Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Informatik

Quantencomputer

Vorgelegt von Michael Graf

20. Januar 2011

Inhaltsverzeichnis

1. Einleitung

Dieser Text beschäftigt sich mit Quantencomputern, einer neuen Technologie, die sich derzeit im Forschungsstadium befinden. Es wird erklärt auf welche Art sie arbeiten und wie sie sich von klassischen Computern unterscheiden. Da einzelne Atome (Quanten) für die Speicherung von Informationen (Bits) benutzt werden, gelten dort die Gesetze der Quantenmechanik. Klassische Algorithmen müssen neu geschrieben werden um auf dieser Hardware laufen zu können.

In dieser Arbeit werden ein Suchalgorithmus, eine Verschlüsselungsverfahren und ein Entscheidungsproblem analysiert. Diese Algorithmen benutzen Quanteneigenschaften wie die Verschränkung, Interferenz oder die Superposition um Probleme effizient zu lösen. Die

Wahrscheinlichkeit spielt eine große Rolle für die Algorithmen. Sie können ein Ergebnis immer nur mit einer gewissen Wahrscheinlichkeit berechnen, welche es in den Algorithmen möglichst hoch zu halten gilt. Zur Informationsübertragung werden Verfahren wie die Teleportation oder die Dichte Kodierung vorgestellt.

Quantencomputer können Probleme lösen, die eine Turingmaschine nicht effizient lösen kann, z.B. die Zerlegung großer Zahlen in ihre Primfaktoren. [Sho94] Ungeklärt ist, ob Quantencomputer Probleme aus der Klasse NP-Vollständig effizient lösen können. Abschließend werden unterschiedliche Hardwarerealisierungen vorgestellt, wie z.B. Qubits durch polarisierende Photonen, die in unterschiedlichen Ebenen Schwingen.

Als Grundlage dient ‘Quantum Computing verstehen‘ von Matthias Homeister.[1]

2. Quanteneigenschaften

2.1. Superposition

Quantencomputer werden mit so kleinen Elementen arbeiten, dass die Gesetze der Quantenmechanik für diese gelten werden. Die Quantenmechanik beschreibt die Gesetze aller Mikroskopischen Teilchen im Universum, so wie die Allgemeine Relativitätstheorie alle Makroskopischen Ereignisse beschreibt. Als Quantum versteht man z.B. ein einzelnes Ion oder Photon. Diese Atome unterliegen den Quantengesetzen und man kann, wenn sie von der Umwelt isoliert werden, z.B. durch einsperren in ein Vakuum, nichts ohne Messung über sie in Erfahrung bringen. Eine Messung würde die Isolation von der Umwelt zerstören und der Zustand des Quantum, der sich zuvor in einer Superposition befand, wird zerstört. Schrödingers Katze [Cam06] ist wohl die berühmteste Analogie dafür. Eine lebendige Katze wird in eine Kiste eingesperrt, wobei die verschlossene Kiste die Abschirmung von der Umwelt repräsentiert. In dieser Kiste ist ein grausamer Mechanismus installiert, der mit einer Wahrscheinlichkeit von 50% ein tödliches Gift freisetzt und die Katze tötet. Sobald wir die Kiste schließen, soll der Mechanismus in Kraft gesetzt werden. In diesem Moment befindet sich die Katze in einer Superposition der beiden Zustände lebendig und tot, beide sind mit gleicher Wahrscheinlichkeit, nämlich 50% möglich. Solange die Kiste nicht geöffnet wird, ist es unmöglich zu bestimmen, was im Inneren stattgefunden hat. Die Katze befindet sich also in einem Schwebezustand, der erst dann bestimmt werden kann, wenn man die Kiste wieder öffnet. Das öffnen der Kiste ist gleichzusetzten mit einer Messung. Findet das statt, geht der Zustand der Katze in einen der beiden möglichen klassischen Zustände über und man sieht entweder eine tote oder eine lebendige Katze. Eine Superposition ist also ein Schwebezustand beliebig vieler Zustände bei denen alle einzelnen Wahrscheinlichkeiten der möglichen Zustände zusammen 100% ergeben müssen.

[1] Alle Tabellen und Formeln entstammen diesem Buch.

2.2. Verschränkung

Eine weitere wichtige Eigenschaft ist die Verschränkung von Teilchen. Es ist in der Quantenwelt möglich, dass räumlich getrennte Quanten ein und dasselbe Objekt sind. Die Information über den Zustand dieser verschränkten Quanten steckt in beiden zusammen und eine Veränderung des einen Partners führt zur instantanen (Zeitlosen) Veränderung des anderen, egal wie weit entfernt sie sind. Diese Eigenschaft macht sich z.B. die Teleportation von Quanten zunutze.

