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 $|\mathbf{z}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\mathbf{x}}|1\rangle) = H|x\rangle$.
- 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 $\omega = 0.x_1$ folgt

$$\begin{aligned} |z\rangle &= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i (0.x_1) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i x_1 y} |y\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x_1 y} |y\rangle = H|x_1\rangle \end{aligned}$$

- 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 $\omega = 0.x_1 x_2 \ldots x_n$ gilt

$$|z\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle = \frac{|0\rangle + e^{2\pi i 0.x_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i 0.x_1 x_2 \ldots x_n}|1\rangle}{\sqrt{2}}.$$

Beweis:

$$\begin{aligned}
|z\rangle &= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} e^{2\pi i \omega \sum_{\ell=0}^{n-1} y_\ell 2^\ell} |y_{n-1} \ldots y_0\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \cdots \sum_{y_{n-1}=0}^{1} \bigotimes_{\ell=0}^{n-1} e^{2\pi i \omega y_\ell 2^\ell} |y_\ell\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=0}^{n-1} \left(\sum_{y_\ell=0}^{1} e^{2\pi i \omega y_\ell 2^\ell} |y_\ell\rangle \right) = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=0}^{n-1} \left(|0\rangle + e^{2\pi i \omega 2^\ell} |1\rangle \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\left(|0\rangle + e^{2\pi i 0.x_1 x_2 \ldots x_n} |1\rangle \right) \otimes \ldots \otimes \left(|0\rangle + e^{2\pi i x_1 x_2 \ldots x_{n-1}.x_n} |1\rangle \right) \right)
\end{aligned}$$

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 $\omega = 0.x_1 x_2 x_3$

Gesucht: $\omega = 0.x_1 x_2 x_3$

- $|z\rangle = \left(\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_2 x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_1 x_2 x_3}|1\rangle}{\sqrt{2}}\right)$
- 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 $\alpha(x) \in \mathbb{C}[x]$ vom Grad $2^n - 1$. 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* 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 $\Omega(\frac{1}{\log\log r})$.