Grover-Algorithmus

Referent: Mohamed TARIK

RWTH-Aachen

SS 2005

Geleitet von: Dr. Koch.

Gliederung:

Algorithmen:

Was ist ein Algorithmus?

• Ein Algorithmus ist ein geeignetes Verfahren zur Lösung eines Problems.

Problem —Algorithmus→ Lösung

Quantenalgorithmen (QA):

• Die Quantengatter können die durch Qubits repräsentierte Information verarbeiten. Sie lassen sich durch unitäre Operatoren darstellen. Sie sind physikalisch verwirklichbar (Ionen-Falle).

• Beispiele: Ein-Qubit-Gatter (Hadamard-Gatter)
Zwei-Qubit-Gatter (CNOT-Gatter).

Algorithmen:

• Die gesamte Wahrscheinlichkeit vor und nach einer Operation muss gleich sein. Wegen dieser Bedingung und der Linearität sind nur umkehrbare Operationen (Reversibilität) erlaubt, d.h. die Gatter sind unitär.

• Die QA benutzen die Überlagerung in einem Quantensystem, dadurch kann man paralleles Rechnen auszuführen.

• Quantenalgorithmen müssen möglichst ohne Zwischenmessungen auskommen, da bei Messungen Quanteninformation verloren geht.

Problemdarstellung:

Das Problem:

- Eine oder mehrere Elemente in einer unstrukturierten Datenbank suchen, die gesuchte Elemente besitzen z.B. ein gemeinsames Kriterium.

Beispiel:

- zu einer Telefonnummer den Name einem Telefonbuch zu finden (die Telefonnummer sind nicht sortiert).

Problemdarstellung:

- Suchraum: $S = \{ x_0, x_1, \ldots x_{N-1} \}$.
- Indexmenge: $I=\{ 0,1,...,N \}$.
- Für zwei dimensionalen Systeme: $N=2^n$.
- wir werden bestimmte Elemente x_i aus S durchsuchen.
- Sei L die Lösungsmenge von x_i, und M die Lösungsanzahl, d.h.
  $0 \leq M \leq N$
- Sei die Funktion f: $f(x)=1$ wenn $x \in L$.
  $f(x)= 0$ sonst.

Lösung:

Klassischer Suchalgorithmus:

• Alle Datensätze werden durchprobiert, die Funktion f wird im Mittel N/2 aufgerufen, d.h. der Algorithmus benötigt O(N).

Grover-Algorithmus:

• Grover-Algorithmus braucht nur $O(N^{1/2})$! (Grover in 1996.)

• Z.B. das Problem mit 1000 000 Telefonnummer wird eine Lösung in 1000 Schritten gefunden, statt 500 000 klassisch.

Die im Grover-Algorithmus verwendeten Operatoren:

Hadamard-Operator:

• Der Hadamard-Operator wird durch die Matrix H beschrieben:

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

• H ist unitär. Für ein Zwei-Qubit-System gilt:

$$H|0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right)$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right)$$

Die im Grover-Algorithmus verwendeten Operatoren:

Die Walsh-Hadamard-Transformation:

• Wird der Hadamard-Operator auf jedes Qubit eines n-Dimensionalen Registers angewandet, so erhalten wir die sog. „Walsh-Hadamard-Transformation“:

$$\mathrm{H}^{\otimes n} = \mathrm{H} \otimes \mathrm{H} \otimes \ldots \otimes \mathrm{H}$$

$$\mathrm{H}^{\otimes n} \left|0\right\rangle = \frac{1}{\sqrt{\mathrm{N}}} \sum_{x=0}^{N-1} \left|x\right\rangle$$

$$\left|0\right\rangle \equiv \left|0\right\rangle^{\otimes n} \equiv \left|00.....0\right\rangle$$

Die im Grover-Algorhitmus verwendeten Operatoren:

Der Phasenverschiebungsoperator:

• Er ist definiert durch (P ist unitär):

$$P = 2|0\rangle\langle 0| - I \qquad P = \begin{pmatrix} 1 & 0 & 0 & . & . \\ 0 & -1 & 0 & . & . \\ 0 & 0 & -1 & . & . \\ . & . & . & . & . \\ . & . & . & . & . \end{pmatrix}$$

• P verändert nicht den Zustand $|0\rangle$, und für die anderen Zustände wird die Phase um π verschoben.

Die im Grover-Algorithmus verwendete Operatoren:

Das Orakel:

• Ein Orakel ist ein Black Box, d.h. die interne Implementierung bleibt im voraus unbekannt, d.h. es ist nicht von Algorithmus vorgegeben.