2.3. Interferenz

Interferenz beschreibt die Welleneigenschaften von Quanten, wobei Wellenberge und Wellentäler als positive oder negative Amplituden (Wahrscheinlichkeiten) zu sehen sind. Zwei aufeinandertreffende Wellen addieren sich zu einer größeren. Das Auftreffen eines Wellenberges auf ein Wellental eliminiert die Welle dagegen. Von konstruktiver Interferenz spricht man, wenn sich die Werte der Amplituden addieren und von destruktiver Interferenz, wenn sich die Amplituden gegenseitig auslöschen.

3. Quantenbit (Qubit) und die Hadamard-Transformation

Ein Qubit ist die unterste Einheit auf der eine Information gespeichert wird, so wie im Klassischen Bit auch. Das klassische Bit kann die Zustände 1 und 0 speichern, ein Qubit dagegen kann beliebig viele Kombinationen dieser beiden Zustände in einer Superposition enthalten. Die beiden Klassischen Zustände werden im Qubit als $|0\rangle$ für 0 und $|1\rangle$ für 1 definiert.
Allgemeine Definition für den Zustand eines Qubits:

$$\alpha * |0\rangle + \beta * |1\rangle$$

α und β sind komplexe Zahlen und heißen Amplituden. Es gilt:

$$|\alpha|^2 + |\beta|^2 = 1$$

$|\alpha|^2$ und $|\beta|^2$ sind die Wahrscheinlichkeiten für die jeweils folgenden Zustände. Der Zustand von Schrödingers Katze wäre z.B.

$$\frac{1}{\sqrt{2}}(|tot\rangle + |lebendig\rangle)$$

Um die folgenden Rechenschritte zu verstehen, wird der Zustand des Quantenbits als Vektor in einem zweidimensionalen Vektorraum über den komplexen Zahlen gesehen.

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

Um den Zustand von Schrödingers Katze zu realisieren, muss auf den Ausgangszustand $|0\rangle$, der für lebendige Katze steht, eine Transformation mit einer Matrix angewendet werden. Die Matrix, die einen Zustand in eine Superposition mit gleichen Wahrscheinlichkeiten transferiert, heißt Hadamard-Matrix [2] und spielt eine sehr wichtige Rolle. Sie ist folgendermaßen definiert:

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

Weil H zu sich selber invers ist, H^{-1}=H oder HH = I, kann man einen klassischen Zustand in eine Superposition bringen und durch eine weitere Transformation wieder den ursprünglichen Zustand herstellen.

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

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H} |1\rangle$$

Durch diese Transformation, kann ein Algorithmus umgesetzt werden, der echte Zufallszahlen generiert. Klassische Rechner können nur Pseudo-Zufallszahlen liefern, die auf verschiedene Art berechnet werden. Das Messen eines Quantum, welches sich in einer Superposition befindet, nimmt per echtem Zufall eines der beiden Zustände $|0\rangle$ oder $|1\rangle$ an, je nach Wahrscheinlichkeit seiner Amplituden. Für den Algorithmus sind 3 Schritte notwendig.

1. $|x\rangle \leftarrow |0\rangle$ Ein Qubit $|x\rangle$ wird in den Anfangszustand $|0\rangle$ versetzt
2. $|x\rangle \leftarrow \mathrm{H}|x\rangle$ Auf das Bit wird die Hadamard Transformation ausgeführt
3. $Miss\ |x\rangle$ Das Bit wird gemessen und liefert mit je 50% $|1\rangle$ oder $|0\rangle$

Damit kann eine Zufallszahl generiert werden, die nicht vorhersehbar ist.

4. Quantenregister

Ein Quantenregister ist eine Folge von *n* Bits und hat als Zustand eine Superposition der 2^n klassischen Zustände. Aus einem Register mit zwei Qubits lässt sich durch Umformung ein übersichtlicher Zustand erkennen:

[2] Benannt nach dem französischen Mathematiker Jacques Hadamard 1865-1963.

$$R = |x_1\rangle|x_0\rangle$$

$$|x_1\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

$$|x_0\rangle = \gamma_0|0\rangle + \gamma_1|1\rangle$$

$$R = (\beta_0|0\rangle + \beta_1|1\rangle) * (\gamma_0|0\rangle + \gamma_1|1\rangle)$$

$$R = \beta_0\gamma_0|0\rangle|0\rangle + \beta_0\gamma_1|0\rangle|1\rangle + \beta_1\gamma_0|1|0\rangle + \beta_1\gamma_1|1|1\rangle$$

Aus $\beta_i\gamma_j$ wird α_{ij} zur besseren Übersicht:

$$R = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1|0\rangle + \alpha_{11}|1|1\rangle$$

Die Schreibweise $|0\rangle|0\rangle$ ist äquivalent mit $|00\rangle$ und statt der Bits kann der ganzzahlige Wert der Binärdarstellung geschrieben werden:

$$R = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$$

Auf diese Weise erlangt man eine Superposition über die vier klassischen Zustände: 0, 1, 2 und 3.

