Quantenrechner und Grovers Algorithmus

Dirk Winkler
Informatik
Technische Universität Chemnitz

2. Januar 2005

Inhalt

Entwicklung

- Feynmann, Richard P. (1982): Simulating physics with computers
  - vermutet exponentielle Verlangsamung bei Simulation eines Quantensystems mit R Partikeln
  - Grund: Beschreibungsgrösse exponentiell vs. linear
  - Vermutung: Quantenrechner schneller
- Deutsch, David, 1985: Theorie für Quantenrechner: Beschreibung eines 'universellen Quantenrechners'
- Bernstein, Vazirani, 1997: QTM simuliert QTM in Polynomialzeit

Physikalische Systeme

- physikalisches Modell muss experimentell nachweisbar sein – Beschreibung eines Systemzustandes durch Tupel von Observablen
- zeitliche Veränderung des Zustandes: Gleichungen, Zustand von Zeit abhängig: $x(t)$ – zeitliche Entwicklung (time evolution)

  Beispiel

  - *Partikelzustand Position, Impuls,* $x = (x_1, x_2, x_3, p_1, p_2, p_3)$
  - *erhalten Zustandsraum* $\boldsymbol{R}^6$

- zusammengesetzte Systeme: Kartesisches Produkt

Probabilistische Systeme

- Diskrepanz zwischen Modellen und Realität; ggf. nur Wahrscheinlichkeitsaussagen möglich
- Annahme: System habe beobachtbare Zustände $x_1, \ldots, x_n$ (reine Zustände), diese korrespondieren mit Basisvektoren $[x_1], \ldots [x_n]$
- Zustand nur durch Verteilung gegeben: $p_1[x_1] + \cdots + p_n[x_n]$ (gemischter Zustand), Vektorschreibweise: $(p_1, \ldots, p_n)^T$

Beispiel

Beim Wurf einer fairen Münze lässt sich der Zustand als $\frac{1}{2}[Kopf] + \frac{1}{2}[Zahl]$ *auffassen (solange das Ergebnis nicht feststeht).*

Probabilistische Systeme

- Zeit diskret betrachten; Zustandsübergänge probabilistisch: $[x_i] \mapsto p_{1i}[x_1] + \cdots + p_{ni}[x_n]$, dabei $p_{1i} + \cdots + p_{ni} = 1$ und $p_{ji} = P(x_i \mapsto x_j | x_i)$
- Entwicklung eines gemischten Zustandes $p_1[x_1] + \cdots + p_n[x_n]$ zu
  $p_1(p_{11}[x_1] + \cdots + p_{n1}[x_n]) + \cdots + p_n(p_{1n}[x_1] + \cdots + p_{nn}[x_n]) = p'_1[x_1] + \cdots + p'_n[x_n]$

$$\begin{pmatrix} p'_1 \\ p'_2 \\ \vdots \\ p'_n \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}$$

- Markov-Matrix: Zeilensummen gleich Eins, damit $p'_1 + \cdots + p'_n = p_1 + \cdots + p_n$, Markovkette

Quantensysteme

Definition (Superposition für n-stufiges System)
Ein Quantenzustand besteht aus einer Überlagerung (Superposition)

$$\alpha_1 |x_1\rangle + \cdots + \alpha_n |x_n\rangle$$

- x_i: Zustände, $|x_i\rangle$: ONB des Zustandsraumes $\mathbf{H}_n$
- die komplexen α_i heissen Amplituden von x_i, die Wahrscheinlichkeit, x_i zu beobachten, ist $|\alpha_i|^2$ mit $|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$
- Messung des Zustandes (Beobachtung) führt zur Zerstörung der Superposition, System behält ermittelten Status bei

Quantensysteme

- Markovketten sind kein ausreichendes Beschreibungsmittel
- $\alpha_i = \Psi(x_i)$, Wellenfunktion
- Vektordarstellung und zeitliche Entwicklung analog zu probabilistischen Systemen:

$$\begin{pmatrix} \alpha'_1 \\ \alpha'_2 \\ \vdots \\ \alpha'_n \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Quantensysteme – Eigenschaften

