WiSe '23/'24, hhu
K. Halupczok

K12: Grovers Algorithmus am QC

Stichworte: Such-Problem, Grovers Algorithmus am QC, geom. Erklärung

12.1. **Einleitung:** Neben den Algorithmen von Shor sind weitere QC-Algorithmen bekannt geworden, die klassischen überlegen sind. Ein besonders bekannter ist Grovers Algorithmus für das Suchproblem, das wir hier vorstellen.

12.2. **Das Such-Problem:** Gegeben sei eine Funktion $f: S \to \{0,1\}$, wo S eine Menge sei. Es soll nach bestimmten Elementen von S gesucht werden; es sei $f(x)=0$, falls x ein gültiges Suchergebnis ist, und $f(x)=0$ sonst. Dafür sei insbesondere $S := \{0,1\}^n = \{(x_1,\dots,x_n);\ \text{die } x_i \in \{0,1\} \text{ für alle } i=1,\dots,n\}$; dabei ist n die Bitgröße des Suchraums. Das Such-Problem ist nun die Suche nach einem $x_0 \in S$ mit $f(x_0)=1$.

12.3. **Bem.:** Schlimmstenfalls muss f insg. 2^n-1 mal ausgewertet werden, um alle Möglichkeiten durchzugehen: Nach 2^n-1 vielen erfolglosen Suchen ist das letzte El. das gesuchte. Grovers Algorithmus schafft die Suche mit nur $\approx \sqrt{2^n} = 2^{n/2}$ vielen Auswertungen.

12.4. **Def.:** Die Hadamard-Transformation sei $H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, welche auf ein Qubit angewendet werden kann gemäß $H\cdot\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$, $H\cdot\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$.

In „Dirac-Notation": $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Auf ein Register mit n Qubits angewandt: $H^{\otimes}|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle$

12.5. **Def.:** Für eine Funktion $f: \{0,1\}^n \to \{0,1\}^m$ sei $O = O_f$ definiert durch $O|x\rangle = (-1)^{f(x)}|x\rangle$. Die Transformation O_f heißt Phasen-Orakel.

12.6. <u>Beschreibung von Grovers Algorithmus:</u> Sei $N = 2^n$ die Anzahl aller Elemente von S. Seien die Elemente von S indiziert mit den ganzen Zahlen $0, \dots, N-1$. Weiter gebe es M viele verschiedene $x \in S$ mit $f(x) = 1$. ($f: \{0,1\}^n \to \{0,1\}^m$)

<u>1. Schritt:</u> Initialisiere ein Register aus n vielen Qubits auf $|0\rangle$.

<u>2. Schritt:</u> Setze das Register durch Anwenden von H auf

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \qquad \text{(gleichmäßige Überlagerung aller Zustände).}$$

<u>3. Schritt:</u> Wende N_0-mal die folgenden Operationen auf das Register an:

<u>(3a)</u>: Das Phasen-Orakel O_f, welches einen Faktor -1 an die Suchobjekte hinzufügt.

<u>(3b)</u>: Wende H auf jedes Qubit im Register an.

<u>(3c)</u>: Wende einen Phasenshift von -1 auf jeden Berechnungsgrundzustand an, außer auf $|0\rangle$.
Dies kann durch $-O_0$ dargestellt werden, wo O_0 das Hinzufügen des Faktors -1 an $|0\rangle$ bedeutet.

<u>(3d)</u>: Wende H auf jedes Qubit im Register an.

<u>4. Schritt:</u> Führe eine Messung am Register durch, um mit hoher W. ein x mit $f(x) = 1$ zu erhalten.

<u>5. Schritt</u>: Checke, ob x eine gültige Lösung ist; falls nicht, beginne von vorne.

Dabei ist $N_0 = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2} \right\rfloor$ die optimale Anzahl Iterationen, die die Erfolgswahrscheinlichkeit maximiert.

12.7. <u>Bem.:</u>
- Die Schritte (3b), (3c), (3d) heißen oft "Grovers Diffusionsoperator".
- Die unitäre Gesamtoperation am Register ist $\left(-H^{\otimes n} O_0 H^{\otimes n} O_f\right)^{N_0} \cdot H^{\otimes n}$.

12.8. <u>Durchführung am Bsp.:</u> Sei $n = 2$, und das zu suchende El. sei $|01\rangle$.

1. $|00\rangle$
2. H anwenden: $\frac{1}{\sqrt{4}} \sum_{i \in \{0,1\}^2} |i\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$.

3a. O_f anwenden: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$.

3b. H anwenden auf alle Zustände: $\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$.

⌈Denn haben $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, also ist

$H|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, $-H|01\rangle = -\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

$H|10\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$, $H|11\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. ⌋

3c. Den Kond. Shift auf alle Zustände außer $|00\rangle$ anwenden:

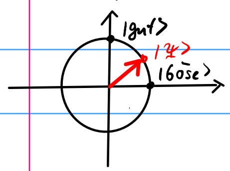
$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

3d. Zuletzt H anwenden auf alle Zustände: $|01\rangle$

(Haben 1 Iteration benötigt: Für $N=4$ ist $N_0 = 1$.)

