltkreis C_n mit $\mathcal{O}(n^2)$ Gatter.
- D.h. wir realisieren für $\omega = 0.x_1 \dots x_n = \frac{x}{2^n}$ die Abbildung

$$\frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle \mapsto |x\rangle.$$

Definition Quanten Fourier Transformation (QFT)

Wir bezeichnen die Abbildung

$$\mathrm{QFT}_{2^n} : |x\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle$$

als *Quanten Fourier Transformation* (QFT).

Schaltkreis für QFT_{2^n}

Satz Schaltkreis für QFT_{2^n}

Es gibt einen Quantenschaltkreis für QFT_{2^n} mit $\mathcal{O}(n^2)$ Gattern.

Beweis:

- Verwenden Schaltkreis C_n zur Phasenbestimmung.
- Der Schaltkreis C_n implementiert $\mathrm{QFT}_{2^n}^{-1}$.
- D.h. wir können C_n in umgekehrter Reihenfolge anwenden.

Vergleich zur Diskreten Fourier Transformation (DFT)

Definition Diskrete Fourier Transformation

Sei $\alpha(x) = \sum_{\ell=0}^{2^n-1} a_i x^i \in \mathbb{C}[x]$. Sei $\beta_y = \alpha(e^{2\pi i \frac{y}{2^n}})$ für $y \in \mathbb{Z}_{2^n}$. Dann bezeichnen wir $\beta = (\beta_0, \ldots, \beta_{2^n-1})$ als *Diskrete Fourier Transformierte (DFT)* von $\alpha(x)$.

Zusammenhang mit QFT:

- DFT liefert $\beta_y = \sum_{\ell=0}^{2^n-1} \alpha_\ell e^{2\pi i \frac{y}{2^n}\ell}$.
- Betrachten allgemeinen Quantenzustand $|z\rangle = \sum_{\ell=0}^{2^n-1} \alpha_\ell |\ell\rangle$.

$$\begin{aligned} \mathrm{QFT}_{2^n}(|z\rangle) &= \sum_{\ell=0}^{2^n-1} \alpha_\ell \mathrm{QFT}_{2^n}(|\ell\rangle) = \sum_{\ell=0}^{2^n-1} \alpha_\ell \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{\ell}{2^n} y} |y\rangle \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \sum_{\ell=0}^{2^n-1} \alpha_\ell e^{2\pi i \frac{y}{2^n}\ell} |y\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \beta_y |y\rangle \end{aligned}$$

- D.h. die Amplituden β_y sind die DFTs der Amplituden α_ℓ.

Vergleich zum klassischen Ansatz

Speedup:

- Berechnung der DFT entspricht Auswerten eines Polynoms vom Grad kleiner als 2^n an 2^n verschiedenen Stellen.
- Komplexität mit Horner-Schema: $2^n \cdot \mathcal{O}(2^n) = \mathcal{O}(2^{2n})$.
- Schnelle Fourier Transformation (DiMaI): $\mathcal{O}(n2^n)$.
- Berechnung der QFT benötigt dagegen nur $\mathcal{O}(n^2)$ Gatter.
- D.h. wir erhalten einen exponentiellen Speedup.
- **Aber:** QFT liefert die Amplituden nicht explizit. Aus $\mathrm{QFT}_{2^n}(|z\rangle)$ kann daher die DFT nicht einfach bestimmt werden.

Approximieren von ω

Szenario:

- Bisher war ω stets von der Form $\omega = \frac{x}{2^n}$.
- **Frage:** Was geschieht für allgemeines ω?

Fakt Approximation von ω

Sei $|z\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$ für $\omega \in [0,1)$. Dann liefert $\mathrm{QFT}^{-1}(|z\rangle)$ mit Wahrscheinlichkeit mindestens $\frac{4}{\pi^2}$ ein x mit $|\frac{x}{2^n} - \omega| \leq \frac{1}{2^{n+1}}$.

- D.h. wir erhalten mit Ws $\frac{4}{\pi^2}$ dasjenige ganzzahlige Vielfache von $\frac{1}{2^n}$, das am nächsten zu ω ist.

Definition Periodischer Zustand

Sei $|z_{r,b}\rangle$ ein Quantenzustand der Form $|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr + b\rangle$ mit $b \in \mathbb{Z}_r$. Dann heißt $|z_{r,b}\rangle$ *periodischer Zustand* mit *Periode* r, *Vielfachheit der Periode* m und *Shift* b.