- Matrizen sind unitär, daher ist zeitliche Entwicklung reversibel
- Zusammengesetzte Systeme:
  - Basiszustände je $|x_1\rangle, \ldots, |x_n\rangle$ und $|y_1\rangle, \ldots, |y_m\rangle$
  - neue Basisvektoren $\left(|x_i\rangle, |y_j\rangle\right)$
  - Darstellung $\sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij} |x_i, y_j\rangle$ mit $\sum_{i=1}^{n}\sum_{j=1}^{m} |\alpha_{ij}|^2 = 1$
  - mathematisches Modell: Tensorprodukt der Zustandsräume $\mathbf{H}_n \otimes \mathbf{H}_m$ mit Basis $|x_i\rangle \otimes |y_j\rangle = |x_i\rangle\,|y_j\rangle = |x_i, y_j\rangle$ (Dimension mn)
  - Tensorprodukt nicht kommutativ
  - Zustand *zerlegbar*, falls

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij} |x_i\rangle\,|y_j\rangle = \left(\sum_{i=1}^{n} \alpha_i |x_i\rangle\right)\left(\sum_{j=1}^{m} \beta_j |y_j\rangle\right)$$

  - ansonsten *verschränkt*

Quanteninformation

- Quantenbit in zweistufigem System speichern: $c_0 \left|0\right\rangle + c_1 \left|1\right\rangle$
- $\left|0\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \left|1\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Ein-Bit-Operation durch unäres Quantengatter: unitäre Abbildung $U : \mathbf{H}_2 \mapsto \mathbf{H}_2$ mit
  $\left|0\right\rangle \mapsto a \left|0\right\rangle + b \left|1\right\rangle, \left|1\right\rangle \mapsto c \left|0\right\rangle + d \left|1\right\rangle$
- unitäre Matrix

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} c \\ d \end{pmatrix}$$

Quantengatter

- Walsh-Matrix, Hadamard-Matrix:

$$H = W_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

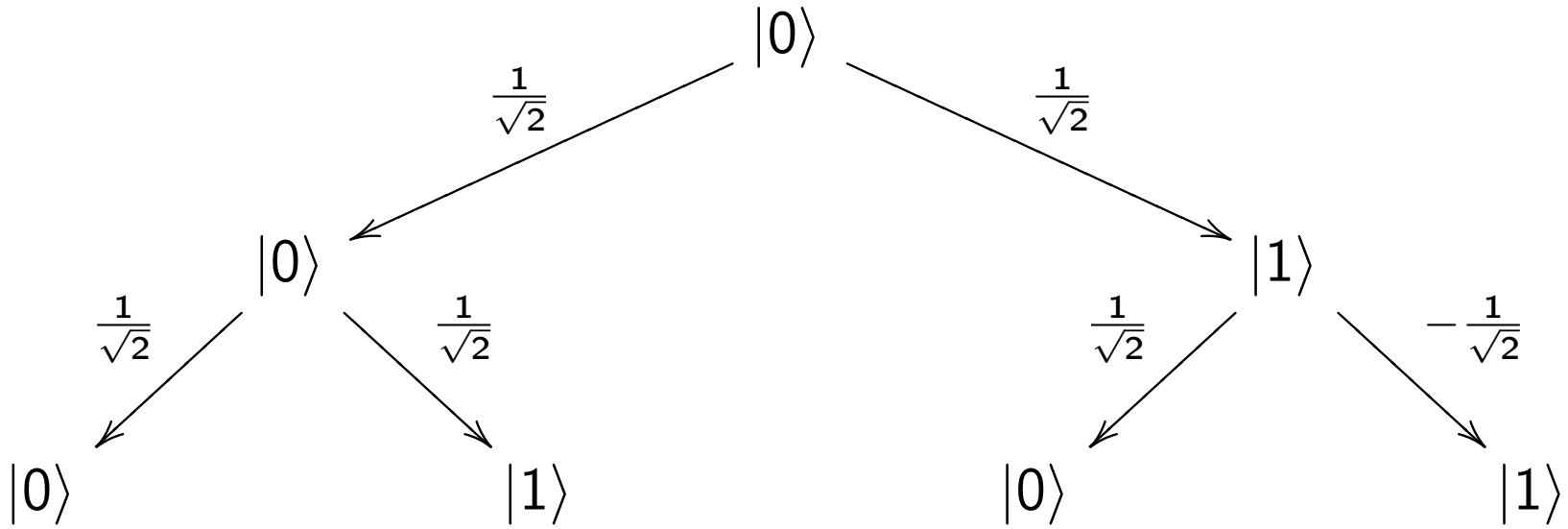
- $W_2 W_2 = I$, W_2 ist unitär

Beispiel

- *Simulation eines Münzwurfs mit W_2; wir definieren die Zustände $|Kopf\rangle = \binom{1}{0}$ und $|Zahl\rangle = \binom{0}{1}$.*
  $|Kopf\rangle \mapsto \frac{1}{\sqrt{2}} |Kopf\rangle + \frac{1}{\sqrt{2}} |Zahl\rangle = \frac{1}{\sqrt{2}} \binom{1}{1}$.
- *Im Folgezustand wird also Kopf oder Zahl mit Wk. $\frac{1}{2}$ beobachtet. Verzichtet man auf die Messung und führt die Operation erneut aus, ergibt sich der Zustand $\binom{1}{0} = W_2 \frac{1}{\sqrt{2}} \binom{1}{1}$, also $|Kopf\rangle$.*
- *Beim zweiten Münzwurf kann nur Kopf herauskommen—probabilistisch nicht modellierbar.*

Interferenz

- auf ein Quantenbit bezogen:



- Grund: Wahrscheinlichkeiten werden nicht selbst überlagert, aber die Amplituden α_i bzw. Wellenfunktionen Ψ
- bei probabilistischen Systemen nicht möglich, da nur nichtnegative reelle Koeffizienten auftauchen

Quantenregister

- Zwei-Bit-Register: $\mathbf{H}_4 = \mathbf{H}_2 \otimes \mathbf{H}_2$
- Basis $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
- Zustand $c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle$ mit $\sum_{i=0}^{3} |c_i|^2 = 1$
- Wahrscheinlichkeit, dass erstes Qubit im Zustand 0 bzw. 1 ist: $|c_0|^2 + |c_1|^2$ und $|c_2|^2 + |c_3|^2$
- n-Bit-Register: $\mathbf{H}_{2^n} = \mathbf{H}_2 \otimes \cdots \otimes \mathbf{H}_2$
- Zustand teilbar (decomposable), wenn als Produkt darstellbar

Quantenregister

Beispiel

- *teilbarer Zustand:*
  $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- *Dagegen ist* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *nicht teilbar.*

Beweis.
Sei $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b_2|1\rangle)$. Dann
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + a_2b_2|11\rangle$.

$$\Longrightarrow \qquad a_1a_2 = 1/\sqrt{2} \qquad b_1a_2 = 0$$
$$b_1b_2 = 1/\sqrt{2} \qquad a_1b_2 = 0$$

Dies führt zum Widerspruch. □

Operationen auf Quantenregistern

- betrachten ohne Einschränkung Zwei-Bit-Register

Definition (Binäre Quantengatter)

Ein binäres Quantengatter ist eine unitäre Abbildung $U : \mathbf{H}_4 \longrightarrow \mathbf{H}_4$.

- $\mathbf{H}_4 = \mathbf{H}_2 \otimes \mathbf{H}_2$ enthält Vektoren, die Tensorprodukte aus Vektoren von $\mathbf{H}_2$ sind
- Tensorprodukt zweier Matrizen $M \otimes N$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} =$$

$$\begin{pmatrix} a \begin{bmatrix} e & f \\ g & h \end{bmatrix} & b \begin{bmatrix} e & f \\ g & h \end{bmatrix} \\ c \begin{bmatrix} e & f \\ g & h \end{bmatrix} & d \begin{bmatrix} e & f \\ g & h \end{bmatrix} \end{pmatrix} = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix}$$

Operationen auf Quantenregistern

Beispiel

- *Hadamard-Transformation $W_2 = H$ auf zwei Qubits erweitern:*

$$H_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

- *Anwendung auf Basisvektor $|x_1\rangle\,|x_2\rangle\,,\ x_1, x_2 \in \{0,1\}$:*

$$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_2}|1\rangle\right) =$$

$$\frac{1}{2}\left(|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_1+x_2}|11\rangle\right)$$