Allgemeine Definition:

$$R = \sum_{i=0}^{2^n-1} \alpha_i\,|i\rangle$$

Die Bits des Registers sind entsprechend der Binärdarstellung der natürlichen Zahl i gesetzt. Bei einer Messung des Registers betrachtet man mit der Wahrscheinlichkeit $|\alpha_i|^2$ den Zustand $|i\rangle$.

Man kann nicht nur in der Basis der Klassischen Zustände eine Superposition messen, man kann jede Basis nehmen, deren Elemente Senkrecht aufeinander stehen, also Orthogonale Basen. Wird zur Basis

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

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

gemessen, betrachtet man mit der Wahrscheinlichkeit $|\alpha'|^2$ den Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und mit Wahrscheinlichkeit $|\beta'|^2$ den Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Auch die Messung einer anderen Basis zerstört die Superposition und es wird einer der Zustände der gemessenen Basis angenommen.

Befindet sich ein Quantenregister $R = |xy\rangle$ in dem Zustand

$$|\Phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

so wird die Superposition des Registers beim Messen des Bits $|x\rangle$ mit der Wahrscheinlichkeit $|\alpha_{00}|^2 + |\alpha_{01}|^2$ in den Zustand

$$|\Phi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

und mit der Wahrscheinlichkeit $|\alpha_{10}|^2 + |\alpha_{11}|^2$ in den Zustand

$$|\Phi'\rangle = \frac{\alpha_{00}|10\rangle + \alpha_{01}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

übergehen. Im ersten Fall wäre das gemessene Bit $|x\rangle = |0\rangle$ und im zweiten $|x\rangle = |1\rangle$.

Das gemessene Bit $|x\rangle$ verschränkt sich mit dem Zustand des Registers und dadurch entsteht eine neue Superposition. Das Messen eines einzelnen Bits aus einem Register zerstört die Superposition des Registers nicht, sondern erzeugt eine neue die abhängig vom Ergebnis des gemessenen Bits ist.

5. Verschränkte Bits

Sind zwei Qubits miteinander verschränkt, wirkt sich eine Manipulation bzw. Messung eines dieser Qubits unmittelbar auf dessen verschränkten Partner aus. Eine Verschränkung zwischen zwei Qubits $|x\rangle$ und $|y\rangle$ lässt sich durch die Operation CNOT (Controlled NOT) realisieren, die in Abbildung 1 zu sehen ist.

x	**y**	**CNOT (x,y)**
0	0	00
0	1	01
1	0	11
1	1	10

(Abbildung 1: CNOT Wahrheitstabelle)

Diese Operation wird durch die Binäre Addition, oder das Exklusivoder realisiert.

$$CNOT: |x, y\rangle \rightarrow |x, y \oplus x\rangle$$

Zwei Qubits werden in den Ausgangszustand $|00\rangle$ versetzt um dann auf das erste Qubit $|x\rangle$ die Hadamard-Transformation anzuwenden. Wird auf diesen Zustand die Operation CNOT ausgeführt, geht das Register in einen Verschränkten Zustand über.

$$|00\rangle \xrightarrow{H\otimes I_2} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Ist eins der Qubits $|0\rangle$, kann es nur den Zustand $|00\rangle$ geben. Ist eines der Qubits $|1\rangle$, gibt es nur den möglichen Zustand $|11\rangle$. Misst mal also ein Qubit dieses verschränkten Paares, so kann das andere nur den gleichen Zustand annehmen. Diese Beziehung zueinander ist räumlich absolut unabhängig. Wird eines dieser Qubits über einen Quantenkanal an einen anderen Ort (Entfernung spielt keine Rolle) transportiert, bleibt diese Bindung erhalten. Dieser Zustand ist einer von vier möglichen verschränkten Zuständen, die den Namen Bell-Zustände[3] tragen:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Diese Zustände bilden eine Orthonormalbasis des Zustandsraumes der beiden Qubits. Die Zustände Ψ^+ und Ψ^- haben eine negierende Wirkung auf die beiden Qubits. Ist das eine $|0\rangle$, kann das andere nur den negierten Zustand $|1\rangle$ annehmen und umgekehrt. Ein verschränkter Zustand lässt sich nicht in das Produkt von Zuständen seiner einzelnen Bits zerlegen. 2 Qubits im Zustand Ψ^+ oder Φ^+ werden auch Einstein-Podolsky-Rosen (EPR) Paar [Cam062] genannt.

6. Informationsübertragung

6.1. Teleportation

Eine Teleportation ist eine instantane (zeitlose) Überwindung einer beliebigen Entfernung. Laut der Allgemeinen Relativitätstheorie [Fli06] ist das Bewegen durch den Raum höchstens mit Lichtgeschwindigkeit möglich. Mit Hilfe der Verschränkung kann der Zustand eines Quantum teleportiert werden. Die Einschränkung ist, dass eine Transformation beim Empfänger benötigt wird, die abhängig von der Messung des Absenders ist. Diese Information muss über einen Klassischen Kanal stattfinden. Der Kanal ist den klassischen Gesetzen unterworfen und widerspricht nicht der Allgemeinen Relativitätstheorie.