Finden der Periode mit Vielfachheit

Problem Finden der Periode mit Vielfachheit

Gegeben: mr, periodischer Zustand $|z_{r,b}\rangle$ mit $b \in_R \mathbb{Z}_r$
Gesucht: r

Lösung:

- Messen von $|z_{r,b}\rangle$ liefert jeden Zustand $|x\rangle$, $x \in \mathbb{Z}_{mr}$ mit Ws $\frac{1}{mr}$.
- D.h. Messung von $|z_{r,b}\rangle$ liefert keine Information über r.
- Berechnen stattdessen $\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \frac{b}{r}\ell}|m\ell\rangle$. (Lemma auf nächster Folie)
- Messung liefert nur Basiszustände $|m\ell\rangle$, die Vielfache von m sind.
- Wir berechnen $\frac{m\ell}{mr} = \frac{\ell}{r}$. Falls $\gcd(\ell, r) = 1$ liefert dies r.
- Es gilt $\gcd(\ell, r) = 1$ mit Wahrscheinlichkeit $\Omega(\frac{1}{\log\log r})$.

QFT entfernt den Shift

Lemma Entfernen des Shifts durch QFT

$$\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1} e^{2\pi i \frac{b}{r}\ell}|m\ell\rangle$$

Beweis:

- Es gilt $\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\mathrm{QFT}_{mr}|kr+b\rangle$. Umformung liefert
$$\frac{1}{\sqrt{m^2 r}}\sum_{y=0}^{mr-1}\sum_{k=0}^{m-1} e^{2\pi i \frac{kr+b}{mr}y}|y\rangle$$
- Wir ziehen den vom Shift b abhängigen Term aus der 1. Summe
$$\frac{1}{\sqrt{m^2 r}}\sum_{y=0}^{mr-1} e^{2\pi i \frac{by}{mr}}\sum_{k=0}^{m-1} e^{2\pi i \frac{ky}{m}}|y\rangle.$$
- Für $y = m\ell$, $\ell \in \mathbb{Z}_r$ erhalten wir $e^{2\pi i \frac{by}{mr}} = e^{2\pi i \frac{b}{r}\ell}$ und $\sum_{\ell=0}^{m-1} e^{2\pi i \frac{ky}{m}} = m$. Dies liefert sofort die geforderte obige Formel.
- Übungsaufgabe: Rechnen Sie nach, dass für $m \not| y$ gilt
$$\sum_{k=0}^{m-1}\left(e^{2\pi i \frac{y}{m}}\right)^k = 0.$$
- D.h. die restlichen Amplituden heben sich gegenseitig auf.

Finden der Ordnung von 2 in $\mathbb{Z}_{15}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{15}^*$

Gegeben: $mr = |\mathbb{Z}_{15}^*| = 8$
Gesucht: $r = \mathrm{ord}_{\mathbb{Z}_{15}^*}(2)$

- Sei $f(x) = 2^x \bmod 15$ mit reversibler Einbettung U_f.
- Auf $|0^3\rangle|0^3\rangle$ wird $H_3 \otimes I_3$ und U_f angewendet. Dies liefert
$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle|2^x \bmod 15\rangle = \frac{1}{\sqrt{8}} \Big(|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle + |4\rangle|1\rangle + |5\rangle|2\rangle + |6\rangle|4\rangle + |7\rangle|8\rangle \Big).$$
- Angenommen wir messen $|2\rangle$ im rechten Teil.
- Dann steht in den ersten 3 Qubits der periodische Zustand
$$|z_{4,1}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |5\rangle).$$
- $\mathrm{QFT}_8(|z_{4,1}\rangle) = \frac{1}{2} \sum_{\ell=0}^{3} e^{2\pi i \frac{1}{4}\ell} |2\ell\rangle = \frac{1}{2}(|0\rangle + i|2\rangle - |4\rangle - i|6\rangle)$.
- Bei Messung von $m\ell = 6$ erhalten wir $\frac{m\ell}{mr} = \frac{6}{|\mathbb{Z}_{15}^*|} = \frac{3}{4}$.
- Der Nenner impliziert $4 \mid \mathrm{ord}(2)$.
- Wir prüfen $2^4 = 1 \bmod 15$, d.h. $\mathrm{ord}(2) = 4$.

