Der Suchalgorithmus von Grover

Seminar: Quantenrechner
Dozenten: Prof. Johannes Köbler und Olaf Beyersdorff
Referent: Gregor Pickert

Das Problem

Will man z.B. in einem Telefonbuch mit 1.000.000 Einträgen eine bestimmte Telefonnummer finden, muss man so lange einen Eintrag nach dem anderen durchsehen, bis man den Richtigen findet. Im Mittel braucht man, um einen bestimmten Eintrag in einer unsortierten n-lange Liste zu finden, $\frac{n}{2}$ Versuche, beim Telefonbuch z.B. 500.000. 1994 wurde von Bennett, Bernstein, Brassard und Vazirani bewiesen, dass jedes Verfahren $\Omega\left(\sqrt{n}\right)$ Schritte benötigt, um ein Element aus einem unstrukturierten Raum der Größe n zu finden. Lov Grover, ein Forscher der Bell Labs, hat auf der Tagung der „Association for Computing Machinery´s“ 1996 seinen neuen Algorithmus für die Suche in Datenbanken vorgestellt. Mit der verbesserten Abfrage wird es möglich, die Suche in einer Datenbank mit einer Million Einträge von bisher 500.000 Schritten auf weniger als 1.000 Schritte zu reduzieren. Mit seinem Quantenalgorithmus benötigt man im Schnitt nur $O(\sqrt{n})$ Schritte.

Dies ist möglich, indem durch die sog. "Grover-Iteration" im Quantenregister die Wahrscheinlichkeit für das richtige Ergebnis erhöht wird, die für die falschen aber verringert.

Man kann sich natürlich an dieser Stelle keine Gedanken über die Implementation einer solchen Datenbank machen, die eine Quantenanfragen mit Superpositionen beantworten könnte, sondern sollte das Problem abstrakter, dafür aber formal beschreiben.
Gegeben sei eine Funktion

$f: \{0,1\}^n \rightarrow \{0,1\}$. Zu bestimmen ist ein Element $x \in \{0,1\}^n$ mit $f(x) = 1$.

Die Funktion f stellt also ein Prädikat über dem Suchraum $\{0,1\}^n$, der $N = 2^n$ Elemente umfasst, dar. Für unsere Betrachtungen bezeichnen wir ferner die Anzahl der Lösungen, also derjenigen x, für die $f(x) = 1$ gilt, mit t. Damit ist

$t = |\{x \in \{0,1\}^n | f(x) = 1\}|$.

Mit einem *deterministischen Ansatz* müsste im worst case N-1 mal angefragt werden, um den Wert für a zu erhalten. Mit probabilistischen Mitteln liegt die erwartete Anzahl von Tests genau in der Mitte, also bei $\frac{N}{2}$. Die Behauptung ist nun, dass dieses Problem mit einem Quantenschaltkreis mit der Komplexität $O\sqrt{N}$ gelöst werden kann, d.h. eine Verbesserung durch die Halbierung des Exponenten erreicht wird.

Für die Lösung des Problems steht indes keinerlei weitere Information zur Verfügung, man müssen f also gewissermaßen als Blackbox betrachten.

Der Algorithmus als Quantenschaltkreis

Zur Lösung des Problems dient nun folgender Quantenschaltkreis:

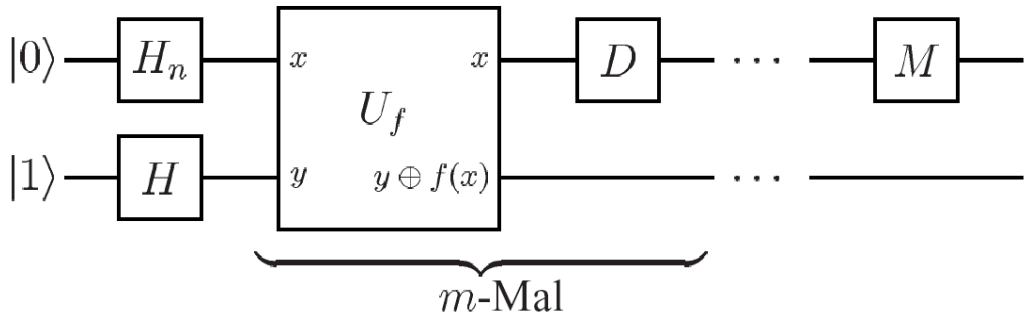


Abbildung 1: Der Quantenschaltkreis

Verwendete Operatoren

notwendige Voraussetzung sind:

- Zustände eines Quantensystems könne durch Vektoren der Länge 1 in einem unitären Raum beschrieben werden.
- Die mathematische Beschreibung eines System aus zwei Teilsystemen ist das Tensorprodukt ($\otimes$)der Teilvektoren
- Ein Qubit wird durch einen normierten Vektor des Raums $\mathbb{C}^2$ beschrieben
- $|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ und $|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ bilden die Standartbasis
- Wir interpretieren einen beliebigen Zustand $\alpha|0\rangle + \beta|1\rangle$, mit $|\alpha|^2 + |\beta|^2 = 1$ wegen der Normierung, als Superposition der klassischen Zustände 0 und 1 und nennen α bzw. β jeweils die **Amplituden** dieser Zustände
- Wir bezeichnen die Menge der Lösungen (und auch die Menge der „Lösungsbasisvektoren") mit $\mathrm{L} = \{x | f(x) = 1\}$ und die der Nichtlösungen mit $\overline{\mathrm{L}} = \{x | f(x) = 0\} = \{0,1\}^n \setminus \mathrm{L}$

Die Walsh-Hadamard-Transformation

Der Operator wird durch die Matrix

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

beschrieben. Durch Ausrechnen bekommt man folgende Eigenschaften dieser Operation:

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

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \text{ sowie}$$

$H \cdot H = I$, also $H = H^{-1}$

Damit lassen sich also aus den Standardzuständen (Basis) gleich wahrscheinliche Superpositionen und umgekehrt herstellen. Wendet man diese Transformation auf jedes Qubit eines Registers der Breite n an, so erhält man eine Transformation, die wir im Folgenden mit H_n bezeichnen.

Es gilt dann für Anwendung auf einen Basisvektor $|x\rangle$

$$\mathrm{H_n}\,|\mathrm{x}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{2^n-1}(-1)^{x\odot i}\,|i\rangle,$$

wobei $\mathrm{x}\odot\mathrm{i} = \sum_{\mathrm{j}=1}^{\mathrm{n}} \mathrm{x_j i_j} \bmod 2$ das innere Produkt für Binärdarstellungen $x_n x_{n-1} \ldots x_1$ von x und $i_n \ldots i_1$ von i darstellt. Insbesondere ist

$$\mathrm{H_n}\,|0^{\mathrm{n}}\rangle = \frac{1}{\sqrt{N}}\sum_{\mathrm{i}=0}^{2^{\mathrm{n}}-1}|\mathrm{i}\rangle,$$

Der Hadamard Operator erzeugt aus Basis-Zuständen deren Superpositionen. Dies entspricht z.B. bei Photonen einer Drehung der Polarisation um 45 Grad

Darstellung von Funktionen (U_f)

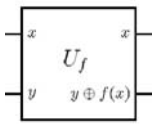
Erinnerung: Eine mit einem Quantenschaltkreis berechenbare
Funktion ist immer bijektiv also reversibel.