[3] Benannt nach dem in Belfast geborenen Physiker John Bell (1928-1990).

Absender und Empfänger haben jeweils ein Pärchen eines EPR-Paares, das sich im Zustand

$$|ae\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

befindet. Der Absender besitzt $|a\rangle$ und der Empfänger $|e\rangle$. Der Absender möchte ein Qubit $|x\rangle$, das sich im Zustand $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ befindet, zum Empfänger teleportieren. Dazu verschränkt er $|x\rangle$ und $|a\rangle$ miteinander mittels CNOT:

$$|x\rangle|a\rangle \leftarrow |x\rangle|a \oplus x\rangle.$$

Dann wird die Hadamard-Transformation auf $|x\rangle$ angewandt, damit das Register $|x\rangle|a\rangle$ in eine Superposition der 4 Zustände $|00\rangle, |01\rangle, |10\rangle$ und $|11\rangle$ mit gleicher Wahrscheinlichkeit $\frac{1}{4}$ geht. Werden nun $|x\rangle$ und $|a\rangle$ vom Absender gemessen, so geht der verschränkte Zustand $|b\rangle$ beim Empfänger in einen Zustand, der abhängig ist von der Messung des Absenders.

Zustände Absender	Zustand Empfänger
$\|00\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
$\|01\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$
$\|10\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$
$\|11\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$

(Abbildung 2: Aus den Zuständen des Absenders beeinflussen den Zustand beim Empfänger)

Um den Zustand $|x\rangle$ beim Empfänger herzustellen, muss das Ergebnis der Messung vom Absender bekannt sein, um die richtige Transformation anwenden zu können. Dieser Informationsaustausch kann über irgendeinen klassischen Kanal stattfinden. Ist der Zustand des Absenders $|00\rangle$, so ist der Zustand $|\Psi\rangle$ bereits im Qubit $|b\rangle$ übergegangen und die Teleportation ist abgeschlossen. Ist der Zustand des Absenders $|01\rangle$, muss der Empfänger die beiden Amplituden α und β tauschen, dies gelingt mit der Transformation folgender Matrix:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Ist der Zustand des Absenders $|10\rangle$, muss die Amplitude β negiert werden und zwar mit folgender Matrix:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Ist der Zustand des Absenders $|11\rangle$, muss beides stattfinden, also X und Z angewandt werden. Der Zustand kann also vom Empfänger erst benutzt werden, nachdem er die Information des Messvorgangs erhalten und die Transformation durchgeführt hat. Dadurch steht die Teleportation auch nicht im Konflikt mit dem Gesetz ‘Information is physical‘[Svo96], was bedeutet, dass Information jeglicher Art den klassischen Gesetzen der Allgemeinen Relativitätstheorie unterliegen. Sobald die Teleportation abgeschlossen ist, kann der Absender

den übermittelten Zustand $|\Psi\rangle$ mit keinen Mitteln mehr Rekonstruieren. Da sich Quantenzustände nicht kopieren lassen, wird sich auch in diesem Fall an das Gesetz gehalten.

6.2.Dichte Kodierung

Dieses Verfahren kann mit einem Qubit die doppelte Informationsmenge eines klassischen Bits übertragen. Absender und Empfänger besitzen wie bei der Teleportation jeweils ein EPR-Paar $|a\rangle$ und $|e\rangle$, die sich in dem verschränkten Zustand

$$|ae\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

befinden. Der Absender muss sein verschränktes Qubit nun in einen der vier Bell-Zustände transferieren. Da es sich durch die Verschränkung bereits im Zustand $|\Phi^+\rangle$ befindet, kann dieser ohne weitere Transformation als Information genutzt werden. Die anderen drei Zustände werden durch folgende Matrizen realisiert:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};\ Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Sei N die zu übermittelnde Nachricht, werden die in Abbildung 3 gezeigten Transformationen durchgeführt:

N = 00	Nichts tun
N = 01	$\|a\rangle \leftarrow Z\|a\rangle$
N = 10	$\|a\rangle \leftarrow X\|a\rangle$
N = 11	$\|a\rangle \leftarrow Y\|a\rangle$

(Abbildung 3: Notwendige Transformationen)

Nach der Transformation schickt der Absender sein Qubit $|a\rangle$ mittels eines Quantenkanals an den Empfänger. Dieser misst die beiden Qubits bezüglich der Bell-Basis und kann aus der Messung die Nachricht aus Abbildung 4 erschließen:

Messergebnis:	Nachricht:
$\|ae\rangle = \|\Phi^+\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	N = 00
$\|ae\rangle = \|\Phi^-\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	N = 01
$\|ae\rangle = \|\Psi^+\rangle = \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	N = 10
$\|ae\rangle = \|\Psi^-\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	N = 11

(Abbildung 4: Aus den Messergebnissen wird die Nachricht extrahiert)

Damit wurde mit einem Qubit eine 2Bit Information gesendet. Das jedoch steht im Konflikt mit der Holevoschranke[4], die aussagt, dass sich mit einem Quantenbit nur ein Bit Information übertragen lässt. Genau genommen trifft das auch auf dieses Verfahren zu, da man das verschränkte EPR-Paar $|ae\rangle$ erst erzeugen und dann $|e\rangle$ zum Empfänger schicken muss, was als Übertragung zählt. Demnach sind doch zwei Qubits für die Information übertragen worden. Der einzige Unterschied ist, dass das Verschränkte Qubit übertragen werden kann bevor die zu übermittelnde Information feststeht.

