Hauptseminar „Quantenlogik“, LMU München
Grovers Algorithmus
Andrea Stubbe, 19.08.2005

1 Einleitung

Grovers Algorithmus findet aus einer ungeordneten Menge von Elementen dasjenige heraus, das eine bestimmte Bedingung erfllt. Die klassische Methode wäre es, jedes der Elemente anzuschauen und zu prüfen, ob es das gesuchte ist. Bei N Elementen ergibt sich also eine durchschnittliche Komplexität von $O(N/2)$, im schlechtesten Fall liegt sie sogar bei $O(N)$. Quantenmechanische Systeme können durch die *Superposition* (Überlagerung) mehrerer Zustände meherere Elemente gleichzeitig überprüfen. Dadurch benötigt Grovers Suchalgorithmus nur $O(\sqrt{N})$ Schritte.

2 Der Algorithmus

Der Algorithmus besteht aus drei grundsätzlichen Schritten: Initialisierung der Eingangsdaten, Identifizieren des gesuchten Elements und Erhöhen dessen Amplitude.

2.1 Initialisierung

Grovers Algorithmus hat zwei Register, eines mit n Qubits und ein Hilfsregister mit einem Qubit. Als erstes muss eine Superposition der $N = 2^n$ Basisizustände $\{|0\rangle, ..., |2^n - 1\rangle\}$ erzeugt werden, in der alle Amplituden gleichgroß sind. Dies wird erreicht, indem man das erste Register mit $|0, ...0\rangle$ belegt und die Hadamrd-Transformation $H^{\otimes n}$ darauf anwendet - denn das n-fache Tensorprodukt der Hadamard-Transformation angewandt auf das n-fache Produkt des 0-ten Basisvektors liefert eben dieses gewünschte Ergebnis:

$$\begin{aligned} |\phi\rangle &= H^{\otimes n}|0, ..., 0\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \end{aligned}$$

Das Hilfsregister wird zu Beginn mit $|1\rangle$ belegt, und ebenfalls durch ein Hadamard-Gatter in den Zustand $|-\rangle$ gebracht:

$$|-\rangle = H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad (1)$$

2.2 Oracle

Um das gesuchte Element zu identifizieren, wird ein unitärer Operator U_f (*Oracle*) verwendet, der auf der Testfunktion

$$f(i) = \begin{cases} 1 \text{ falls i das gesuchte Element } i_0 \text{ ist} \\ 0 \text{ sonst.} \end{cases}$$

des klassischen Algorithmus beruht, und für den gilt:

$$U_f(|i\rangle|j\rangle) = |i\rangle|j \oplus f(i)\rangle$$

Belegt man die Eingänge mit einem beliebigen $|i\rangle$ und $|-\rangle$ ergibt sich:

$$\begin{aligned} U_f(|i\rangle, |-\rangle) &= \tfrac{1}{\sqrt{2}}(U_f(|i\rangle|0\rangle) - U_f(|i\rangle|1\rangle)) \qquad \text{(nach 1)} \\ &= \tfrac{1}{\sqrt{2}}(|i\rangle|f(i)\rangle - |i\rangle|1 \oplus f(i)\rangle) \end{aligned}$$

Durch Unterscheidung der Fälle $i = i_0$ (a) und $i \neq i_0$ (b) und daher

$$\begin{array}{lll} (a) & f(i) = 1 & \text{bzw.} \quad 1 \oplus f(i) = 0 \\ (b) & f(i) = 0 & \text{bzw.} \quad 1 \oplus f(i) = 1 \end{array}$$

lässt sich dies weiter umformen zu

$$\begin{aligned} U_f(|i\rangle, |-\rangle) &= \tfrac{1}{\sqrt{2}}(-1)^{f(i)}(|i\rangle|0\rangle - |i\rangle|1\rangle) \\ &= (-1)^{f(i)}|i\rangle|-\rangle \qquad \text{(nach 1)} \end{aligned}$$

Wendet man U_f auf den Überlagerungszustand $|\phi\rangle|-\rangle$ an, ist das Ergebnis

$$\begin{aligned} |\phi_U\rangle|-\rangle &= U_f(|\phi\rangle|-\rangle) \\ &= \tfrac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_f(|i\rangle|-\rangle) \\ &= \tfrac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)}|i\rangle|-\rangle \end{aligned}$$

Wie man erkennen kann, wird $|\phi\rangle$ durch U_f nicht verändert, außer dass das Vorzeichen des gesuchten Elements umgedreht wird. Also

$$|\phi_U\rangle = |\phi\rangle - \tfrac{2}{\sqrt{N}}|i_o\rangle \tag{2}$$

Allerdings wird es dadurch noch nicht messbar, da das Quadrat der Amplitude das gleiche bleibt wie bei den anderen Elementen.