Finden der Periode ohne Vielfachheit

Problem Finden der Periode

Gegeben: n, periodischer Zustand $|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k:0\leq kr+b<2^n} |kr+b\rangle$ mit geeignetem m, $r \leq m \leq \frac{2^n}{r}$, so dass $\||z_{r,b}\rangle\| = 1$.

Gesucht: r

Idee der Lösung:

- Es gilt $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle) = \frac{1}{\sqrt{m2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{by}{2^n}} \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y} |y\rangle$.
- Amplitude $\sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y}$ wird groß, falls y nahe einem Vielfachem von $\frac{2^n}{r}$ ist. Wir zeigen $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$ für ein $\ell \in \mathbb{Z}_r$ mit hoher Ws.
- Wegen $2^n \geq r^2$ folgt damit $\left| \frac{y}{2^n} - \frac{\ell}{r} \right| \leq \frac{1}{2^{2n}} \leq \frac{1}{2r^2}$.
- Damit kommt $\frac{\ell}{r}$ in der Kettenbruchentwicklung von $\frac{y}{2^n}$ vor.
- Zeigen alternativ, dass man $\frac{r}{\gcd(\ell,r)}$ mittels Gittern finden kann.
- 2 Durchgänge des Algorithmus liefern $r_1 = \frac{r}{\gcd(\ell_1,r)}$, $r_2 = \frac{r}{\gcd(\ell_2,r)}$.
- Mit Ws $\geq \frac{6}{\pi^2}$ gilt $r = \mathrm{kgV}(r_1, r_2)$.

Messung von y

Lemma Gemessenes y approxiert Vielfaches von $\frac{2^n}{r}$

Mit Ws mindestens $\frac{4}{\pi^2} \geq 0.4$ erhalten wir ein y mit $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$.

Beweisskizze:

- Sei $y_\ell = \frac{2^n}{r}\ell + \delta_\ell$ für $|\delta_\ell| \leq \frac{1}{2}$ und $p(y_\ell) = \frac{1}{m2^n} \left| \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y_\ell} \right|^2$.
- Für die Berechnung von $p(y_\ell)$ trägt nur der Term δ_ℓ bei.
- Übung: $m2^n \cdot p(y_\ell) = \left| \frac{e^{2\pi i \frac{r}{2^n} m\delta_\ell} - 1}{e^{2\pi i \frac{r}{2^n} \delta_\ell} - 1} \right|^2 = \frac{\sin^2(\pi \frac{r}{2^n} m\delta_\ell)}{\sin^2(\pi \frac{r}{2^n} \delta_\ell)}$.
- Wegen $m \approx \frac{2^n}{r}$ und $sin(x) \approx x$ für kleine x erhalten wir

$$p(y_\ell) \approx \frac{1}{m2^n} \left(\frac{\sin(\pi\delta_\ell)}{\pi \frac{r}{2^n} \delta_\ell} \right)^2 \approx \frac{1}{r} \left(\frac{\sin(\pi\delta_\ell)}{\pi\delta_\ell} \right)^2 .$$

- Es gilt $\sin(x) \geq \frac{2}{\pi}x$ für $x \in [0, \frac{\pi}{2}]$, d.h. $p(y_\ell) \geq \frac{1}{r} \left(\frac{\frac{2}{\pi}\pi\delta_\ell}{\pi\delta_\ell} \right)^2 = \frac{1}{r}\frac{4}{\pi^2}$.
- Ws gilt für alle $p(y_\ell)$ mit $\ell \in \mathbb{Z}_r$, d.h. wir messen ein y mit Ws $\geq \frac{4}{\pi^2}$.

Berechnen von $r/\gcd(\ell, r)$

Lemma Berechnen von ℓ und r

Sei $y \in \mathbb{Z}$ mit $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$ und $\ell \in \mathbb{Z}_r$, $r^2 \leq 2^n$. Dann kann $\frac{r}{\gcd(\ell,r)}$ in Zeit $\mathcal{O}(n^2)$ berechnet werden.