7. QuantenOrakel

Der Begriff Orakel wird für eine Funktion benutzt, dessen Funktionswerte in einer Superposition stehen, d.h. das Orakel kennt alle Ergebnisse aller möglichen Eingabewerte. Durch geschickte Transformationen dieser Superposition wird dann versucht, dass die Amplitude (die Wahrscheinlichkeit) des gesuchten Funktionswertes deutlich höher wird als die anderen, so dass man beim Messen mit sehr hoher Wahrscheinlichkeit das gewünschte Ergebnis erhält.

8. Algorithmen

8.1. Das Problem von Deutsch

Um eine Münze auf ihre Echtheit zu überprüfen, muss ein klassischer Algorithmus, bei diesem Problem [Deu92], beide Seiten betrachten um eine ausreichende Antwort zu geben. Echtheit wird dadurch definiert, dass beide Seiten unterschiedlich seien müssen (Kopf und Zahl). Das Problem kann man in folgender Funktion wiederspiegeln:

$$f: \{0,1\} \rightarrow \{0,1\}$$

Die Funktion wird in Abbildung 5 definiert:

$f(0) = f(1)$	Münze ist unecht
$f(0) \neq f(1)$	Münze ist echt

(Abbildung 5: Funktion wird definiert)

Diese Funktion liegt uns als Orakel vor. Man erstellt aus zwei Qubits eine Superposition der beiden möglichen Eingabewerte $|0\rangle$ und $|1\rangle$. Mit dieser Superposition wird dann das Orakel

[4] Benannt nach Alexander Holevo vom Moskauer Steklov Institut.

einmal aufgerufen. Dies wird folgendermaßen realisiert: Man initialisiert zwei Qubits $|xy\rangle$ mit dem Zustand $|01\rangle$, wendet dann auf beide Qubits die Hadamard-Transformation an und folgender Zustand entsteht:

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) * \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Durch Ausmultiplizieren ergibt das:

$$|\Phi_2\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Damit hat man eine Superposition aller Basiszustände, wobei das Vorzeichen eine wichtige Rolle spielt. Dann wird mit diesem Zustand die Funktion aufgerufen:

$$|\Phi_3\rangle = \frac{1}{2}(|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

Durch Ausklammern der Basiszustände ergibt das:

$$|\Phi_3\rangle = \frac{1}{2}(|0\rangle * (|f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle * (|f(1)\rangle - |1 \oplus f(1)\rangle))$$

Dies ist die Superposition über alle Funktionswerte, wenn diese jetzt gemessen werden würde, erhielte man mit jeweils gleicher Wahrscheinlichkeit einen der vier möglichen Zustände $|00\rangle - |11\rangle$, was keinerlei Information zu dem Problem liefert. Deshalb muss man erneut die Hadamard-Transformation anwenden. Zunächst aber wird festgestellt das

$$(|f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$$

gilt. Daraus ergibt sich eine Umformung in $|\Phi_3\rangle$:

$$|\Phi_3\rangle = \frac{1}{2}\left((-1)^{f(0)}|0\rangle * (|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle * (|0\rangle - |1\rangle)\right)$$

$$|\Phi_3\rangle = \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right) * (|0\rangle - |1\rangle)$$

Damit wurde der Funktionswert in das Vorzeichen verlagert. Dann wird der Zustand

so umgeformt, dass er auf

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

und

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

verteilt wird. Dann wird auf beide Qubits die Hadamard-Transformation ausgeführt.

Im Falle einer unechten Münze ist $(-1)^{f(0)} = (-1)^{f(1)}$ und der Zustand von $|x\rangle$ entweder $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ oder $-\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Die Hadamard-Transformation macht aus dem ersten $|0\rangle$ und dem zweiten $-|0\rangle$. Das Qubit $|y\rangle$ dagegen wird durch die Transformation zu $|1\rangle$, also wird das Register $|xy\rangle$ im Falle einer unechten Münze am Schluss auf

$$|\Phi_4^{unecht}\rangle = \pm|0\rangle|1\rangle$$

stehen.

