

Quanten Computing verstehen: Grovers Algorithmus

Sabrina Cielas,¹ Till Pilarczyk²

Abstract:

Keywords: Quantencomputer; Quantum Computing; Grovers-Algorithmen

1 Begriffserklärung (nur wenn Platz ist)

Der Text bezieht sich auf die Quelle... Kapitel 6.

Es Wird vorausgesetzt, das bekannt ist, was die folgende Begrifflichkeiten sind

- Superposition
- Amplitude
- Messen
- Quantenorakel
- Hadamar Gatter bzw Pauli-Gatter Lokalitätsprinzip

Falls wird noch Platz haben können wir diese begriffe noch erklären

2 Einleitung

Fragestellung Motivation Aufbau des Papers

3 Grovers-Algorithmus

Um den Algorithmus besser verstehen zu können, werden die Rahmenbedingungen formalisiert. Die Datenbank, besitzt N Elemente wobei $N = 2^n$ entspricht. Den Datensätzen

¹ Hochschule Düsseldorf, Gebäude 4, Münsterstraße 156, 40476 Düsseldorf, Deutschland sabrina.cielas@study.hs-duesseldorf.de

² Hochschule Düsseldorf, Gebäude 4, Münsterstraße 156, 40476 Düsseldorf, Deutschland till.pilarczyk@study.hs-duesseldorf.de

ordnen wir die Elemente $\{0, 1\}^n$ zu. Wenn $n = 2$ entspräche erhielt man die Elemente **00, 01, 10, 11**. Das gesuchte Elemente bezeichnen wir als \hat{x} . Die Datenbank wird als eine Funktion $f: \{0, 1\}^n \rightarrow \{0, 1\}$ mit folgender Eigenschaft umgesetzt:

$$f(x) = \begin{cases} 1 & \text{für } x = \hat{x} \\ 0 & \text{sonst} \end{cases}$$

Mithilfe dieser Funktion haben wir unser Quantenorakel. $U_f: |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$. Die Funktion f gibt nur ein zurück, wenn die Eingabe das gesuchte Element \hat{x} ist. Das Quantenorakel, negiert daher nur das Vorzeichen des gesuchten Elements.

3.1 Prinzip

Der Grover Algorithmus lässt sich in drei Schritte aufteilen.

1. **Superpositionen aufbauen**
im ersten Schritt werden alle Quantenbits in die Superposition gebracht.
2. **Amplitudenveränderung durchführen (Grover Iteration G)**
Der Zweite Schritt verändert die Amplituden der Elemente. Dabei wird die Amplitude des gesuchten Elementes erhöht und alle anderen verringert. Dieser Schritt wird auch (Grover Iteration G) genannt und abhängig von der Anzahl der Elementen öfters wiederholt. Wie oft die Grover Iteration ausgeführt werden muss, wird im Abschnitt 4.1.2 erläutert.
3. **Messen**
Im letzten Schritt werden die Quantenbits gemessen und man erhält mit einer hohen Wahrscheinlichkeit, das gesuchte Element \hat{x} .

3.1.1 Amplitudenveränderung

Die Amplitudenveränderung besteht aus zwei Schritten. Beim ersten Schritt handelt es sich um die Negation der Amplitude von \hat{x} . Im zweiten Schritt wird die negative Amplitude ausgenutzt um die Amplitude zu verstärken. Dies passiert in dem alle Amplituden am Mittelwert aller Amplituden gespiegelt werden.

Negieren der Amplitude

Um die Amplitude von \hat{x} zu negieren, wird ein Hilfsbit benötigt. Das Hilfsbit wird in den Zustand $H|1\rangle$ mithilfe eines Hadamar Gatters gebracht. Dadurch erhalten wird $|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Anschließend wird das Quantenorakel angewendet und damit das Vorzeichen der Amplitude des gesuchten Elementes negiert. Das Hilfsbit wird nun nicht mehr benötigt und kann in folgenden Berechnungen weggelassen werden. Dies lässt sich auch an folgender Abbildung erkennen. Dort ist Anwendung des Quantenorakel und

beispielhaft die Amplituden alle Elemente der Datenbank vor und nach der Anwendung des Quantenorakels zu sehen. Die negative Amplitude von \hat{x} hat keinen Einfluss auf das

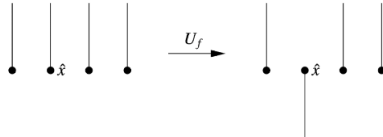
$$\begin{aligned}
 |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &\xrightarrow{U_f} |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\
 &= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
 \end{aligned}$$


Abb. 1: Amplitudenveränderung

Messen, um mit einer erhöhten Wahrscheinlichkeit das Element \hat{x} nach dem Messen zu erhalten benötigt man den Schritt Spiegeln am Mittelwert.