- *Mit $x \odot i = \left(\sum_{j=1}^{n} x_j i_j\right)$ mod 2 gilt für die Erweiterung auf $\mathbf{H}_n$*

$$\mathbf{H}_n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{x\odot i}|i\rangle$$

Grovers Suchalgorithmus

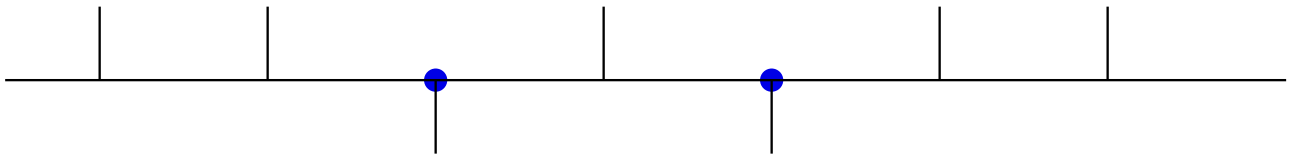
- gegeben: $f : \{0,1\}^n \rightarrow \{0,1\}$
  gesucht: x mit $f(x) = 1$
- Suchraum mit $N = 2^n$ Elementen, Annahme: $t \geq 1$ Lösungen
- f als Quanten-Blackbox-Funktion darstellen:
- für $f : \{0,1\}^n \rightarrow \{0,1\}^m$ existiert ein umkehrbares $F : \{0,1\}^{m+n} \rightarrow \{0,1\}^{m+n}$ sowie die zugehörige unitäre Transformation U_f

$$\begin{aligned} F(x,b) &= (x, b \oplus f(x)) \\ U_f \left|x,b\right\rangle &= \left|x, b \oplus f(x)\right\rangle \end{aligned}$$

- $F(x,0) = (x, f(x))$, hier ist $m = 1$
- jeder Basisvektor $\left|x_i\right\rangle$ (Dimension $N = 2^n$) stellt eine mögliche Lösung dar

Vorgehen

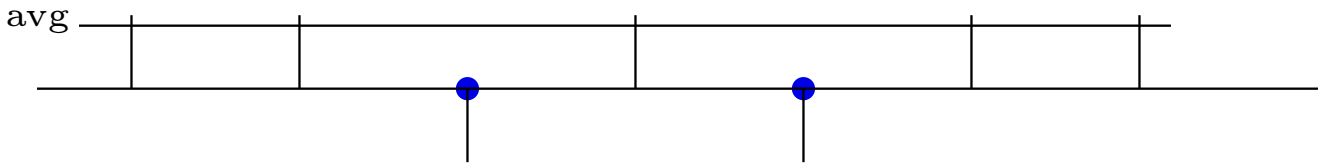
- Idee: Superposition aller Eingaben für f erzeugen, Amplituden der Lösungen verstärken, anschliessend Messung durchführen
- Walsh-Hadamard-Transformation
  - Erzeugen einer Superposition, in der alle Zustände (Eingaben für f) gleichwahrscheinlich enthalten sind
  - $H_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{x \odot i} |i\rangle$, $H_n = H_n^{-1}$
  - Qubits anschliessend jeweils im Zustand $\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$
- V_f-Operator: separiert die Lösungsvektoren durch Negation der Amplitude (bei Grover rein reellwertig):
  - $V_f |x\rangle = (-1)^{f(x)} |x\rangle$
  - Wahrscheinlichkeiten bleiben (noch) erhalten
  - Umsetzung durch $U_f |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = V_f |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$, Skizze:



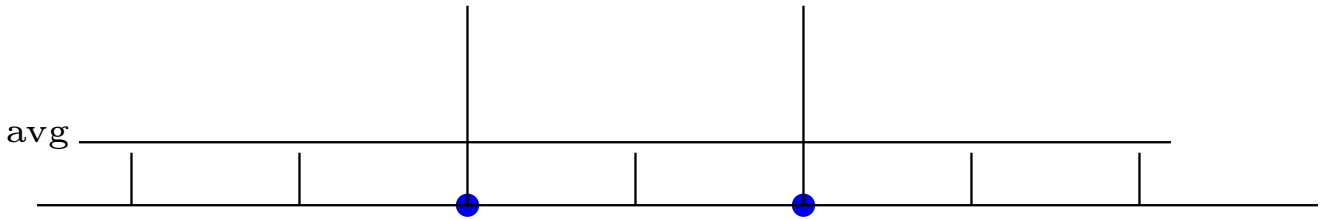
Vorgehen

D_n: Inversion am Durchschnitt

- Amplituden müssen betragsmäßig geändert werden
- sei der Durchschnitt der Amplituden $A = (\sum_{i=1}^{N} \alpha_i)/2^n$:



- Operator D_n hat folgende Wirkung:



Inversion am Durchschnitt – Operator D_n

$$D_n \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} A - (\alpha_1 - A) \\ \vdots \\ A - (\alpha_n - A) \end{pmatrix} = \begin{pmatrix} 2A - \alpha_1 \\ \vdots \\ 2A - \alpha_n \end{pmatrix}$$

$$D_n = \begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{2^n} & \cdots & \frac{2}{2^n} & \frac{2}{2^n} - 1 \end{pmatrix}$$

- auf Basis von Quantengattern:
  - $D_n = H_n R_n H_n$, wobei

$$R_n = \begin{cases} |x\rangle, & |x\rangle = \left|0^{(n)}\right\rangle \\ -|x\rangle, & \textit{sonst} \end{cases}$$

  - R_n entspricht V_f mit $f(x) = x_1 \vee \cdots \vee x_n$

Algorithmus

1: gleichmäßige Superposition generieren: $|z\rangle := H_n \left|0^{(n)}\right\rangle$

2: $G_f = D_n V_f$ $\left\lfloor \frac{\pi}{4 arcsin\sqrt{\frac{t}{N}}} \right\rfloor$-mal auf $|z\rangle$ anwenden

3: Beobachtung des Registers, Wert in x_0 speichern

4: $\exists 1 : f(x_0) = 1 \rightarrow$ Ende, x_0 ausgeben

5: $\exists 2 : f(x_0) = 0 \rightarrow$ gehe zu 1.

- Bemerkungen
  - Wirkung des Grover-Operators:
    für $|z_0'\rangle = V_f |z_0\rangle = \frac{1}{\sqrt{N}} \left(\sum_{i \in \bar{L}} |i\rangle - \sum_{i \in L} |i\rangle\right)$,
    ist $|z_1\rangle = D_n |z_0'\rangle \approx \frac{1}{\sqrt{N}} \left(\sum_{i \in \bar{L}} |i\rangle + 3 \sum_{i \in L} |i\rangle\right)$
  - $x \in (0,1] \Longrightarrow \arcsin x > x :$ $\left\lfloor \frac{\pi}{4 \arcsin \sqrt{\frac{t}{N}}} \right\rfloor < \frac{\pi}{4} \sqrt{\frac{N}{t}}$

Analyse

- Eigenschaften
  - erwartete Iterationen*: $O(\sqrt{N/t})$, probabilistisch: $\Omega(N/t)$
  - Laufzeit: je Iteration $O(n) = O(\log N)$ Qubit-Operationen, also insgesamt $O(\sqrt{N/t}\log N)$
- Beweisskizze (*)
  - l_i: Amplitude einer Lösung nach Anwendung von G_f^i, k_i: Nichtlösung
  - Durchschnitt in Runde $i > 0$: $A_i = (t\,l_{i-1} + (N-t)k_{i-1})/N$
  - Einsetzen Rekursion ($k_i = 2A_i - k_{i-1}$, $l_i = 2A_i - l_{i-1}$ ergibt

$$l_0 = k_0 = 1/\sqrt{N} \tag{1}$$

$$k_i = \frac{N-2t}{N}k_{i-1} - \frac{2t}{N}l_{i-1} \tag{2}$$

$$l_i = 2\frac{N-t}{N}k_{i-1} + \frac{N-2t}{N}l_{i-1} \tag{3}$$

Analyse

- Fortsetzung Beweisskizze
  - definieren $\theta = \arcsin\sqrt{t/N}$, damit gilt

$$\sin\theta = \sqrt{t/N} \qquad \sin^2\theta = t/N$$
$$\cos^2\theta = (N-t)/N \qquad \cos\theta = \sqrt{(N-t)/N}$$