• Das Orakel ist der unitäre Operator U_f :

$$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

• Sei $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, wenn $|x\rangle$ eine Lösung ist (f(x)=1), wird ihre Phase um π verschoben :

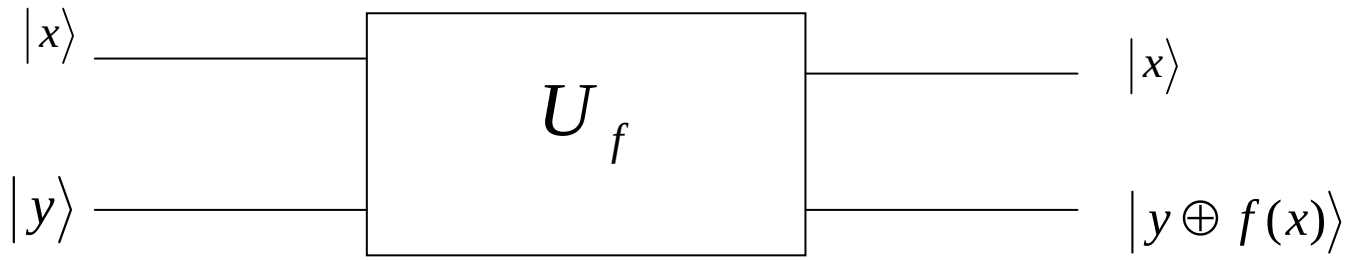
$$U_f |x\rangle|y\rangle = \left(\frac{1}{\sqrt{2}}\right) U_f |x\rangle \ (|0\rangle - |1\rangle)$$

$$= \left(\frac{1}{\sqrt{2}}\right) |x\rangle \ [(|0\rangle - |1\rangle) \oplus f(x)]$$

$$= \left(\frac{1}{\sqrt{2}}\right) (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

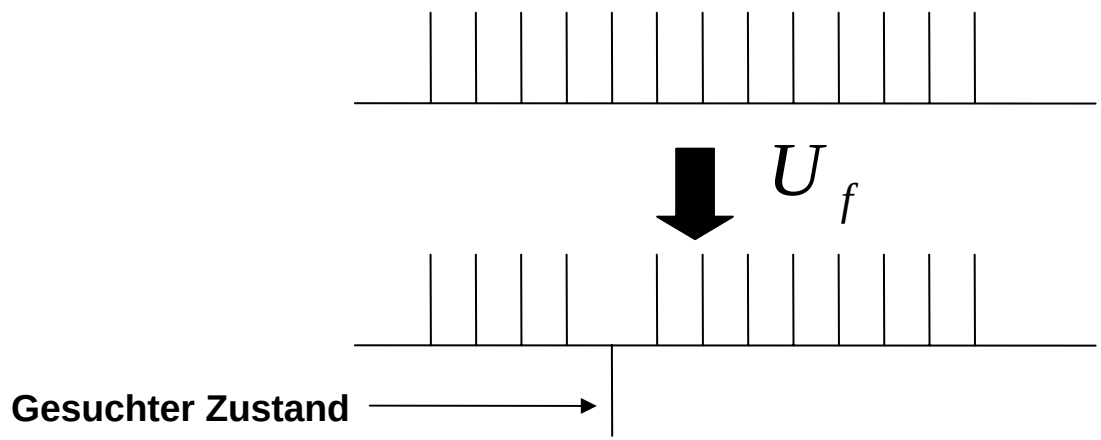
Die in Grover-Algorhitmus verwendete Operatoren:

Der Schaltkreis Des Orakels:



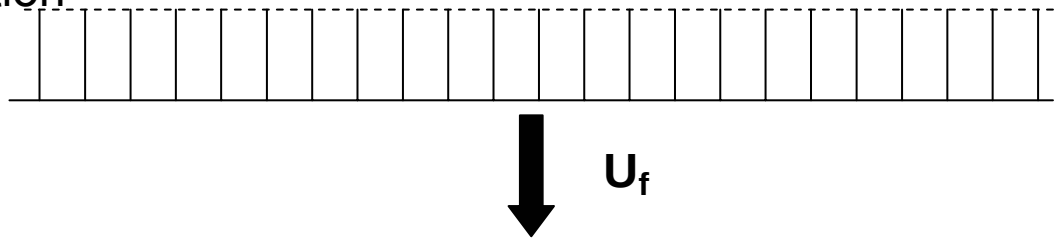
Schematische Darstellung:

• Im Grover-Algorithmus invertiert das Orakel die Amplitude des Lösungszustandes.