Zu einer Funktion $f: \{0,1\}^n \rightarrow \{0,1\}^m$ kann man immer eine zugehörige umkehrbare Funktion F : $\{0,1\}^{n+m} \rightarrow \{0,1\}^{n+m}$ wie folgt angeben:

$$F(x, y) = (x, y \oplus f(x))$$

Diese ist offensichtlich reversibel ($\oplus$ sei das bitweise exklusive Oder) und liefert für $y = 0$ in der zweiten Komponente genau das gewünschte Resultat *f(x)*. Wir bezeichnen mit $\boldsymbol{U_f}$ die unitäre Transformation, die diese Abbildung F realisiert:

$$|xy\rangle \xrightarrow{U_f} |x, y \oplus f(x)\rangle$$



Der Operator V_f

Da wir am Ende einer Quantenrechnung nur eine Messung zur Verfügung haben, müssen wir die Amplitude für die „guten" Basisvektoren innerhalb der Superposition vergrößern.
Dazu benötigen wir einen Mechanismus, der auf ein n-Qubit-Register angewendet, eine Unterscheidung zwischen den Amplituden für x mit $f(x) = 1$ und $f(x) = 0$ herbeiführt.

Wir definieren für eine Funktion $f: \{0,1\}^n \rightarrow \{0,1\}$ eine unitäre Abbildung $\mathbf{V_f}$ für ein entsprechendes n-Qubit-Register wie folgt:

$$V_f |x\rangle = \begin{cases} |x\rangle, f(x) = 0 \\ -|x\rangle, f(x) = 1 \end{cases}$$

Diese Abbildung verschiebt also die Phase der Komponenten x, die Lösung der Suchaufgabe sind, während die Amplituden der nicht erfüllenden Anteile unverändert bleiben. Für eine Superposition ergibt Anwenden dieses Operators:

$$V_f \sum_{i=0}^{2^n-1} \alpha_i |i\rangle = \sum_{i=0}^{2^n-1} (-1)^{f(i)} \alpha_i |i\rangle$$

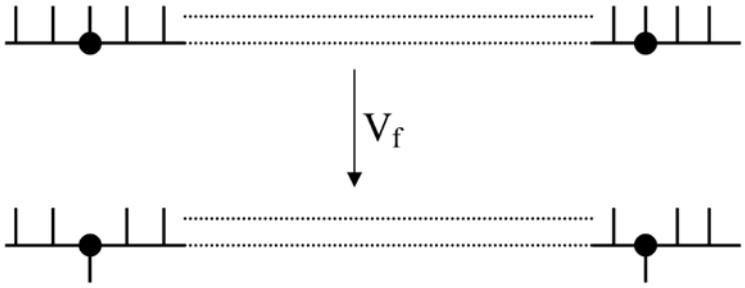


Abbildung 2: Die Wirkung des Operators V_f

Diese Operation kann einfach unter Zuhilfenahme des vorher definierten U_f realisiert werden, x sei wiederum ein beliebiger Basisvektor:

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

Wir benutzen also den Schaltkreis von U_f, wobei wir an die zweite Komponente die Superposition $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = H|1\rangle$ „anlegen". Es wird nur ein zusätzliches Qubit benötigt. Innerhalb des Algorithmus wird dies die einzige Verwendung der gegebenen Funktion f sein.

Inversion am Durchschnitt D_n

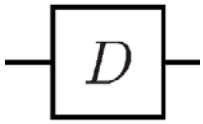
Für einen beliebigen Zustand $\varphi = \sum_{i=0}^{2^n-1} \alpha |i\rangle$ eines n-Qubit-Registers als Superposition aus den $N = 2^n$

Basiszuständen legen wir den Wert der Durchschnittsamplitude $\text{avg}(\varphi)$ einfach als fest.

$$\text{avg}(\varphi) = \frac{\sum_{i=0}^{2^n-1} \alpha_i}{N}$$

Der Abstand einer Amplitude α_i zum Durchschnitt ergibt sich als $\alpha_i - \text{avg}(\varphi)$.
Damit ist eine Operation D_n, genannt „Inversion am Durchschnitt", folgendermaßen defieniert:

$$D_n = \sum_{i=0}^{2^n-1} \left(\text{avg}(\varphi) - \left(\alpha_i - \text{avg}(\varphi)\right)\right)|i\rangle$$
$$= \sum_{i=0}^{2^n-1} \left(2\text{avg}(\varphi) - \alpha_i\right)|i\rangle$$