Im Falle einer echten Münze ist $(-1)^{f(0)} \neq (-1)^{f(1)}$ und der Zustand von $|x\rangle$ entweder $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ oder $-\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Die Hadamard-Transformation macht aus dem ersten $|1\rangle$ und dem zweiten $-|1\rangle$. Das Qubit $|y\rangle$ dagegen wird durch die Transformation zu $|1\rangle$, also wird das Register $|xy\rangle$ im Falle einer unechten Münze am Schluss auf

$$|\Phi_4^{echt}\rangle = \pm|1\rangle|1\rangle$$

stehen.

Dieses Verfahren nutzt die Quanteneigenschaft Interferenz, um die Wahrscheinlichkeit der richtigen Lösung zu erhöhen und die der falschen Lösungen zu verringern.

Angenommen die Münze sei unecht, dann ist das erste Qubit $|x\rangle$ im 3. Schritt

$$|x\rangle = \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Die Hadamard-Transformation überführt den Zustand in

$$|x\rangle = \pm\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)).$$

Dadurch werden die Amplituden $|0\rangle$ zu $\frac{1}{2} + \frac{1}{2} = 1$ und die von $|1\rangle$ zu $\frac{1}{2} - \frac{1}{2} = 0$. Also kann beim anschließenden Messen nur das Ergebnis $|0\rangle$ sein.

Dieser Quantenalgorithmus kann eine Münze durch einmaliges Aufrufen des Quantenorakels (Funktion) auf ihre Echtheit überprüfen, wobei ein klassischer Algorithmus zwei Aufrufe benötigt.

8.2.Grovers Suchalgorithmus

Der Suchalgorithmus [Gro96] lässt sich z.B. auf eine Datenbanksuche mit N Elementen anwenden. Dazu wird eine Funktion benutzt, die als Eingabe das gesuchte Element x hat und der Rückgabewert für das richtige Element $\hat{x} = 1$ ist. Für alle falschen Elemente $x \neq \hat{x}$ ist der

Rückgabewert 0. Diese Funktion ist als Quantenorakel verfügbar. Aus der Superposition des Orakels aller möglichen Elemente, wird die Amplitude der tatsächlichen Lösung erhöht und die aller anderen verkleinert, so dass eine Messung das gewünschte Ergebnis mit einer sehr hohen Wahrscheinlichkeit liefert. Die gleichverteilte Superposition über alle Datenbankelemente sieht folgendermaßen aus:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Sei $|x\rangle$ unsere Eingabe und $|y\rangle$ unsere Ausgabe, dann wird $|y\rangle$ auf $|1\rangle$ gesetzt und die Hadamard-Transformation darauf angewandt. Dann folgt aus dem Register $|xy\rangle$

$$|x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

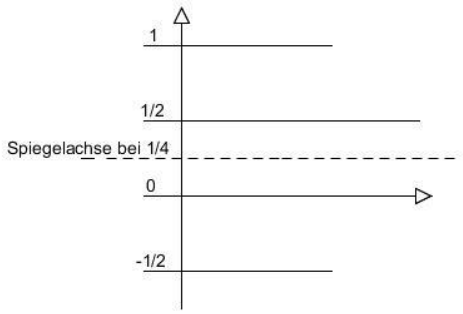
Wendet man nun das Orakel auf $|y\rangle$ an, dann erhält man

$$|x\rangle \frac{1}{\sqrt{2}} (|f(x)\rangle - |1 \oplus f(x)\rangle).$$

Durch Verlagern des Funktionswertes in das Vorzeichen erhält man

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

Da das erwünschte Ergebnis $\hat{x}$ als einziges auf 1 abgebildet wird, bekommt dies als einziges eine negative Amplitude. Die Amplitude des gesuchten Elements unterscheidet sich von allen anderen und muss erhöht werden. Das Spiegeln der Amplituden an ihrem Mittelwert führt den gewünschten Effekt herbei. Im Fall von vier Elementen ist der Mittelwert der Amplituden $\frac{1}{4} * \left(\frac{1}{2} - \frac{1}{2} + \frac{1}{2} + \frac{1}{2}\right) = \frac{1}{4}$. Die $-\frac{1}{2}$ zeigt das gesuchte Element. Spiegelt man nun, wie in Abbildung 6 ersichtlich, alle Amplituden am Mittelwert $\frac{1}{4}$, so wird aus $\frac{1}{2} \rightarrow 0$ und aus $-\frac{1}{2} \rightarrow 1$.