Spiegelung am Mittelwert

Um zu zeigen, dass die Spiegelung der Amplituden am Mittelwert den gewünschten Effekt hat, folgen nun einige Beispiel Rechnungen. Eine Spiegelung an einem Wert \mathbf{m} entspricht der Abbildung: $\alpha \rightarrow 2 \times \mathbf{m} - \alpha$.

Nimmt man an die Datenbank enthält vier Elemente ($\mathbf{n} = 2$) so entspricht - nach der Negation von \hat{x} - der Mittelwert $\mathbf{m} = \frac{1}{4} \times (\frac{1}{2} - \frac{1}{2} + \frac{1}{2} + \frac{1}{2}) = \frac{1}{4}$. Die Spiegelung von \hat{x} entspricht $-\frac{1}{2} \times \frac{1}{4} - (-\frac{1}{2}) = 1$. Damit ist die Amplitude des gesuchten Elements gleich eins. Würde man nun die Bits messen, erhält man mit einer Wahrscheinlichkeit von 100% das Element \hat{x} . Die Amplituden aller anderen Elemente entwickeln sich wie folgt: $\frac{1}{2} \times \frac{1}{4} - \frac{1}{2} = 0$

Wäre $\mathbf{n} = 3$, so würde die Amplitude von \hat{x} nach der ersten Grover Iteration $\frac{5}{5\sqrt{8}}$ und alle anderen Amplituden $\frac{1}{2\sqrt{8}}$ betragen. Nach einer Spiegelung am Mittelwert ist die Amplituden von \hat{x} wieder positiv, bevor ein erneutes Spiegeln möglich ist um die Amplituden weiter zu verstärken oder zu verringern, muss zuerst erneut das Quantenorakel angewandt werden. Ein erneutes Spiegeln, nach der Negation, der Amplituden würde diese wie folgt verändern. Das gesuchte Element \hat{x} hätte eine Amplitude von **0,973**, alle anderen Elemente eine von **-0,088**. Würde nun gemessen werden erhielte man mit einer Wahrscheinlichkeit von 93 % das gesuchte Element.

Ein erneutes Spiegeln würde die Amplituden des gesuchten Elementes im Gegensatz zu Erwartung wieder verringern und alle anderen erhöhen, daher ist es besonders wichtig, dass nicht zu viele Grover Iterationen ausgeführt werden. Wie die Genaue Anzahl an Iterationen jedoch berechnet werden kann, folgt im Abschnitt 4.1.2 **SOUFFLE?**

3.1.2 Graphische Darstellung des Grover Algorithmus

Der Grover Algorithmus sieht nach den bisherigen Erklärungen wie folgt aus. Alle Bits



Abb. 2: Graphische Darstellung des Grover Algorithmus
Quelle EIGENS ERSTELLEN!!!!

werden mithilfe der Hadamard Gatter in Superpositionen gebracht. Alles danach bis zum Messen Symbol am Ende ist die Grover Iteration. Der Äußere Kasten steht für das mehrfache Wiederholen dieser Iterationen. V_f steht für das Quantenorakel, jedoch wird hier das Hilfsbit nicht mit eingezeichnet. Anschließend folgt die Spiegelung am Mittelwert, wie diese genau mithilfe von Gattern umgesetzt wird folgt im nächsten Abschnitt 3.2. Nach dem ausführen der Grover Iterationen werden die Bits gemessen.

3.2 Realisierung der Spiegelung am Mittelwert

Die Abbildung $\alpha \rightarrow 2 \times \mathbf{m} - \alpha$ lässt sich mithilfe einer Matrixberechnung umsetzen.

$$\mathbf{D}_N \times \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{N-1} \end{pmatrix}^T, \text{ mit } \mathbf{D}_N = \begin{pmatrix} -1 + \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & -1 + \frac{2}{N} & \dots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \dots & -1 + \frac{2}{N} \end{pmatrix}$$

3.2.1 Beispielrechnung

Sei $N = 4$ so ergibt sich folgende Rechnung:

$$\mathbf{D}_4 \times \begin{pmatrix} 0,5 & -0,5 & 0,5 & 0,5 \end{pmatrix}^T.$$

$$\begin{pmatrix} -0,5 & 0,5 & 0,5 & 0,5 \\ 0,5 & -0,5 & 0,5 & 0,5 \\ 0,5 & 0,5 & -0,5 & 0,5 \\ 0,5 & 0,5 & 0,5 & -0,5 \end{pmatrix} \times \begin{pmatrix} 0,5 \\ -0,5 \\ 0,5 \\ 0,5 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Dieses Ergebnis gleicht sich mit dem Ergebnis aus Abschnitt 3.1.1, in dem wir ebenfalls alle Elemente einer Datenbank mit $N = 4$ Elementen an dem Mittelwert der Amplituden gespiegelt haben. Folgende Abbildung zeigt ebenfalls nochmal wie sich die Amplituden verändert haben. Wenn eine $N \times N$ Matrix verwendet wird, dann verstößt dies gegen das