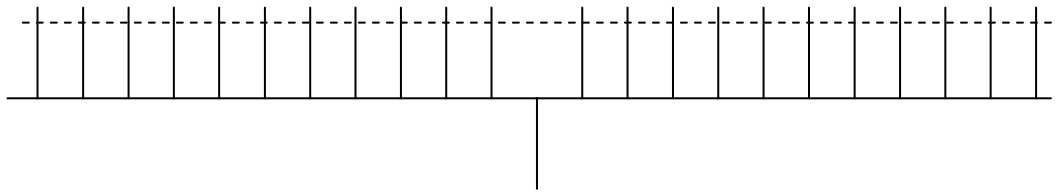


Idee zur Amplitudeverstärkung:

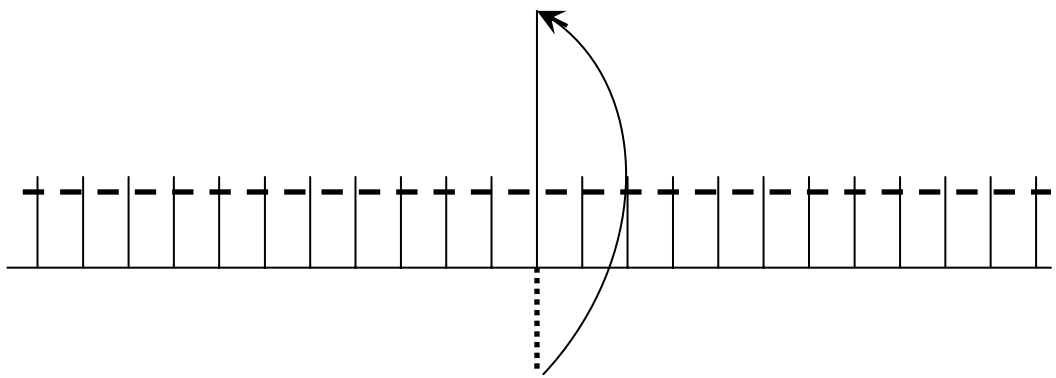
- Anfangszustand: Linearkombination



- Die Wirkung des Orakels:



- Idee: Spieglung um Mittelwert:



- Frage: mit welchem unitären Operator ist diese Spieglung realisierbar?

Grover-Iteration:

Grover-Idee:

• Man verwendet den Parallelismus der Quantentheorie und die sog. „Grover-Iteration“ in einem Quantenregister, um die Wahrscheinlichkeit des richtigen Ergebnis zu erhöhen und die der Nichtlösungen zu verringern .

Das Verfahren:

1- Das Register wird im Anfangszustand präpariert: $|0\rangle$

2- Eine gleichmäßige Superposition durch $H^{\otimes n}$ wird erzeugt: $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$

3- Das Orakel wird angewandt, und dadurch die Amplituden der gefundenen Lösungen geflippt.

4- Wir wenden $H^{\otimes n}$ an.

5- Wir wenden der Phasenverschiebungsoperator P an.

6- Dann wieder $H^{\otimes n}$ anwenden.

Grover-Iteration:

Die Grover-Iteration/ der Grover-Operator:

• Die drei letzten Schritten werden die Amplitude der Lösung erhöhen, d.h. die Wahrscheinlichkeit –bei einer Messung- wird größer.

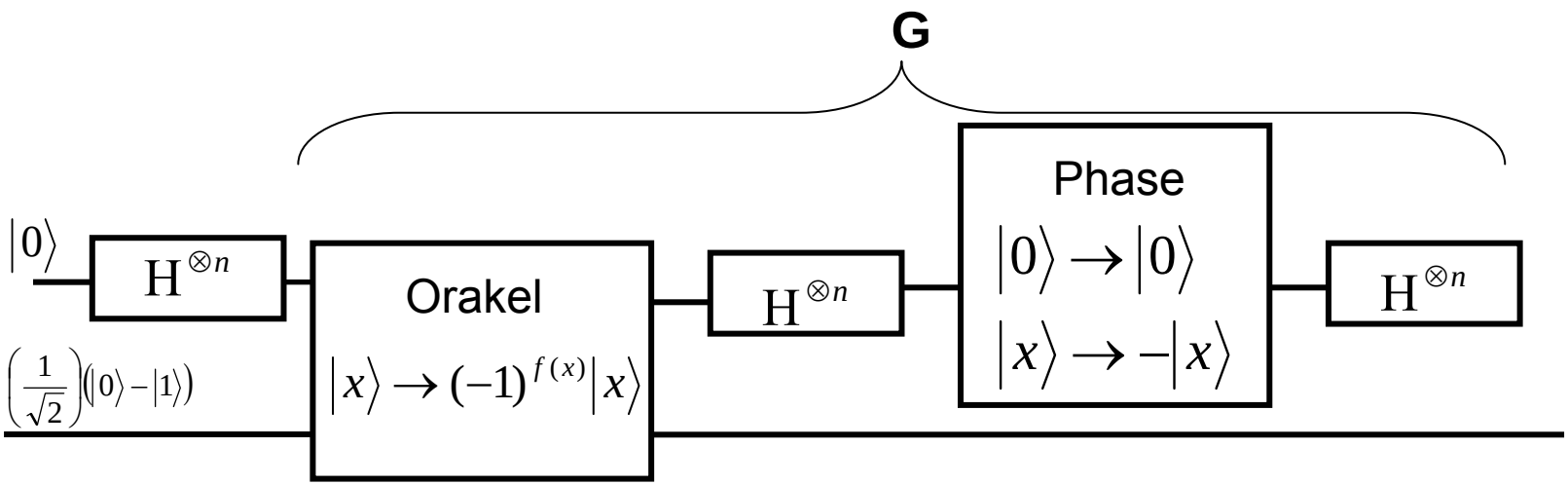
• Die vier letzten Schritten sind die Grover-Iteration –oder Grover-Operator genannt-.