Beweisskizze:

- Es gilt $yr - 2^n\ell = x$ für ein $x \in \mathbb{Z}$ mit $|x| \leq \frac{r}{2}$.
- Seien r', ℓ', x' die durch $\gcd(\ell, r)$ gekürzten Unbekannten r, ℓ, x.
- Definieren $f(r', x') = yr' - x'$ mit $f(r', x') = 0 \bmod 2^n$.
- f ist modulares lineares Polynom mit Nullstelle (r', x'), so dass
$$|r' \cdot x'| \leq r' \cdot \frac{r}{2} \leq 2^{n-1}.$$
- Vorlesung Kryptanalyse: r', x' werden in Zeit $\mathcal{O}(n^2)$ gefunden, sofern $|r' \cdot x'|$ kleiner als der Modul 2^n ist.
- Sei $B = \begin{pmatrix} 1 & y \\ 0 & 2^n \end{pmatrix}$. Dann gilt $(r', -\ell') \cdot B = (r', x')$ und (r', x') ist eine kürzeste ganzzahlige Linearkombination von Vektoren aus B.
- D.h. ein kürzester Vektor liefert $r' = \frac{r}{\gcd(\ell,r)}$.

Gaußalgorithmus

Definition Gitter

Sei $B \in \mathbb{Z}^{2\times 2}$. Wir bezeichnen mit $L(B) = \{\mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{a}B = \mathbf{x}, \mathbf{a} \in \mathbb{Z}^2\}$ das von den Vektoren von B aufgespannte *Gitter*. Wir verwenden für die Länge von Gittervektoren $\mathbf{x} = (x_1, x_2)$ die ℓ_2-Norm $\|\mathbf{x}\| = \sqrt{x_1 + x_2}$.

Algorithmus Gaußalgorithmus

EINGABE: Basis $B = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ mit $\|\mathbf{b}_1\| \geq \|\mathbf{b}_2\|$

1. Bestimme $k \in \mathbb{Z}$, das $\|\mathbf{b}_1 - k \cdot \mathbf{b}_2\|$ minimiert.
2. Setze $\mathbf{b}_1 := \mathbf{b}_1 - k \cdot \mathbf{b}_2$. Falls $k \neq 0$, gehe zu Schritt 1.

AUSGABE: Basis $\mathbf{b}_1, \mathbf{b}_2$ minimaler Länge

Gaußalgorithmus liefert kürzeste Vektoren

Fakt Gaußalgorithmus

Der Gaußalgorithmus liefert bei Eingabe einer Basis B mit maximalem Basiseintrag b_m in Zeit $\mathcal{O}(\log^2 b_m)$ eine reduzierte Basis mit kürzestem Gittervektor in $L(B)$.

Shor's Algorithmus (1994)

Algorithmus Shor's Algorithmus zum Finden der Ordnung

EINGABE: a, N

1. Benötigen $2^n \geq N^2 \geq \phi^2(N)$, d.h. wähle $n = \lceil 2 \log N \rceil$.
2. Sei U_f die reversible Einbettung von $f(x) = a^x \bmod N$.
3. Wende auf $|0^n\rangle|0^n\rangle$ zunächst $H_n \otimes I_n$ dann U_f an. Liefert
$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|a^x \bmod N\rangle = \sum_{b=0}^{r-1} \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{m-1} |kr+b\rangle \right) |a^b \bmod N\rangle.$$
4. Messen der hinteren n Register liefert in den ersten n Registern
$$|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr+b\rangle.$$
5. Berechne $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle)$ und messe ein y_1.
6. Wiederhole Schritte 1-5 für ein y_2.
7. Berechne $r_1 = \frac{r}{\gcd(\ell_1, r)}$, $r_2 = \frac{r}{\gcd(\ell_2, r)}$ aus y_1, y_2 mit Gauß-Alg.
8. Berechne $r = \mathrm{kgV}(r_1, r_2)$. Falls $a^r \neq 1 \bmod N$, Ausgabe "Fehler".

AUSGABE: $r = \mathrm{ord}_{\mathbb{Z}_N *}(a)$

Finden der Ordnung von 2 in $\mathbb{Z}_{21}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{21}^*$

- Wähle der Einfachheit halber nur $n = 6$. Wir erhalten
$$\frac{1}{8}\sum_{x=0}^{63}|x\rangle|2^x \bmod 21\rangle = \frac{1}{8}\Big(|0\rangle|1\rangle + |1\rangle|2\rangle + \quad \ldots \quad + |5\rangle|11\rangle$$
$$\vdots$$
$$+|60\rangle|1\rangle + |61\rangle|2\rangle + |62\rangle|4\rangle + |63\rangle|8\rangle\Big).$$
- Messung von $|4\rangle$ im rechten Teil liefert im linken Teil
$$|z_{6,2}\rangle = \frac{1}{\sqrt{11}}\sum_{i=0}^{10}|6k+2\rangle.$$
- $\mathrm{QFT}_{2^6}(|z_{6,2}\rangle)$ und Messung liefert ein $y = 11\ell$ mit Ws $\geq \frac{4}{\pi^2}$.
- Bei Messung von $y = 11 \cdot 1$ erhalten wir die Gitterbasis
$$B = \begin{pmatrix} 1 & 11 \\ 0 & 64 \end{pmatrix}.$$
- Gaußalgorithmus liefert kürzesten Vektor
$$(6,2) = (6,-1)\cdot B = (r,x) \text{ in } L(B).$$
- Wir prüfen $2^r = 2^6 = 1 \bmod 21$.