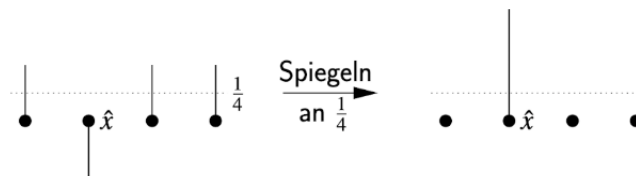


Abb. 3: Spiegelung am Mittelwert
Quelle: HOEMEISTER SEITE

Lokalitätsprinzip. Daher muss die \mathbf{D}_n Matrix in verschiedene unitäre Matrizen zerlegt werden. \mathbf{D}_n kann in ein Produkt aus drei unitäre Matrizen zerlegt werden.

$$\mathbf{D}_n = -\mathbf{H}_n \times \mathbf{R}_N \times \mathbf{H}_n, \text{ mit } \mathbf{R} = \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

3.2.2 Beispielrechnung

Um zu zeigen, dass die Matrix \mathbf{D}_N wie oben als Produkt dreier Matrizen zerlegt werden kann, folgt ein Beispiel mit \mathbf{D}_4 . Das Ergebnis der Berechnung ist wie in der beschrifteten Rechnung 4) zu sehen gleich mit der zu erwarteten Matrix \mathbf{D}_4 . Der Beweis, dass dies auch für beliebige N zutrifft befindet sich in dem Buch vom Hoemeister auf der Seite 309 QUELLE.

3.2.3 Matrix \mathbf{R} als lokale Transformation

Es wurde gezeigt, dass die Matrix \mathbf{D}_N in ein Produkt aus Matrizen zerlegt werden kann. Das die Hadamar Matrizen mit Hilfe eines Gattern als lokale Transformation umgesetzt werden können ist bekannt. Dies muss jedoch auch noch für \mathbf{R}_N gezeigt werden.

$$\begin{array}{ccc}
\frac{1}{2} \begin{pmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{pmatrix} & \times \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & = \frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \\
-H_2 & R_4 & \text{Zwischenergebnis} \\
\\
\frac{1}{2} \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} & \times \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} & = \frac{1}{4} \begin{pmatrix} -2 & 2 & 2 & 2 \\ 2 & -2 & 2 & 2 \\ 2 & 2 & -2 & 2 \\ 2 & 2 & 2 & -2 \end{pmatrix} \\
\text{Zwischenergebnis} & H_2 & D_4
\end{array}$$

Abb. 4: Beispielzerlegung von D_4
 Quelle: eigene Darstellung

Um ein Gatter zu entwickeln zu können, welches die Transformation R_N umsetzt, muss sich angeschaut werden wie sich R_N bei einer Multiplikation von Matrizen auswirkt. Alle Werte einer Matrix die mit R_N multipliziert wird bleiben gleich. Lediglich die erste Zeile oder Spalte wird negiert. Dies ist davon abhängig, ob die Matrix R_N auf der Linken oder Rechten Seite der Multiplikation ist. In ersten Zeile der Abbildung 4 ist die Negation der ersten Spalte zu sehen.

Multipliziert man R_N mit Amplituden, bedeutet dies, dass lediglich die Amplitude des ersten Elementes ($|0\dots 0\rangle$) negiert wird. Falls R_4 wäre, dann sähe das Gatter wie in Abbildung 5 aus.

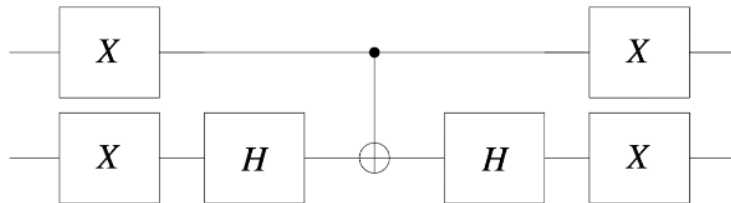


Abb. 5: R_4 Realisierung
 Quelle: HOEMEISTER SEITE

Es folgt eine weitere Beispielrechnung, um zu verdeutlichen, dass dieses Gatter die Transformation R_4 ausführt.

