

Einführung in die Quantencomputik für Informatiker

Ingo Feinerer

18. Mai 2003

Kurzfassung

Basierend auf den Erkenntnissen von Eleanor Rieffel und Wolfgang Polak [10] beschäftigt sich dieser Artikel mit einer grundlegenden Einführung in die Welt der Quantencomputer. Es sollen Grundprinzipien vorgestellt, interessante Möglichkeiten der Technologie erläutert und in Einzelbereichen ein kurzer, aber etwas detaillierterer Eindruck vermittelt werden, wo jedoch der Schwerpunkt auf Themenbereiche der Informatik gelegt wird. Als Ergebnis soll dem geneigten Leser ein leicht zu lesender Einführungsartikel zur Verfügung stehen, der die Möglichkeiten zur weiteren Vertiefung in die Materie bildet.

Einleitung

In der Zeit immer schneller werdender Computer und auf der Suche nach neuen Möglichkeiten will dieser Artikel eine Übersicht darlegen, da bei weiteren erfolgversprechenden Ergebnissen der Quantencomputik Quantencomputer einen immer wichtigeren Schwerpunkt der Forschung belegen werden. Im wesentlichen beschäftigt sich dieser Artikel mit zwei Punkten: Quantenmechanik und Quantum Bits. So wird eine Einführung in die Quantenmechanik gegeben, die die Grundlage des Verständnisses für weitere Aspekte bildet. Diese Grundverhalte sollen mit der Beschreibung eines Experimentes der Photon Polarization verdeutlicht werden. Hierzu wird die Bra/Ket Notation vorgestellt. Folgend werden Quantum Bits definiert und deren Anwendungsbereiche Quantum Key Distribution, Multiple Qubits, das Problem der Messung (measurement) und das Einstein/Podolsky/Rosen (EPR) Paradoxon behandelt.

Der Themenbereich über Quantum Key Distribution wird ausführlicher behandelt, weil hier auf die Arbeiten von Charles Bennett et al. [3] in einem umfassenden Überblick eingegangen wird.

Quantenmechanik

Das Photon Polarization Experiment

Um einen Einstieg in die Materie zu gewähren, bietet sich ein einfaches Experiment an: Im Wesentlichen beruht es auf dem Fakt, dass Photonen die einzigen Teilchen sind, die wir direkt beobachten können. So reichen für den Versuchsaufbau ein helle und starke Lichtquelle und drei Polarisationsfilter (polarization filters/polaroids). Als Lichtquelle verwenden wir einen Laser, hinzu benennen wir die drei Polarisationsfilter als Filter A, B und C. Filter