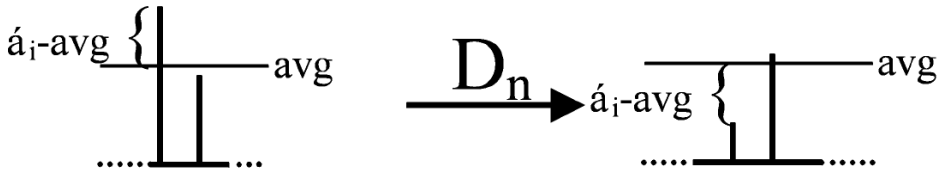


Abbildung 3: Die Wirkung des Operators D_n

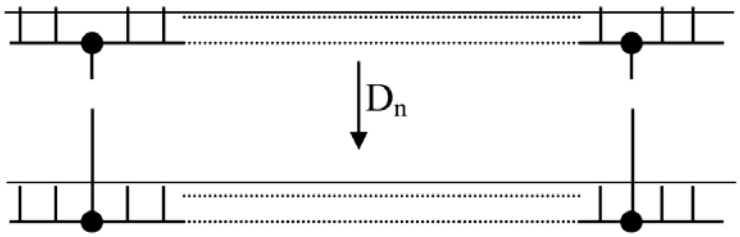


Abbildung 4: Die Anwendung auf eine Superposition

Für die Verwendung im Rahmen eines Algorithmus bleibt allerdings zu zeigen, dass diese Operation durch Quantenschaltkreise realisiert werden kann. Dazu muss D_n natürlich unitär sein.

$$\mathrm{D}_n = \begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} - 1 & \ddots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{pmatrix}$$

Die *i*-te Spalte ist also ein Vektor d_i, der aus lauter Einträgen von $\frac{2}{2^n}$ besteht, außer an der i-ten Position, dort steht $\frac{2}{2^n} - 1$

Grovers Idee

Ziel des Quantenalgorithmus muss sein, ein n-Qubit-Register so zu präparieren, dass die Wahrscheinlichkeitsamplitude einer Lösungskomponente hinreichend groß ist. Andererseits muss der Algorithmus für jede Funktion *f* funktionieren, das heißt, jeder Basisvektor könnte eine Lösung beschreiben.

Beginnen wir also damit, ein Register, beschrieben durch $|z_1\rangle$, in eine Superposition aus allen *N* Möglichkeiten zu setzen. Dies lässt sich nach den Betrachtungen des vorangehenden Abschnitts leicht durch Anwenden einer Hadamard-Transformation erreichen:

$$|z_0\rangle \leftarrow \mathrm{H}_n \left|0^{(n)}\right\rangle = \bigotimes_{i=1}^{n} \mathrm{H}|0\rangle$$

Es ergibt sich ein Zustand, in dem jede Basiskomponente mit der Amplitude $\frac{1}{\sqrt{N}}$ eingeht.

Wenden wir hierauf den bereits bekannten Operator V_f an, der genau die Amplituden der Lösungskomponenten negiert und der die Funktion *f* tatsächlich nur als „Blackbox" verwendet, erhalten wir folgendes Amplitudenspektrum. Alle *N-t* Nichtlösungskomponenten haben unverändert Amplitude $\frac{1}{\sqrt{N}}$, während sich die *t* Lösungskomponenten durch $-\frac{1}{\sqrt{N}}$ auszeichnen. Formal ist dieser Schritt $|z_0'\rangle = \mathrm{V}_f |z_0\rangle$
mit dem Ergebnis

$$|z_0'\rangle = \frac{1}{\sqrt{N}} \left(\sum_{i \in \bar{L}} |i\rangle - \sum_{i \in L} |i\rangle \right)$$