Komplexität und Vergleich mit klassischen Algorithmen

Satz Komplexität von Shor's Algorithmus

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

Beweis:

- Anwendung von H_n benötigt $n = \mathcal{O}(\log N)$ Hadamard-Gatter.
- Anwednung von U_f 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

$$\mathrm{ggT}(a^{2^i t} \pm 1, N).$$

Finden einer Periode und Diskrete Logarithmen

Definition Diskretes Logarithmus Problem (DLP)

Gegeben: Abelsche Gruppe G, $a \in G$ und $b \in \langle a \rangle$
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
$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{für } x \neq a \\ -|x\rangle & \text{für } x = a. \end{cases}$$

Anmerkung:

- Sei $|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_a|x\rangle$ ein beliebiger Quantenzustand.
- V flippt das Vorzeichen des zu $|a\rangle$ parallelen Anteils $\alpha_a|a\rangle$.
- Der Anteil orthogonal zu $|a\rangle$ bleibt unverändert.
- D.h. $V|z\rangle = |z\rangle - 2\alpha_a|a\rangle$ 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
$$\langle a|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \langle a|x\rangle = \alpha_a.$$
- D.h. die Projektion von $|z\rangle$ auf $|a\rangle$ ist
$$\alpha_a|a\rangle = \langle a|z\rangle|a\rangle = |a\rangle\langle a|z\rangle = |a\rangle\langle a||z\rangle.$$
- 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 $|x\rangle$.

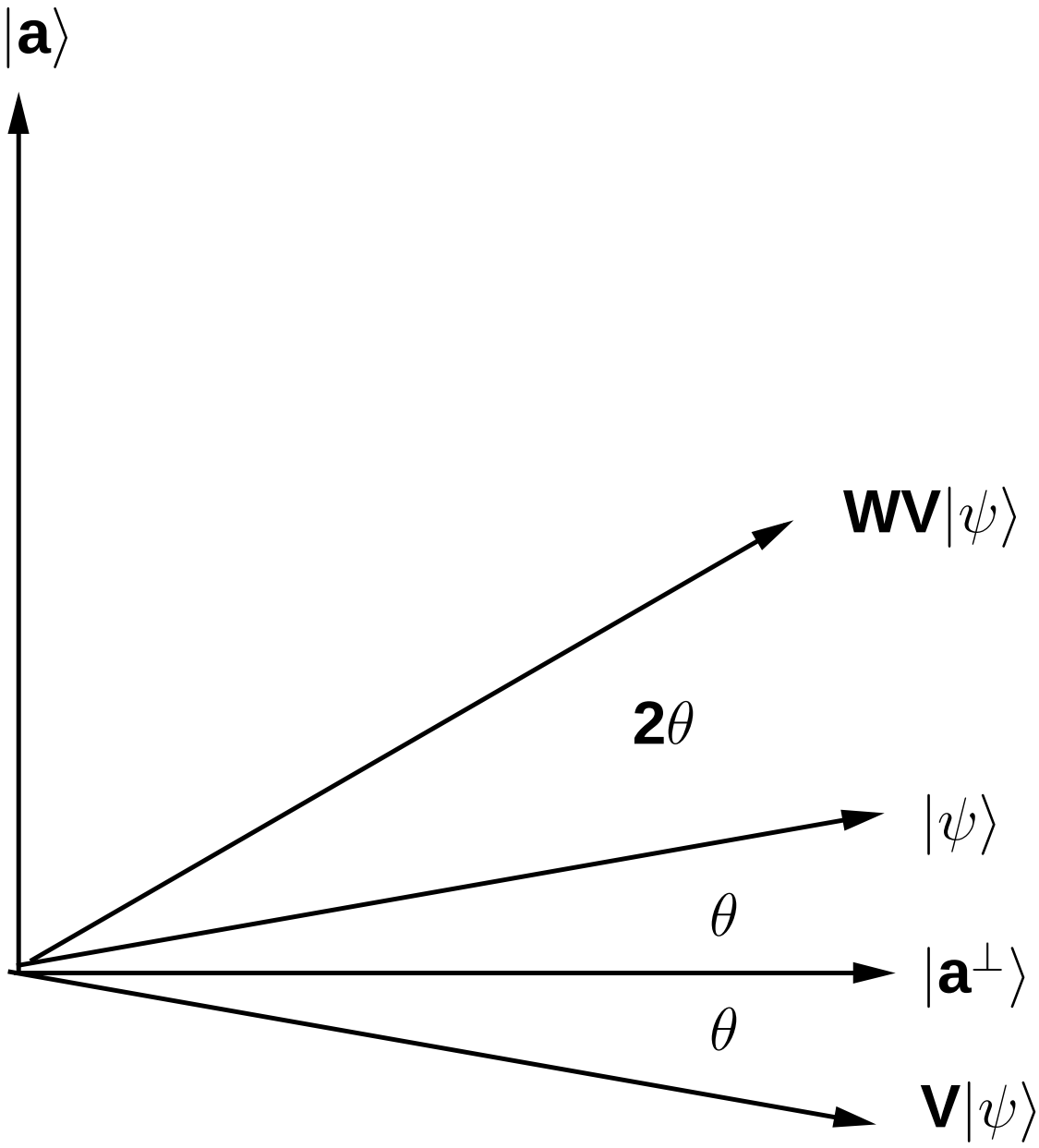
Definition der Drehung W:

- 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

$$\sin\theta = \langle \bar{a}^{\perp} | \psi \rangle = m \cdot \frac{1}{\sqrt{m 2^n}} = \sqrt{\frac{m}{2^n}}.$$

- 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.

Fehlerkorrektur

Notwendigkeit und Probleme der Quanten-Fehlerkorrektur

- Qbits müssen komplett isoliert von der Rechnerumgebung sein.
- Unmöglich, d.h. die Umgebung degeneriert Quantenzustände.
- Beobachtung von Fehlern durch Messung zerstört Zustand.
- Amplituden sind nicht diskret.
- Bitflips sind nicht die einzigen möglichen Fehler.
- Z.B. können einfache Phasenflips $|0\rangle + |1\rangle \mapsto |0\rangle - |1\rangle$ auftreten.
- Diese Fehler sind durch Messung nicht zu erkennen.

Klassisch:

- Auftretende Fehler sind ausschließlich Bitflips.
- Einfachste Lösung ist ein Repetitionscode der Länge 3.
- Wir codieren $0 \mapsto 000$ und $1 \mapsto 111$.
- Code erkennt zwei Fehler und korrigiert einen Fehler.

Repetition für Quanten

3-Qubit Repetition

Gegeben: Zustand $|z\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
Gesucht: Zustand $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$

Lösung:

- Verwende zwei Hilfsbits in Zustand $|0\rangle$, d.h. $|z00\rangle$.
- Kopiere die Basiszustände mittels CNOT.
- Sei C_{ij} ein CNOT auf Qubit j mit Kontrollbit i. Es gilt

$$|r\rangle = C_{12}C_{13}(\alpha_0|000\rangle + \alpha_1|100\rangle) = \alpha_0|000\rangle + \alpha_1|111\rangle.$$

Fehlermodell:

- Wir nehmen vereinfachend an, dass nur Bitflips auftreten.
- D.h. unsere fehlerbehafteten Zustände sind

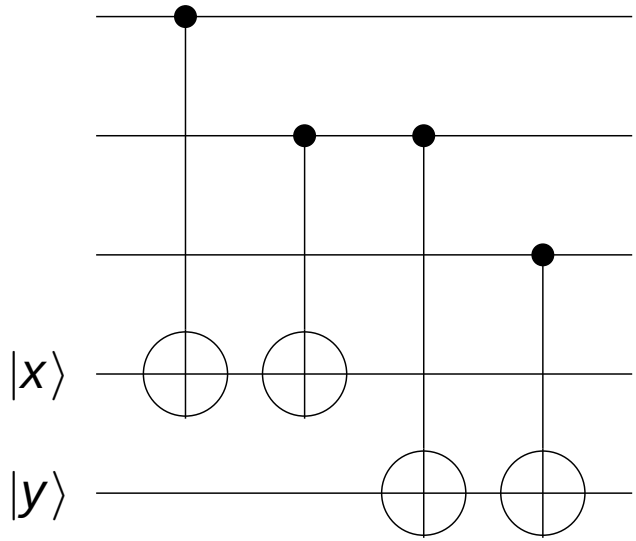
$$\begin{aligned} |e_1\rangle &= \alpha_0|100\rangle + \alpha_1|011\rangle \\ |e_2\rangle &= \alpha_0|010\rangle + \alpha_1|101\rangle \\ |e_3\rangle &= \alpha_0|001\rangle + \alpha_1|110\rangle. \end{aligned}$$