• Der Grover-Operator lautet:

$$G = H^{\otimes n}.(2|0\rangle\langle 0| - \mathrm{I})H^{\otimes n}.U_f$$
$$= (2|\Psi\rangle\langle\Psi| - \mathrm{I}).U_f$$

Grover-Iteration:

Schaltkreis der Grover-Iteration:



Verstärkung der Amplitude:

Inversion um den Mittelwert:

- Sei der Operator: $D = 2|\psi\rangle\langle\psi| - \mathrm{I}$
- Die Wirkung von D auf einen allgemeinen Zustand ist:

$$|\phi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad und \quad |\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$\langle\psi|\phi\rangle = \frac{1}{\sqrt{N}} \sum_x \alpha_x = \sqrt{N} A \quad \therefore \quad A = \frac{1}{N} \sum_x \alpha_x \text{ (Mittelwert)}$$

$$D|\phi\rangle = 2|\psi\rangle\langle\psi|\phi\rangle - |\phi\rangle$$

$$= 2\left(\frac{1}{\sqrt{N}} \sum |x\rangle\right)(\sqrt{N} A) - \sum \alpha_x |x\rangle$$

$$= 2\sum |x\rangle A - \sum \alpha_x |x\rangle$$

$$= \sum (2A - \alpha_x)|x\rangle$$

$$D: \qquad \alpha_x \rightarrow 2A - \alpha_x$$

d.h. die Koeffizienten von |x> werden um den Mittelwert A gespiegelt , man nennt D die „Inversion um den Mittelwert“.

Verstärkung der Amplitude:

Die Matrix von D:

$$D = \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \frac{2}{N} & \cdot & \cdot & \cdot & \frac{2}{N}-1 \end{pmatrix}$$

Grover-Algorithmus:

- Die Grover-Iteration wird „oft“ angewandet, um mit Sicherheit bei einer Messung eine oder mehrere Lösungen zu finden.

Grover-Algorithmus: (Der Fall M=1)

1- Input: $\left(\frac{1}{\sqrt{2}}\right)|0\rangle\left(|0\rangle-|1\rangle\right)$

2- Anwendung von $H^{\otimes n}$: $H^{\otimes n}|0\rangle=|\Psi\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

3- G k-Mal anwenden : (mit k = O(N½)):

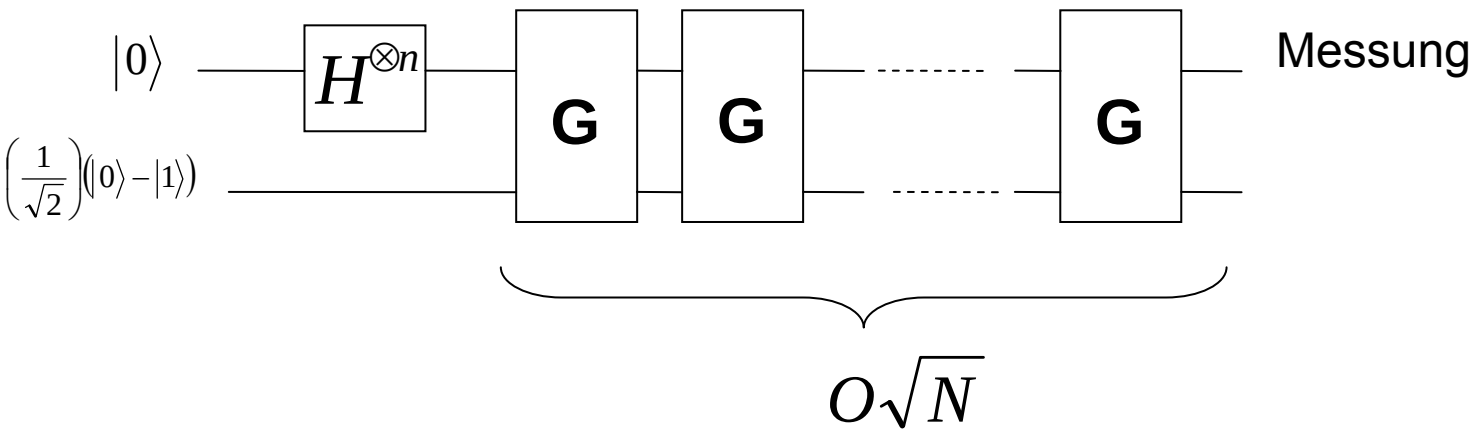
$$(G)^{\otimes k}|\Psi\rangle[(\frac{1}{\sqrt{2}})(|0\rangle-|1\rangle)]=|x_0\rangle[(\frac{1}{\sqrt{2}})(|0\rangle-|1\rangle)]$$

4- Output: $|x_0\rangle$

(aus einer Messung der n-Qubits ergibt sich die gesuchte Lösung x_0).