12.9. Geometrische Erklärung: Sei $|böse\rangle$ die Überlagerung aller Zustände, die keine Lösung des Suchproblems sind, $|böse\rangle = \frac{1}{\sqrt{N-M}} \sum_{x, f(x)=0} |x\rangle$

entsprechend $|gut\rangle = \frac{1}{\sqrt{M}} \sum_{x, f(x)=1} |x\rangle$. Diese Zustände sind orthogonal.



Sei $|\psi\rangle$ ein bel. Zustand in dieser Ebene, d.h. $|\psi\rangle = \alpha|gut\rangle + \beta|böse\rangle$, $\alpha, \beta \in \mathbb{R}$.

Sei R der Spiegelungsoperator, der durch $R_{|\psi\rangle} = 2|\psi\rangle\langle\psi| - Id$ definiert ist und an $|\psi\rangle$ als Spiegelachse spiegelt.

⌈ Betr. ONB $|\psi\rangle, |\psi^\perp\rangle$, mit orth. Komplement $|\psi^\perp\rangle$ von $|\psi\rangle$.

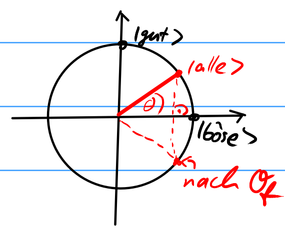
Können $|\xi\rangle = \mu|\psi\rangle + \nu|\psi^\perp\rangle$ schreiben. Die Anw. von $R_{|\psi\rangle}$ auf $|\xi\rangle$ liefert

$$\begin{aligned} R_{|\psi\rangle}|\xi\rangle &= \mu(2|\psi\rangle\langle\psi| - Id)|\psi\rangle - \nu(2|\psi\rangle\langle\psi| - Id)|\psi^\perp\rangle \\ &= 2\mu|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{=\||\psi\rangle\|^2=1} - \mu|\psi\rangle - 2\nu|\psi\rangle\underbrace{\langle\psi|\psi^\perp\rangle}_{=0} - \nu|\psi^\perp\rangle \\ &= \mu|\psi\rangle \underbrace{-}_{\text{Faktor } -1} \nu|\psi^\perp\rangle, \end{aligned}$$

ist also die fragliche Spiegelung. ⌋

Grovers Algo startet nach der ersten H-Anwendung mit $|alle\rangle = \sqrt{\frac{M}{N}}|gut\rangle + \sqrt{\frac{N-M}{N}}|böse\rangle$

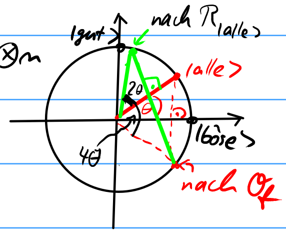
- Nun ist O_f genau die Spiegelung $O_f = R_{|böse\rangle}$, da der Faktor -1 zu guten $|x\rangle$ hinzukommt.



Analog ist O_0 gerade $O_0 = R_{|0\rangle} = -2|0\rangle\langle 0| + Id$.

• Somit ist $-H^{\otimes n} O_0 H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - H^{\otimes n}\, Id\, H^{\otimes n}$

$$\underset{H^2 = Id}{=} 2|alle\rangle\langle alle| - Id = R_{|alle\rangle}.$$



Also ist jede Grover-Iteration die Hintereinanderausführung von $R_{|böse\rangle}$ und $R_{|alle\rangle}$, insgesamt eine Drehung um einen Phasenwinkel 2θ, wo θ der zwischen $|alle\rangle$ und $|böse\rangle$ ist.

Es ist $\cos(\theta) \underset{\text{Cosinus-Satz}}{=} \langle alle|böse\rangle = \left(\sqrt{\frac{M}{N}}\langle gut| + \sqrt{\frac{N-M}{N}}\langle böse|\right)|böse\rangle = \sqrt{\frac{N-M}{M}}$.

Nun ist der Winkel zwischen $|gut\rangle$ und dem Register nach k Grover-Iterationen gleich

$$\sigma(k) := \frac{\pi}{2} - \theta - k\cdot 2\theta = \frac{\pi}{2} - (2k+1)\theta,$$

die W., $|gut\rangle$ zu erhalten ist $\cos^2(\sigma(k)) = \sin^2\left((2k+1)\arccos\sqrt{\frac{N-M}{M}}\right)$.

Da $\sin^2(t)$ das 1. Maximum bei $x = \frac{\pi}{2}$ annimmt, ist $\frac{\pi}{2} = (2k_{optimal} + 1)\arccos\left(\sqrt{\frac{N-M}{M}}\right)$,

also $k_{optimal} = \frac{\pi}{4\arccos(\sqrt{1-M/N})} - \frac{1}{2} \underset{\arccos\sqrt{1-x} = \sqrt{x} + O(x^{3/2})}{=} \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2} - O\left(\sqrt{\frac{M}{N}}\right)$,

so dass $N_0 = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2} \right\rfloor$ optimal gewählt ist.

12.10. Laufzeitanalyse: Insg. werden $O\left(\sqrt{\frac{N}{M}}\right)$ viele Suchanfragen mit dem Orakel O_f benötigt. Mit einer passenden Implementation von O_f mit Laufzeit $O(\log(N))$ erhält man eine Gesamtlaufzeit von $O\left(\sqrt{\frac{N}{M}}\log(N)\right)$.