  - Lösungen (Bew. durch Additionstheoreme und Induktion):

$$k_i = \cos\left((2i+1)\theta\right)/\sqrt{N-t} \tag{4}$$
$$l_i = \sin\left((2i+1)\theta\right)/\sqrt{t} \tag{5}$$

  - Wahrscheinlichkeit, eine der t Lösungen zu messen, ist
    $t\, l_i^2 = \sin^2\left((2i+1)\theta\right) \stackrel{!}{=} 1 \quad \Longrightarrow \quad (2i+1)\theta = \pi/2$
  - es folgt $i = \frac{\pi}{4\theta} - \frac{1}{2}$, daher wird G_f $\lfloor \pi/(4\theta) \rfloor$-mal angewendet

Analyse

- Fortsetzung Beweisskizze
  - $j = \lfloor i \rfloor$ abgerundet, daher Fehlermöglichkeit (Zeile 5, $\sqsupset 2$)
  - erneuter Durchlauf, wenn Nichtlösungsvektor gemessen wird:

$$\begin{aligned} P_E = (N-t)k_j^2 &= \cos^2\left[(2j+1)\theta\right] \\ &= \cos^2\left[(2\lfloor \pi/(4\theta) \rfloor + 1)\,\theta\right] \\ &= \cos^2\left[(2\,(\pi/(4\theta) - \epsilon) + 1)\,\theta\right] \\ &= \cos^2\left[\pi/2 + (1-2\epsilon)\theta\right] \\ &= \sin^2\left[(1-2\epsilon)\theta\right] \end{aligned} \tag{6}$$

  - $\epsilon \in [0,1) \Longrightarrow \sin(-\theta) < \mathit{sin}[(1-2\epsilon)\theta] \leq \sin\theta$, daraus folgt

$$P_E \leq \sin^2\theta = t/N$$

Analyse

- Fortsetzung Beweisskizze
  - Wahrscheinlichkeit für Neudurchlauf ist P_E; Anzahl von Durchläufen $R \sim GEO(1 - P_E)$ hat Erwartungswert $E(R) = \frac{1}{1-P_E} \leq \frac{N}{N-t}$, dieser ist ≤ 2 für $t \leq N/2$ und 1 sonst
  - pro Durchlauf $\left\lfloor \frac{\pi}{4\theta} \right\rfloor + 1 < \frac{\pi}{4}\sqrt{\frac{N}{t}} + 1$ Iterationen, insgesamt also

$$O\left(\sqrt{\frac{N}{t}}\right)$$

□

  - Sonderfall: $t = N/4 \Longrightarrow P_E = 0$, damit ist $\theta = \frac{\pi}{6}$; einsetzen in (6)

Verallgemeinerungen

- unbekannte Lösungszahl ($t < \frac{3}{4}N$): ebenfalls $O\left(\sqrt{\frac{N}{t}}\right)$
- andere Lösungsräume $\{x_1, \ldots x_n\}$: ersetze H_n durch Transformation, die den $|x_i\rangle$ die gleiche Amplitude zuweist
- $\exists$ Grover-basierter Algorithmus, der das Minimum mit Wahrscheinlichkeit $\frac{1}{2}$ in $O(\sqrt{N})$ Iterationen findet
- Lösungen zählen: Amplituden der Vektoren in L und $\overline{L}$ zeigen nach Anwendung des Grover-Operators Periodizitäten; Quanten-Fourier-Transformation bestimmt diese annähernd und lässt auf Lösungsanzahl schlussfolgern

Literatur


Hirvensalo, Mika (2004). *Quantum Computing.* Zweite Auflage. Heidelberg: Springer.


Gruska, Jozef (1999). *Quantum Computing.* London: McGraw-Hill International (UK) Limited.


Berger, Andreas (2002). *Grovers Suchalgorithmus.* Technische Universität Chemnitz. Fakultät für Informatik. <http://www.tu-chemnitz.de/informatik/HomePages/ThIS/Seminare/ss02/QC/berger.pdf>