Grover-Algorithmus:

Schaltkreis des Grover-Algorhitmus: (der Fall M=1)



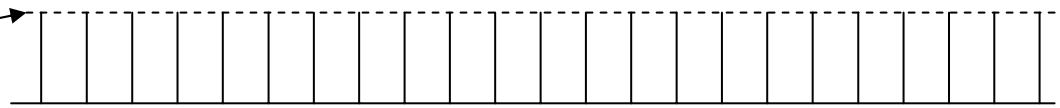
Grover-Algorithmus:

Schematische Darstellung des Grover-Algorithmus im Fall M=1:

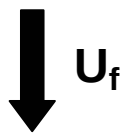
1- Input: $\left(\frac{1}{\sqrt{2}}\right)|0\rangle\left(|0\rangle-|1\rangle\right)$

2- Anwendung von: $H^{\otimes n}|0\rangle=|\Psi_0\rangle=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

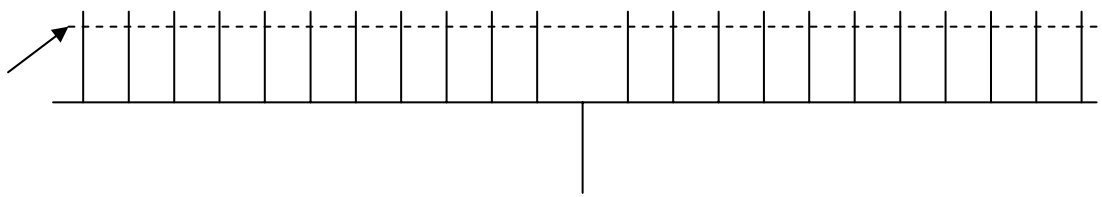
Der Mittelwert: $\frac{1}{\sqrt{N}}$



3- Anwendung von U_f: $|\psi_1\rangle=\frac{1}{\sqrt{N}}\left(\sum_{x\notin L}|x\rangle-\sum_{x\in L}|x\rangle\right)$