3.2.4 Beispielrechnung

ABBILDUNG In den Abbildungen () werden die Werte der QBits $|00\rangle$ und wie diese sich durch die einzelnen Gatter verändern dargestellt. Die Pauli X Gatter invertieren den Wert eines QBits. Aus $|0\rangle$ wird $|1\rangle$ und andersrum. Das erste Bit wird bis zum letzten Pauli-X Gatter nicht mehr verändert. Es wird ausschließlich genutzt um zu schauen, ob das CNOT aktiviert wird. Das zweite QBit wird durch das erste Hadamar Gatter, in folgende Superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Da das erste QBit den Wert $|1\rangle$ hat wird das zweite QBit durch das CNOT negiert - $-\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Anschließend durch läuft das zweite Bit wieder ein Hadamar Gatter, das QBit hat anschließend folgenden Wert: $-|1\rangle$. Zum Schluss werden beide Bits ($|1\rangle$ und $-|1\rangle$) durch die Pauli-X Gatter invertiert und wir erhalten das gewünschte Ergebnis von $-|00\rangle$.

ABBILDUNG

Die Abbildung () zeigt die QBits $|01\rangle$ und wie diese von den Gattern verändert werden. Die ersten Pauli-X Gatter invertieren abermals die QBits, diese haben nun den Wert $|10\rangle$. Das erste QBit wird bis auf von dem letzten Pauli-X Gatter nicht verändert und nur zur Aktivierung der Operation CNOT zuhulfe genommen. Das zweite QBit wird durch das Hadamar Gatter in die Superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gebracht. Diese verändert sich auch nicht durch die CNOT Operation. Nach der CNOT Operation wird das QBit durch das zweite Hadamar Gatter wieder in den Basiszustand $|0\rangle$ gebracht. Zuletzt durchlaufen die beiden QBits ein Pauli-X Gatter welches die QBits von den Basiszustände $|10\rangle$ in den erwarteten Zustand $|01\rangle$ überführt. Die QBits haben nach dem durchlaufen des Gatters die selben Zustände wie vorher.

Bei den QBits $|10\rangle$ und $|11\rangle$, wird die CNOT Operation nicht ausgeführt, da das erste QBit in den Basiszustand $|0\rangle$ überführt werden. Die QBits werden durch die doppelte Ausführung der Gatter ebenfalls nicht verändert.

Daran kann gesehen werden, dass die Gatter die gewünschte Operation **R₄** ausführen.

3.3 Graphische Darstellung des Grover Algorithmus

In der Abbildung() ist wie in der Abbildung() der Grover Algorithmus nochmals Graphisch dargestellt. Dieses mal enthält die Abbildung alle verschiedenen Gatter, die die QBits durchlaufen.

4 Bestimmung der Anzahl an Grover-Iterationen

Nach dem der Genaue Ablauf des Algorithmus erklärt wurde, bleibt noch die Frage: Wie oft muss die Grover Iteration durchgeführt werden, um mit einer hohen Wahrscheinlichkeit das gesuchte Element \hat{x} zu messen?

4.1 Geometrische Veranschaulichung

Mithilfe der Geometrie kann die Anzahl der Iterationen bestimmt werden. Das Schritt weise erhöhen der Amplitude des gesuchten Elements kann auf der Blochs Kugel als Rotation aufgefasst werden. In der Geometrie entspricht die Spiegelung von zwei Ebenen um eine Drehung, um den Winkel $2 \times \beta$ wobei β der Winkel zwischen den Ebenen ist. Dies ist in der Abbildung 6 verdeutlicht. Wie der Name schon sagt, handelt sich sich bei der Spiegelung am

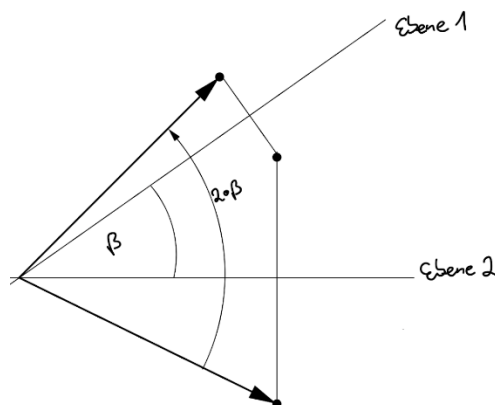


Abb. 6: R_4 Spiegelung an zwei Ebenen
Quelle: eigen Darstellung, angelehnt an HOEMEISTER

Mittelwert um eine Spiegelung. Die zweite Spiegelung ist das negieren von dem gesuchten Element \hat{x} . Die Formel zu Spiegelung an einem Wert \mathbf{m} lautet: $\alpha \rightarrow 2 \times \mathbf{m} - \alpha$. Ist $\mathbf{m} = \mathbf{0}$ erhalten wir $\alpha \rightarrow -\alpha$. Dies zeigt, dass die Negation eines Elementes eine Spiegelung an dem Wert $\mathbf{0}$ ist.