Nutzen man jetzt aus, dass für die Anzahl der Lösungen $t<<N$ gilt, so folgt für die im vorangegangenen Abschnitt definierte Durchschnittsamplitude in Zustand $|z_0'\rangle : \text{avg}(|z_0'\rangle) \approx \frac{1}{\sqrt{N}}$ .Somit verändert die Operation „Inversion am Durchschnitt" die Amplituden der Nichtlösungen sehr wenig, während die Lösungskomponenten verstärkt werden. Anwenden dieser Operation auf $|z_0'\rangle$ führt damit zu

$$|z_1\rangle = \mathrm{D}_n |z_0'\rangle$$

und ergibt in einem Zustand etwa

$$|z_1\rangle \approx \frac{1}{\sqrt{N}} \left(\sum_{i \in \bar{L}} |i\rangle - \sum_{i \in L} 3|i\rangle \right)$$

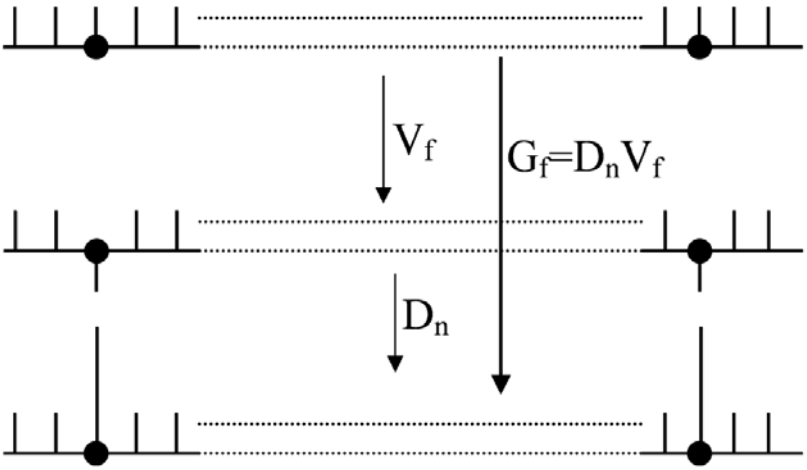


Abbildung 5: Amplitudenverstärkung durch den Groveroperator

Durch die Operationen der „*f-kontrollierten Phasenumkehr*" V_f und der „*Inversion am Durchschnitt*" D_n können also die Amplituden der Lösungsvektoren aus einer gleichmäßigen Superposition verstärkt werden. Die Verknüpfung beider Transformationen $\mathrm{G}_f = \mathrm{D}_n\mathrm{V}_f$ wird auch als Grover-Operator bezeichnet und stellt das „Herzstück" des Suchalgorithmus dar. Dort wird diese Operation solange iteriert, bis die Lösungsvektoren eine hinreichend große Wahrscheinlichkeits-amplitude haben, also bis das Register in einem Zustand ist, dessen Messung zu einer Lösung führt.

Der Algorithmus

1: Erzeuge gleichmäßige Superposition:
$|z\rangle \leftarrow \mathrm{H}_n \left|0^{(n)}\right\rangle$

2: Wende $\left(\frac{\pi}{4 \arcsin\sqrt{\frac{t}{N}}}\right)$ -mal $G_f = D_n V_f$ an.

3: Führe Messung des Registers durch und erhalte x_0

4: Prüfe f(x0)?=1
ja: Ausgabe x0, Ende
nein: Gehe zu 1.

Laufzeitanalyse

Wir betrachten die Iterationen gemäß Schritt 2 im Algorithmus. Sei jeweils l_i die Amplitude einer Lösungskomponente nach der i-ten Grover-Iteration und k_i diejenige eines nicht lösenden Basisvektors. Für den Ausgangszustand vor der ersten Runde gilt demnach

$$l_o = k_0 = \frac{1}{\sqrt{N}} \tag{1}$$

Nach Anwenden von V_f in der i-ten Runde ergibt sich nach Definition des Operators als „Zwischenresultat"

$$k_i' = k_{i-1}$$

$$l_i' = -l_{i-1}$$

Auf diesen Zustand wird dann die „Inversion am Durchschnitt" angewendet, dabei ergibt sich für die Durchschnittsamplitude $avg_i = \frac{t \cdot l_i' + (N-t) \cdot k_i'}{N}$ und mit der Definition von D_n

$$k_i = 2 \cdot avg_i - k_i'$$

$$l_i = 2 \cdot avg_i - l_i'$$

Einsetzen und Ausrechnen führt schließlich zum verschränkten rekursiven Gleichungssystem