Der Mittelwert sinkt

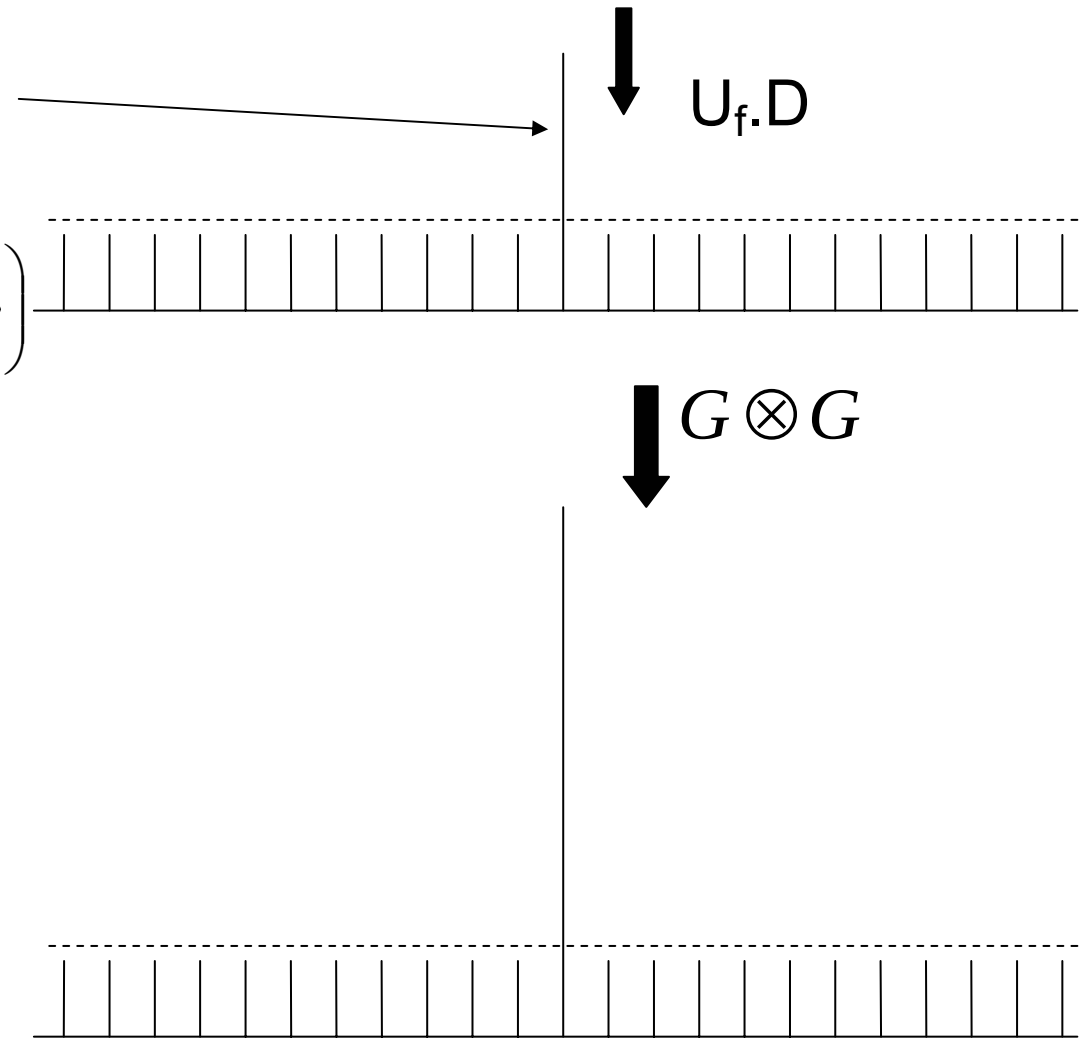


Grover-Algorithmus:

4- Anwendung von D:

Gesuchter Zustand am Mittelwert gespiegelt:

$$|\psi_2\rangle \approx \frac{1}{\sqrt{N}}\left(\sum_{x\notin L}|x\rangle + 3\sum_{x\in L}|x\rangle\right)$$



5- Zweite Iteration von G:

Einfaches Bespiel:

- Der Fall: N=4, M=1

gesuchter Zustand: $|01\rangle$

Input: $|00\rangle$.

$$H^{\otimes 2}|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

$$U_f H^{\otimes 2}|00\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle).$$

$$\begin{aligned} H^{\otimes 2} U_f H^{\otimes 2}|00\rangle = \frac{1}{4}(&|00\rangle + |01\rangle + |10\rangle + |11\rangle \\ &-|00\rangle + |01\rangle - |10\rangle + |11\rangle \\ &|00\rangle + |01\rangle - |10\rangle - |11\rangle \\ &|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\ = \frac{1}{2}(&|00\rangle + |01\rangle - |10\rangle + |11\rangle). \end{aligned}$$

$$PH^{\otimes 2} U_f H^{\otimes 2}|00\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

$$\begin{aligned} H^{\otimes 2} P H^{\otimes 2} U_f (H^{\otimes 2}|00\rangle) &= G(H^{\otimes 2}|00\rangle) \\ &= \frac{1}{4}(|00\rangle + |01\rangle + |10\rangle + |11\rangle \\ &\quad -|00\rangle + |01\rangle - |10\rangle + |11\rangle \\ &\quad |00\rangle + |01\rangle - |10\rangle - |11\rangle \\ &\quad -|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\ &= \frac{1}{4}.4|01\rangle \\ &= |01\rangle \end{aligned}$$

Output: $|01\rangle$

Geometrische Veranschaulichung:

- Die Nichtlösungen : $$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in S, x \notin L} |x\rangle$$

- Die Lösungen: $$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in L} |x\rangle$$

- Der Vektorraum (der Suchraum) aufgespannt durch den Vektor:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

Geometrische Veranschaulichung:

- Der Winkel der Rotation:

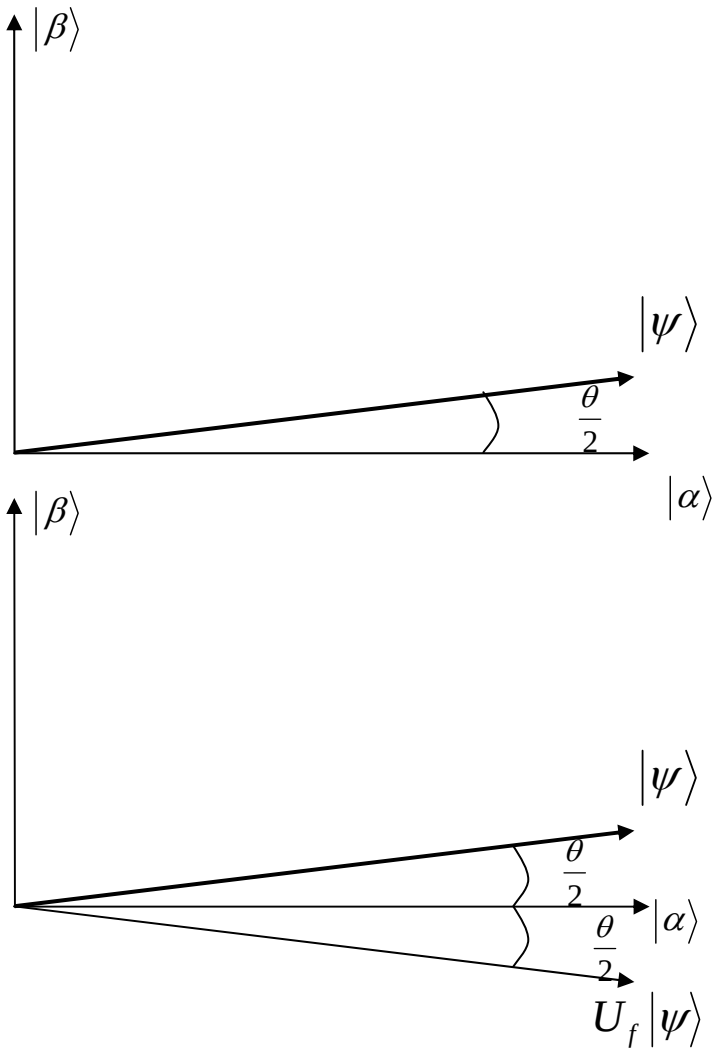
$$\cos(\frac{\theta}{2}) = \sqrt{\frac{N-M}{N}}$$