Der Winkel lautet $\sin(\beta) = \text{Skalarprodukt aus der allgemeinen Superposition und dem gesuchten Element } \hat{x}$. Dies ergibt $\sin(\beta) = \frac{1}{\sqrt{N}}$. Daran lässt sich erkennen, dass die Anzahl der Iterationen abhängig von der Anzahl der Datenbankelemente ist und nicht von \hat{x} , welches zur Folge hätte, dass wir für jedes gesuchte Element die Suche anpassen müssten.

4.1.1 Beispielrechnung

Nimmt man an das $N = 4$, dann folgt daraus, dass $\sin(\beta) = \frac{1}{\sqrt{4}}$ ist. Nach Beta aufgelöst ergibt sich $\beta = \frac{\pi}{6}$.

Wird nun eine Grover Iteration durchgeführt, ändert sich der Winkel wie folgt: $\beta = \frac{\pi}{6} + 2 \times \frac{\pi}{6} = \frac{\pi}{2}$. Wird nun $\sin(\frac{\pi}{2})$ ausgerechnet, erhalten wir **1**. Dies bedeutet, dass wir mit einer Drehung das gesuchte Element erreicht haben. Wird nun gemessen erhalten wir mit einer Wahrscheinlichkeit von 100 % das gesuchte Element. Dies wird auch wie im Abschnitt 3.1.1 beschrieben erwartet.

4.1.2 Anzahl an Grover Iterationen

Durch die rechnung konnte gezeigt werden, dass der Startwinkel $\frac{1}{\sqrt{N}}$ beträgt und der Winkel nach T Grover Iterationen den Wert $(2 \times T + 1) \times \frac{1}{\sqrt{N}}$ hat. Falls für $T = \frac{\pi}{4} \times \sqrt{N}$ gewählt wird, wird immer sehr nah an zu dem gesuchten Element rotiert.

In der Praktischen Umsetzung, muss T immer abgerundet werden, da nur eine gerade Zahl an Iterationen durchgeführt werden kann. Wird T aufgerundet, werden zu viele Grover-Iterationen durchgeführt und es wird sich vom gesuchten Element wieder entfernt.

Dadurch dass die Anzahl der Grover Iterationen $\frac{\pi}{4} \times \sqrt{N}$ beträgt und in jeder Iteration einmal das Quantenorakel aufgerufen wird, beträgt die Laufzeit $O(\sqrt{N})$

5 Varianten der Quantensuche

was für Varianten der Quantensuche gibt es ?

6 Anwendungen des Grovers Algorithmus

Wofür kann man den Algorithmus alles verwenden ?

7 Folgen für die Fähigkeit von Quantencomputern

Hier kommen die Folgen für die Fähigkeit von Quantencomputern hin

Literatur

- [AB00] Abel, K.; Bibel, U.: Formatierungsrichtlinien für Tagungsbände. Format-Verlag, Bonn, 2000.

- [ABC01] Abraham, N.; Bibel, U.; Corleone, P.: Formatting Contributions for Proceedings. In (Glück, H. I., Hrsg.): Proc. 7th Int. Conf. on Formatting of Workshop-Proceedings. Noah & Sons, San Francisco, S. 46–53, 2001.
- [An14] Anteil an Frauen in der Informatik, Statistics Worldwide, 2014.
- [Az09] Azubi, L. et al.: Die Fußnote in LNI-Bänden. In (Glück, H. I., Hrsg.): Formatierung 2009. LNI 999, Format-Verlag, Bonn, S. 135–162, 2009.
- [Ez10] Ezgarani, O.: The Magic Format – Your Way to Pretty Books. Noah & Sons, 2010.
- [GI19] Gesellschaft für Informatik e. V., 2019, URL: <http://www.gi.de>, Stand: 21.03.2019.
- [GI09] Glück, H. I.: Formatierung leicht gemacht. Formatierungsjournal 11/09, S. 23–27, 2009.
- [Wa14a] Wasser, K.; Feuer, H.; Erde, R.; Licht, H.: Essenzen der Informatik. Verlag Formvoll, 2014.
- [Wa14b] Wasser, K.; Feuer, H.; Erde, R.; Licht, H.: Ganz neue Essenzen der Informatik im selben Jahr. Format-Verlag, 2014.