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

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

Wir setzen ferner den Winkel $\theta = arcsin\sqrt{\frac{t}{N}}$. Für weitere Betrachtungen halten wir fest, dass somit gilt:

$$\sin\theta = \sqrt{\frac{t}{N}}$$

$$\sin^2\theta = \frac{t}{N}$$

$$\cos\theta = \sqrt{\frac{N-t}{N}}$$

$$\cos^2\theta = \frac{N-t}{N}$$

Mit dieser Wahl von θ sind

$$k_i = \frac{1}{\sqrt{N-t}}\cos\left((2i+1)\theta\right) \quad \text{und} \tag{4}$$

$$l_i = \frac{1}{\sqrt{t}}\sin\left((2i+1)\theta\right) \tag{5}$$

Beweis

Lösungen des Gleichungssystems (2) und (3) mit Startwert (1)

$$k_0 = \frac{1}{\sqrt{N-t}}\mathbf{cos}(\boldsymbol{\theta}) = \frac{1}{\sqrt{N-t}}\sqrt{\frac{\mathbf{N-t}}{\mathbf{N}}} = \frac{1}{\sqrt{N}} \quad \text{und}$$

$$l_0 = \frac{1}{\sqrt{t}}\mathbf{sin}(\boldsymbol{\theta}) = \frac{1}{\sqrt{t}}\sqrt{\frac{\mathbf{t}}{\mathbf{N}}} = \frac{1}{\sqrt{N}}$$

Wir zeigen die Erfüllung der rekursiven Beziehungen (2) und (3) per Induktion. Seien die Gleichungen also für (*i*-1) korrekt.

$$\begin{aligned} l_i &= \frac{N-2t}{N}l_{i-1} + 2\frac{N-t}{N}k_{i-1} \\ &= \frac{N-2t}{N}l_{i-1} + \sqrt{\frac{N-t}{t}}\cdot 2\frac{\sqrt{t}\sqrt{N-t}}{N}k_{i-1} \\ &= \frac{N-t}{N} - \frac{t}{N}l_{i-1} + \sqrt{\frac{N-t}{t}}\cdot 2\sqrt{\frac{t}{N}}\cdot\sqrt{\frac{N-t}{N}}k_{i-1} \end{aligned}$$

$$l_i = \cos^2(\theta) - sin^2(\theta) l_{i-1} + \sqrt{\frac{N-t}{t}} \cdot 2\sin(\theta) \cdot cos(\theta) k_{i-1}$$

Nach den Funktionen für die doppelten Winkel gilt:
$\sin 2\alpha = 2 \cdot \sin\alpha \cos\alpha$ und $\cos 2\alpha = \cos^2\alpha - \sin^2\alpha$, daraus folgt:

$$\begin{aligned} l_i &= \cos(2\theta) l_{i-1} + \sqrt{\frac{N-t}{t}} \cdot \sin(2\theta) k_{i-1} \\ &= \frac{1}{\sqrt{t}} \sqrt{t} l_{i-1} \cos(2\theta) + \frac{1}{\sqrt{t}} \sqrt{N-t} k_{i-1} \sin(2\theta) \\ &= \frac{1}{\sqrt{t}} \sin((2i)\theta) \cos(2\theta) + \frac{1}{\sqrt{t}} \cos((2i)\theta) \sin(2\theta) \end{aligned}$$

wegen

$l_{i\text{-}1} = \frac{1}{\sqrt{t}} \sin(((2i\text{-}1)+1)\theta)$ und

$k_{i\text{-}1} = \frac{1}{\sqrt{N\text{-}t}} \cos(((2i-1)+1)\theta)$ gelten nach Voraussetzung gilt dann

$l_i = \frac{1}{\sqrt{t}} \sin((2i+1)\theta)$ wegen Additionstheorem $\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta$

also genau die Behauptung (3). Die Korrektheit der entsprechenden Gleichung für k_i kann in analoger Weise erfolgen. Die Gültigkeit von (4) und (5) für alle i folgt dann per Induktionsschluss.