- Wir müssen Fehler beobachten, ohne zu messen.

Beobachten von Fehlern

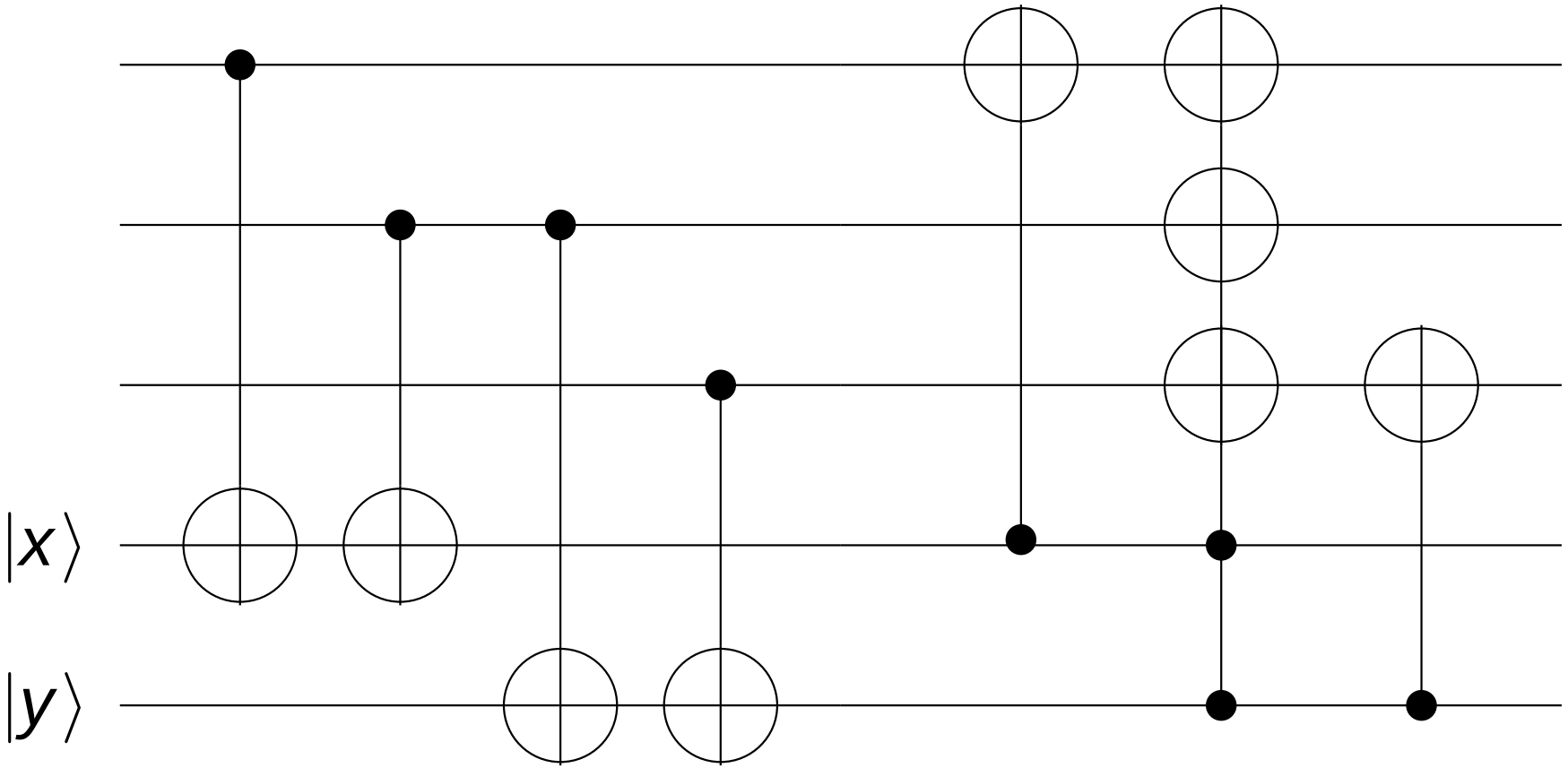
Beobachtung von Bitflips

- Wir verwenden zwei weitere Hilfsbits $|xy\rangle$, initialisiert mit $|0\rangle$.
- Das folgende Gatter erhält als Eingabe $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$.
- Auftretende Bitflips werden mit CNOT-Gattern wie folgt kopiert.