$$\sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}}$$

$$\left|\psi\right\rangle = \cos(\frac{\theta}{2})\left|\alpha\right\rangle + \sin(\frac{\theta}{2})\left|\beta\right\rangle$$

- Die Wirkung des Orakels:

$$U_f \left|\psi\right\rangle = \cos(\frac{\theta}{2})\left|\alpha\right\rangle - \sin(\frac{\theta}{2})\left|\beta\right\rangle$$

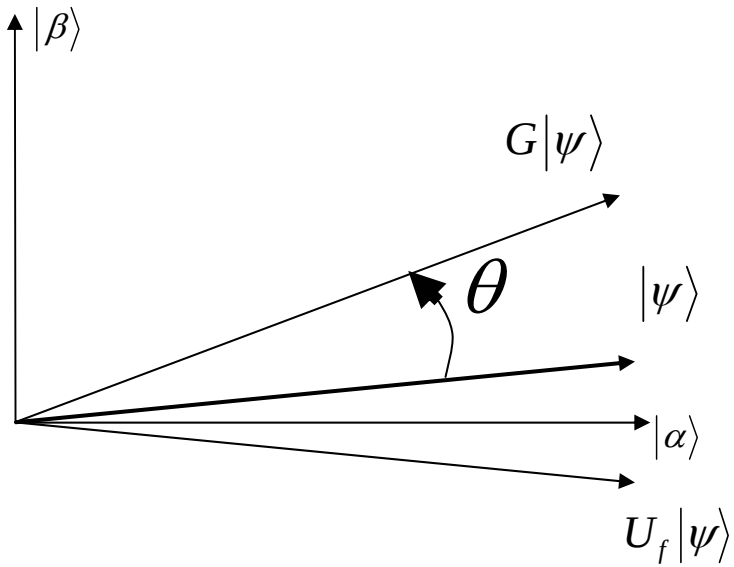


Geometrische Veranschaulichung:

• Aus der Wirkung von $2|\Psi\rangle\langle\Psi| - \mathrm{I}$ (Spieglung an $|\psi\rangle$) ergibt sich:

$$(2|\psi\rangle\langle\psi| - \mathrm{I})U_f|\psi\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|\beta\rangle$$

$$G|\psi\rangle = \cos(\frac{3\theta}{2})|\alpha\rangle + \sin(\frac{3\theta}{2})|\beta\rangle$$



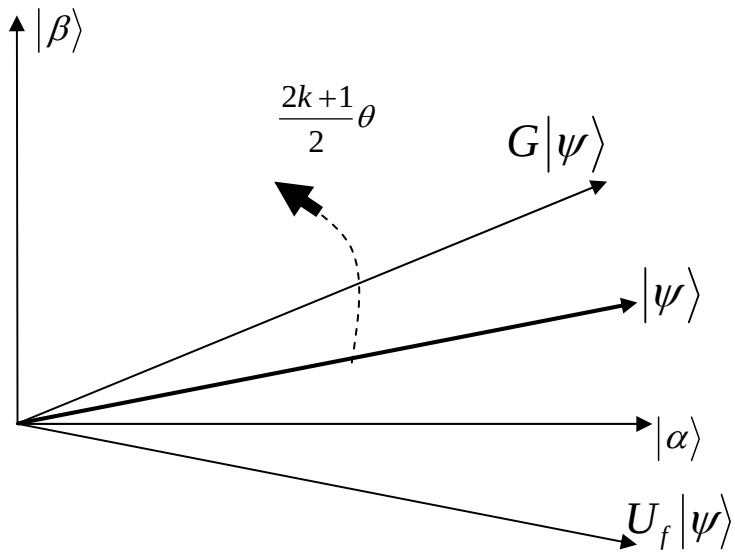
• Die Grover-Iteration ist durch die folgende Matrix gegeben:

$$G = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Geometrische Veranschaulichung:

- Für mehrere Iterationen (k-mal) folgt:

$$G|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$



- Wie viele Iterationen braucht man genau, um eine Lösung zu finden?