(Abbildung 6: Spiegelung der Amplituden an ihrem Mittelwert)

Im Falle N=4 würde eine einzige Spiegelung ausreichen, um die Wahrscheinlichkeit für das gesuchte Element auf 100% zu bringen. Eine Messung liefert das gewünschte Ergebnis mit absoluter Sicherheit. Es muss für alle N herausgefunden werden, wie oft die beiden Schritte

1. Amplitude des gesuchten Elements negieren
2. Spiegelung am Mittelwert

durchgeführt werden müssen. Hat die Amplitude des gesuchten Elements ihr Maximum erreicht, wird sie beim erneuten Anwenden der Spiegelung kleiner. Dazu existiert eine Funktion [Hom08] $G(N) \approx \frac{\pi}{4}\sqrt{N}$, die die Anzahl der erforderlichen Iterationen ausrechnet. Außerdem lässt sich dadurch auch die Laufzeit des Algorithmus berechnen. Für das Orakel werden $\log(n)$ Aufrufe benötigt. Die Funktion G(N) findet in $\sqrt{N}$ Schritten heraus, wie oft die Spiegelung stattfinden muss. Zusammen ergibt sich eine Komplexität von $O(\log(N) * \sqrt{N})$. Ein klassischer Algorithmus dagegen muss sich jedes Element nacheinander ansehen und muss im schlechtesten Fall N-1 Elemente ausprobieren. Im mittleren Fall werden $\frac{(N+1)}{2}$ Versuche benötigt, dadurch hat ein klassischer Algorithmus eine Komplexität von $O(\mathrm{N})$.

8.3.Quantenverschlüsselung: BB84-Protokoll

Das BB84-Protokoll [BB84] ermöglicht den geheimen Schlüsselaustausch, ohne dass dieser manipuliert oder abgehört werden kann. Dieses Verfahren nutzt die echten Zufallsbits. Möchte der Absender A ein geheimes Bit an Empfänger E schicken, so muss der Absender folgende Schritte durchführen:

1. Es wird ein zufälliges Bit a erzeugt, das mit gleicher Wahrscheinlichkeit 0 oder 1 ist, dies wird dann dem Schlüsselbit zugewiesen $|x\rangle = |a\rangle$.
2. Es wird ein weiteres zufälliges Bit a' erzeugt, ist dies 0 gibt es keine Änderung an $|x\rangle$. Ist es aber 1, so wird die Hadamard-Transformation auf $|x\rangle$ angewandt.
3. $|x\rangle$ wird an den Empfänger über einen Quantenkanal gesendet.

Die Anwendung der Hadamard-Transformation auf $|x\rangle$ ergibt folgende Zustände:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ bei } |x\rangle = |0\rangle$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ bei } |x\rangle = |1\rangle$$

Der Empfänger muss folgende Schritte ausführen:

1. Ein zufälliges Bit b' erzeugen. Ist $b' = 0$, so wird das empfangende Bit $|x\rangle$ bezüglich der Basis $B = \{|0\rangle, |1\rangle\}$ gemessen. Im Fall $b' = 1$ wird es bezüglich der Basis $B' = \{|+\rangle, |-\rangle\}$ gemessen.
2. Über einen Klassischen Kanal teilt der Empfänger dem Absender mit, bezüglich welcher Basis er gemessen hat.

Das Messen des Bits $|x\rangle$ beim Empfänger ergibt $|0\rangle$, wenn es vorher im Zustand $|0\rangle$ oder $|+\rangle$ war und es ergibt $|1\rangle$, wenn es vorher im Zustand $|1\rangle$ oder $|-\rangle$ war. Wenn der Empfänger bezüglich der richtigen Basis gemessen hat, so sind Sender und Empfänger im Besitz des gleichen Bits und es wird Teil des Schlüssels, hat der Empfänger aber in der falschen Basis gemessen, so ist das Ergebnis ein zufälliges Bit und wird nicht für den Schlüssel verwendet. Darüber wird über einen Klassischen Kanal entschieden, in dem sich der Absender und der Empfänger darüber austauschen, welche Basis genommen wurde. Abbildung 7 zeigt den Zusammenbau des Schlüssels:

a	0	0	1	1	0	0	1	1
a'	0	1	0	1	0	1	0	1
$\|x\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$
b'	0	0	0	0	1	1	1	1
b	0	Zufall	1	Zufall	Zufall	0	Zufall	1
Schlüssel	0		1			0		1

(Abbildung 7: Erzeugung eines gemeinsamen Schlüssels)

Eine dritte Person, die das Prozedere genau kennt und vollen Zugriff auf den Quanten- und den klassischen Kanal hat, darf trotzdem nicht den geheimen Schlüssel erfahren. Durch Belauschen des klassischen Kanals, kann sie die Zufallsbits a' und b' erfahren, aber erst nach der Messung des Empfängers. Da Qubits nicht kopiert werden können, bleibt einer dritten Person nichts übrig, als es zu messen und weiter zu schicken. Durch eine Messung wird aber in der Hälfte aller Fälle das Ergebnis verändert, da die dritte Person, ebenfalls nur per Zufall in der Basis B oder B' messen kann. Bei der richtigen Wahl der Basis, wird das Ergebnis nicht verfälscht, bei der Falschen aber schon. Nach der Messung muss der Angreifer das Bit an den Empfänger weiterschicken, da dieser sonst den Angriff bemerkt. Um diesen Schwindel aufdecken zu können, tauschen der Absender und der Empfänger eine konstante Anzahl Bits von ihrem angeblich korrekt übermittelten Schlüssel aus, die für den endgültigen Schlüssel nicht mehr benutzt werden. Unterscheiden sie sich, so ist klar, dass eine Manipulation stattgefunden hat und der gesamte Schlüssel wird verworfen und die Prozedur wird zu einem anderen Zeitpunkt erneut durchgeführt.