- **Fall 1** fehlerfrei: $|xy\rangle = |00\rangle$.
- **Fall 2** Bitflip $|e_1\rangle$: $|xy\rangle = |10\rangle$.
- **Fall 3** Bitflip $|e_2\rangle$: $|xy\rangle = |11\rangle$.
- **Fall 4** Bitflip $|e_3\rangle$: $|xy\rangle = |01\rangle$.
- D.h. durch *Messung der Hilfsbits* $|xy\rangle$ erkennen wir einen Fehler.
- Wir nutzen nur Relationen zwischen den ursprünglichen Bits.
- Der ursprüngliche Zustand bleibt in seiner Superposition erhalten.

Korrektur der Fehler



Korrigieren allgemeiner Fehler

Fakt 5-Qubit Code

Es existiert ein 5-Qubit Code zum Korrigieren eines generellen 1-Qubit Fehlers.

- Code korrigiert nicht nur Bit-Flips, sondern auch Phasenfehler.

Bit Commitments

Bit Commitment informal

1. **Commitment-Phase:**
   - Alice platziert ein Bit $b \in \{0, 1\}$ in einem Safe.
   - Alice sendet den Safe an Bob.
   - Bob kann den Safe nicht einsehen, lernt also nichts über b.
     (Concealing Eigenschaft)
2. **Revealing-Phase:**
   - Alice öffnet den Safe und zeigt Bob das Bit b.
   - Alice kann ihr Bit dabei nicht ändern.
     (Binding Eigenschaft)

Realisierung mittels Qubits

Protokoll Quanten Bit Commitment

Sicherheitsparameter: n

Commitment-Phase:

- Alice wählt $\mathbf{x} \in_R \{0,1\}^n$.
- **Fall 1** $b = 0$: Alice sendet $|\mathbf{y}\rangle = |\mathbf{x}\rangle$ an Bob.
- **Fall 2** $b = 1$: Alice sendet $|\mathbf{y}\rangle = H_n|\mathbf{x}\rangle$ an Bob.

Revealing-Phase:

- Alice sendet b und $\mathbf{x}$ an Bob.
- Bob misst $H_n^b|\mathbf{y}\rangle$ in der Standardbasis und vergleicht mit $|\mathbf{x}\rangle$.

Anmerkungen:

- **Conceiling:** Falls Bob in der Standard- oder der Hadamardbasis misst, erhält er 0 bzw. 1 jeweils mit Ws $\frac{1}{2}$.
- **Binding:** Falls $b' \neq b$, gilt $\mathbf{x} = \mathbf{y}$ nur mit Ws 2^{-n}.

Betrügerische Alice

Protokoll Betrügerische Alice

Sicherheitsparameter n

Commitment-Phase:

- Alice wählt n EPR-Paare $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice sendet jeweils das zweite Bit an Bob.

Revealing-Phase:

- **Fall 1:** $b = 0$: Alice misst ihr erstes Bit aller n Paare $|e\rangle$.
- **Fall 2:** $b = 1$: Alice berechnet $H|e\rangle$ und misst ihre n Qubits.
- Sei **x** das Ergebnis der Messung. Sende $b, |\mathbf{x}\rangle$ an Bob.

Anmerkung:

- Für $b = 0$ misst Bob aufgrund der Verschränkung dasselbe.
- Für $b = 1$ gilt $(H \otimes H)|e\rangle = |e\rangle$.
- D.h. auch in diesem Fall messen Alice und Bob dasselbe.

Sicheres Quanten Bit Commitment

Offenes Problem Quanten Bit Commitment

Existiert ein sicheres Quanten Bit Commitment Protokoll?

Anmerkung:

- Mayers 1996: Generische Attacke gegen Quanten BC Protokolle.
- Vermutung: Sichere Quanten-BC Protokolle sind nicht ohne weitere Annahmen konstruierbar.