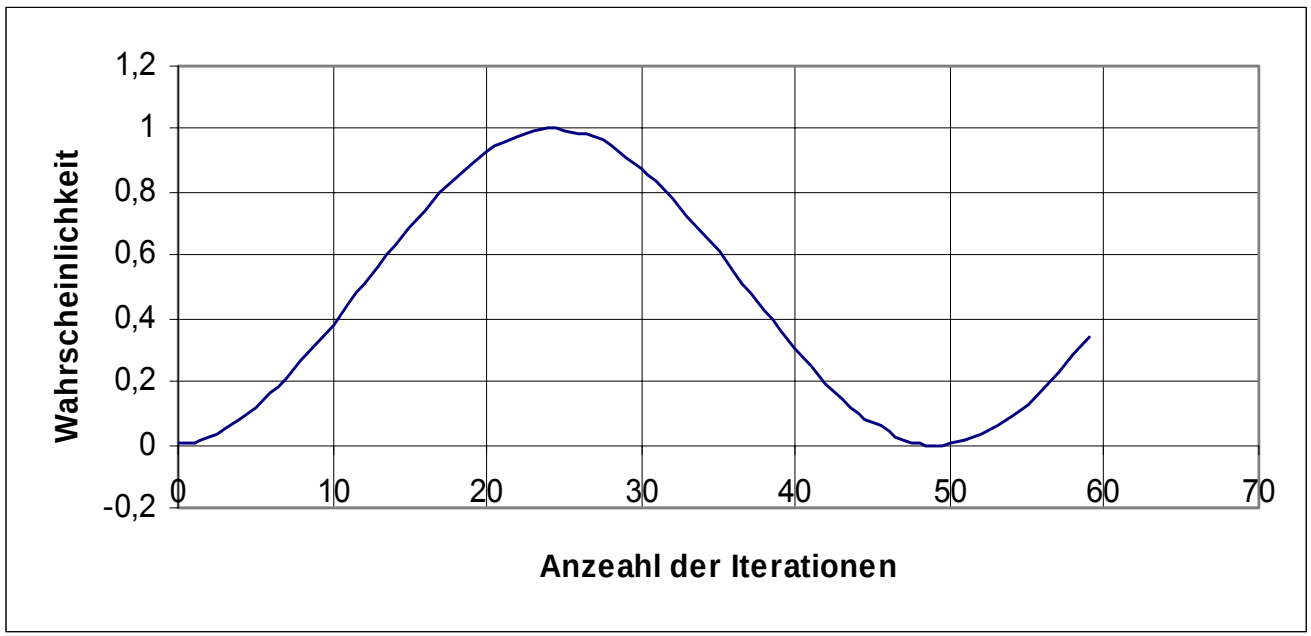
Geometrische Veranschaulichung:

Beispiel für N=1000, M=1:

$$G^{\otimes k}\left|\psi\right\rangle = \cos(\frac{2k+1}{2}\theta)\left|\alpha\right\rangle + \sin(\frac{2k+1}{2}\theta)\left|\beta\right\rangle$$

• Die Wahrscheinlichkeit, die Lösung nach k-Iterationen zu finden ist:

$$f(k) = \sin^2(\frac{2k+1}{2}\theta)$$



Geschwindigkeit / Komplexität:

- Die Komplexität beschreibt den Aufwand an Zeit und Hardware, den ein Algorithmus für seine Ausführung benötigt.
- Um mit Sicherheit (Wahrscheinlichkeit gleich Eins) eine Lösung zu finden, muss: $$\sin(\frac{2k+1}{2}\theta) = 1$$

Wobei K die Anzahl der Iterationen (die Komplexität des Algorithmus) ist. Dann folgt:

$$\frac{2k+1}{2}\theta = \frac{\pi}{2}$$

$$k = \frac{\pi}{2\theta} - \frac{1}{2} \leq \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

$$k = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rfloor$$

$$k = O\left(\sqrt{N}\right)$$

Zusammenfassung:

• Der Grover-Algorithmus ist optimal und hat im Vergleich zum Deutsch-Algorithmus praktische Anwendungen.

• Der Grover-Algorithmus liefert eine quadratische Verbesserung im Vergleich zum klassischen Algorithmus.

• Anwendungen: Kollisionsproblem, Zählen der Lösungen, Minimum finden…

• Offene Frage: Werden regelmäßig neue Quantenalgorithmen gefunden, die effizienter als jeder klassische sind?

Literatur:

- Quantum computing; Mika Hirvesalo; 2001.
- Lecture Notes on Quantum Computation; D. Mermin.
- Classical and quantum information; A.Galindo & M.A.Martin-Delgado.
- weitere Webseiten.

Danke für Ihre Aufmerksamkeit