2.3 Erhöhung der Amplitude

Um das Ergebnis mit einer hohen Wahrscheinlichkeit zu messen, muss die Amplitude des gesuchten Elements gegenüber den anderen angehoben werden. Dies ist das übliche Vorgehen bei Quantenalgorithmen. Hier wird dies durch den unitären Operator G erledigt, der das Hilfsregister $|-\rangle$ unverändert lässt und das erste Register folgendermaßen ändert:

$$|\phi_G\rangle = (2|\phi\rangle\langle\phi| - I)|\phi_U\rangle$$

Da i_0 senkrecht auf allen anderen Basiszuständen steht, ergibt sich das Skalarprodukt aus i_0 und ϕ zu

$$\langle\phi|i_0\rangle = \tfrac{1}{\sqrt{N}}, \tag{3}$$

wobei $|\phi\rangle\langle\phi|$ der Projektor auf ϕ ist. ϕ_G lässt sich mit Hilfe von (2) umformen:

$$\begin{aligned} |\phi_G\rangle &= (2|\phi\rangle\langle\phi| - I)(|\phi\rangle - \tfrac{2}{\sqrt{N}}|i_o\rangle) \\ &= 2|\phi\rangle\langle\phi|\phi\rangle - I|\phi\rangle \quad - \quad \tfrac{2\cdot 2}{\sqrt{N}}|\phi\rangle\langle\phi|i_0\rangle + \tfrac{2}{\sqrt{N}}|i_0\rangle \end{aligned}$$

und mit (3) und $N = 2^n$ weiter zu

$$\begin{aligned} &= 2|\phi\rangle - |\phi\rangle \quad - \quad \tfrac{4}{N}|\phi\rangle + \tfrac{2}{\sqrt{N}}|i_0\rangle \\ &= (1 - \tfrac{4}{2^n})|\phi\rangle + \tfrac{2}{\sqrt{N}}|i_0\rangle \\ &= \frac{2^n - 2^2}{2^n}|\phi\rangle + \frac{2}{\sqrt{2^n}}|i_0\rangle \\ &= \frac{2^{n-2} - 1}{2^{n-2}}|\phi\rangle + \frac{2}{\sqrt{2^n}}|i_0\rangle \end{aligned}$$

Die Amplitude von $|\phi\rangle$ wird also verringert, die von i_0 angehoben.

3 Anzahl der Wiederholungen

Die Grover-Transformation (bestehend aus U und G) muss $O(\sqrt{N})$ mal angewendet werden, da der erreichte Amplitudenunterschied erstmal nur ziemlich klein ist. Die optimale Anzahl an Wiederholungen liegt bei

$$\begin{aligned} k &= round(\frac{\pi - \theta}{2\theta}) \\ k &\approx round(\tfrac{\pi}{4}\sqrt{N}), \end{aligned}$$

die Wahrscheinlichkeit, mit der das richtige Element gefunden wird, beträgt

$$\begin{aligned} p &= \sin^2\left(\frac{2k_0+1}{2}\theta\right) \qquad \text{, wobei} \\ \theta &= 2\arccos\sqrt{1-\tfrac{1}{N}} \end{aligned}$$

θ ist der Winkel, um den $|\phi\rangle$ durch Anwendung des G-Gatters im durch $|i_0\rangle$ und $|\phi\rangle$ aufgespannten Vektorraum in Richtung $|i_0\rangle$ gedreht wird. Nach k Wiederholungen liegt $|\phi_k\rangle$ am nähesten an $|i_0\rangle$ und wird deshalb mit der höchsten Wahrscheinlichkeit gemessen.