9. Hardwarerealisierung

9.1. Polarisierte Photonen

Ein polarisiertes Photon [Ben92] (Lichtteilchen) lässt sich leicht über große Strecken transportieren. Licht lässt sich polarisieren, das bedeutet, dass das Photon in Schwingung versetzt wird. Durch gewisse Filter kann man es in nur einer Ebene Schwingen lassen. Damit könnten sich z.B. die vier Zustände

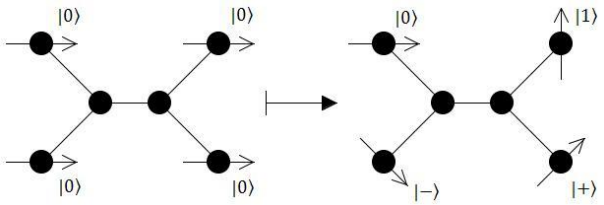
↔	↕	↗	↘
$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$

(Abbildung 8: Schwingungsebenen zeigen den Zustand an)

ergeben, wobei die Pfeile in Abbildung 8 die Schwingungsebene anzeigen. Ein Polarisationsstrahlteiler z.B. ein Kalkspatkristall lässt nur Photonen mit einer Schwingung, die gleich seiner Ausrichtungsebene ist hindurch. Durch zwei Detektoren, die messen ob das Photon durchkam oder abgelenkt wurde, kann man die Information extrahieren.

9.2.Kernspinresonanz

Ein Fluorkohlenstoff-Molekül mit sechs Atomen kann für die Realisierung von vier Qubits verwendet werden. Die Kernspinresonanz [Ger97] entsteht durch Wechselwirkung von Atomkernen mit Magnetfeldern. Der Spinn [5] der einzelnen Atome richtet sich, wie in Abbildung 9 zu sehen ist, parallel zum Magnetfeld aus. Durch elektromagnetische Wellen wird die Ausrichtung beeinflusst und die unterschiedlichen Zustände dargestellt.



(Abbildung 9: Moleküle deren äußere Atome Qubits realisieren)

9.3.Ionenfallen

Ionenfallen [Cir95] bestehen aus elektrisch aufgeladenen Molekülen oder Atomen. Sie werden in einem elektromagnetischen Feld innerhalb eines Vakuums festgehalten. Sie müssen stark gekühlt werden, nahe dem absoluten Nullpunkt, damit sie sich in Ruhe befinden und sich nicht durch die elektrische Aufladung gegenseitig abstoßen. Die Zustände unterscheiden sich durch ihre Energieniveaus, indem sie mit einem Laser beschossen werden und zusätzlich können verschiedene Schwingungsebenen genutzt werden. Auf die Weise kann ein Ion als zwei Qubits realisiert werden.

[5] Ein Spin ist eine Drehung um die eigene Achse.

10.Literaturverzeichnis

[Sho94] Shor, P. W. (1995), Algorithms for quantum computation: discrete logarithms and factorization, S. 124-134.

[Cam06] Camejo, S. A. (2006), Skurrile Quantenwelt, Berlin, Springer, S. 131-139.

[Cam062] Camejo, S. A. (2006), Skurrile Quantenwelt, Berlin, Springer, S. 159-165.

[Fli06] Fließbach, T. (2006), Allgemeine Relativitätstheorie, Heidelberg, Elsevier, Spektrum Akad. Verl., S. 41-68.

[Svo96] Svozil, K. (1996), Quantum information theory, Retrieved 01 19 2011 from http://www.jucs.org/jucs_2_5/quantum_information_theory/Svozil_K.pdf, S. 311-312

[Deu92] Deutsch, D. & Josza, R. (1992), Rapid solution of problems by quantum computation, London, S. 439-533.

[Gro96] Grover, L. K. (1996), A fost quantum mechanial algorithm for database search, Proc. of 28th Annual ACM Symposium on the Theory of Computing (STOC), S. 212-219.

[Hom08] Homeister, M. (2008), Quantum Computing verstehen, Wiesbaden, Vieweg, S. 146-153.

[BB84] Bennett, C. Brassard, G. (1984), Quantum cryptography: Public key distribution and coin tossing, In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, IEE Press, S. 175-179.

[Ben92] Bennett, Bessette, Brassard, Salvail, & Smolin. (1992), Experimental quantum cryptography, Journal of Cryptology, S. 3-28.

[Ger97] Gershenfeld, N. & Chuang, I. L. (1997), Bulk spin resonance quantum computation, Science, S. 275-350.

[Cir95] Cirac, J. I. & Zoller, P. (1995), Quantum Computations with Cold Trapped Ions, Innsbruck, Physical Review Letters, S. 4091-4094.