□

Damit geht nach der i-ten Iteration jede der t Lösungskomponenten im Superpositionsspektrum mit einer Amplitude von $l_i = \frac{1}{\sqrt{t}} \sin((2i+1)\theta)$ ein. Die Wahrscheinlichkeit, eine dieser Lösungen zu messen, beträgt demnach l_i^2 (nach Quantenpostulat). Eine beliebige der t lösenden Komponenten misst man also mit Wahrscheinlichkeit $t \cdot l_i^2$.

Wir würden mit Sicherheit, das heißt mit Wahrscheinlichkeit 1, eine Lösung erhalten, wenn $l_i = \frac{1}{\sqrt{t}}$,

also wenn $\sin((2i+1)\theta) = 1$

Dazu muss $((2i+1)\theta) = \frac{\pi}{2}$ sein, was genau für $i = \frac{\pi}{4\theta} - \frac{1}{2}$ passiert.

Deswegen wird im Algorithmus der Grover-Operator $\left[\frac{\pi}{4\theta}\right] = \left(\frac{\pi}{4 \arcsin\sqrt{\frac{t}{N}}}\right)$ mal angewendet. Durch die notwendige Einschränkung auf ganze Zahlen i ergibt sich ein geringer Fehler.

Komplexitätsabschätzung:

$\sin\theta = \theta$ für θ klein

$$\frac{\pi}{4\arcsin\sqrt{\frac{t}{N}}} \approx \frac{\pi}{4\sqrt{\frac{t}{N}}} = \frac{\pi}{4\sqrt{t}}\sqrt{N} = \mathrm{O}\left(\sqrt{N}\right)$$

Weitere Problemstellungen

Minimum finden

Häufig gibt es zu einem Suchproblem kein Prädikat, welches für jedes Element Aufschluss über die Erfüllung der Suche gibt, sondern es wird nach einem Element gefragt, welches sich durch eine Relation zu den restlichen auszeichnet. Für die Suche nach dem Minimum lässt sich ein Quantenalgorithmus angeben, dessen Kern eine Grover-Iteration ist. Dieser findet das Minimum mit Wahrscheinlichkeit $\frac{1}{2}$ in $\mathrm{O}\left(\sqrt{\mathrm{N}}\right)$ Schritten.

Zählen der Lösungen

Ein Weg, mit einem Quanten-Verfahren die Anzahl von Lösungen eines Suchproblems zu finden, kombiniert grundlegende Ideen von sowohl *Grovers Suche* als auch *Shors Faktorisierungsalgorithmus*. Dabei wird ausgenutzt, dass sich die *Amplituden* der Lösungskomponenten einerseits, sowie der Nichtlösungsanteile andererseits unter Anwendung des Grover-Operators *periodisch verändern*. Die Größe dieser Periode kann mit der *Quanten-Fourier-Transformation* annähernd bestimmt werden und erlaubt damit den gewünschten Rückschluss auf die Anzahl der Lösungen.

Das Kollisionsproblem

Zu einer Funktion f(x) werden $x_o \neq x_1$ mit $f(x_1) = f(x_2)$ gesucht. Dieses Problem spielt in der Kryptologie und -analyse eine Rolle.

Literatur

Vieles für das Thema Grover-Suche von Lov Grover selbst findet sich im lanl e-print Archiv
http://xxx.lanl.gov

Grovers Suchalgorithmus von Andreas Berger
www.tu-chemnitz.de/informatik/HomePages/ ThIS/Seminare/ss02/QC/berger.pdf

Quantencomputer von Jacobo Torán
http://theorie.informatik.uni-ulm.de/Personen/jt.html