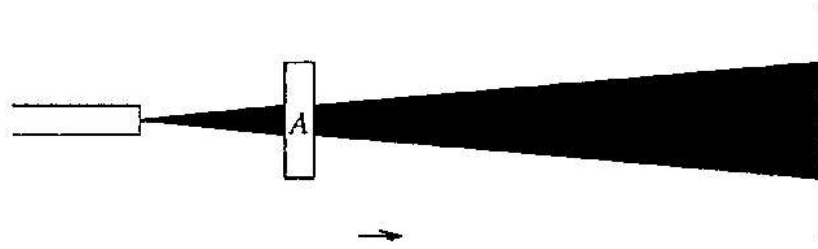


Abbildung 1: Laser mit Filter A

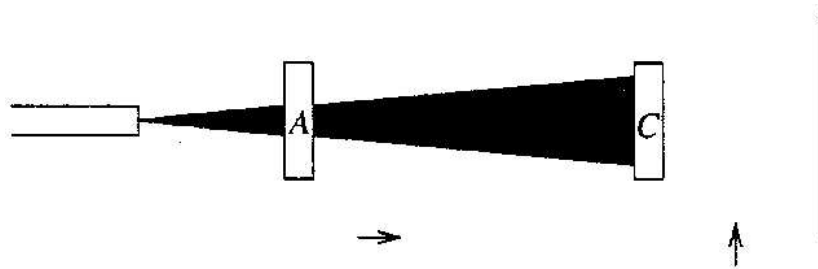


Abbildung 2: Laser mit Filter A und Filter C

A ist horizontal polarisiert, Filter B mit 45° und Filter C ist vertikal polarisiert. Zuerst projizieren wir den Laser auf eine Leinwand. Jetzt wird Filter A eingesetzt (Abbildung 1). Dies bewirkt, sofern der Laser zufällig polarisiert ist, eine Reduktion des ankommenden Lichtkegels um die Hälfte und das Ergebnis, dass alle angekommenen Photonen horizontal polarisiert sind. Fügt man nun Filter C hinzu, verschwindet der Lichtstrahl zur Gänze (Abbildung 2). Ergänzt man das Experiment mit Filter B, zeigt sich jedoch ein schwacher Strahl mit einer Intensität von genau einem Achtel des ursprünglichen Lasers, was nicht aus dem bisherigen Versuchshergang zu schließen war (Abbildung 3).

Versuchen wir uns als Erklärung gleich einer Definition: Die Polaris-

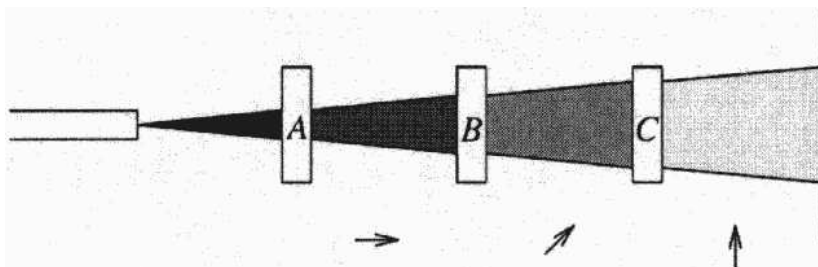


Abbildung 3: Laser mit Filter A, Filter B und Filter C

tion eines Photons kann als Einheitsvektor, der in die jeweilige Richtung zeigt, modelliert werden. Jede beliebige Richtung kann als Linearkombination $a|\uparrow\rangle + b|\rightarrow\rangle$ dargestellt werden. Die zugrunde liegende Basis ist irrelevant, solange die beiden Einheitsvektoren orthogonal zueinander stehen. Es reicht die Einheitsvektoren zu verwenden, weil die Stärke unbedeutend ist, id est $|a|^2 + |b|^2 = 1$. Bei der Messung wird der Zustand $a|\uparrow\rangle + b|\rightarrow\rangle$ mit der Wahrscheinlichkeit von $|a|^2$ als $|\uparrow\rangle$ wiedergegeben, als $|\rightarrow\rangle$ mit der Wahrscheinlichkeit von $|b|^2$. So lässt sich auch das Experiment nachvollziehen. Durch Filter A werden alle horizontal polarisierten Photonen durchgelassen, was im Durchschnitt 50% beträgt. Alle Photonen sind nun $|\rightarrow\rangle$, was gleichbedeutend mit $0|\uparrow\rangle + 1|\rightarrow\rangle$ ist. Bei Filter C werden keine Teilchen durchgelassen, weil sie mit Wahrscheinlichkeit 0 als $|\uparrow\rangle$ erkannt werden. Filter B jedoch misst 50% als $|\nearrow\rangle$ mit der Wahrscheinlichkeit $\frac{1}{2}$. Alle durchgelassenen Photonen sind nun $|\nearrow\rangle$. Filter C nimmt davon wieder 50% mit der Wahrscheinlichkeit $\frac{1}{2}$ als $|\uparrow\rangle$ wahr, was insgesamt dem Versuchsausgang von $\frac{1}{8}$ entspricht.

Bra/Ket Notation

Zustände und Rechnungen von bzw. mit Quanten können entweder mit Vektoren und/oder Matrizen oder auch mit der bra/ket Notation beschrieben werden [5]. Kets, gekennzeichnet durch $|x\rangle$, stellen einen Spaltenvektor dar. Das Gegenstück hierzu, ein sogenanntes Bra entspricht $\langle x|$. Ein Bra stellt den zu $|x\rangle$ konjugierten transponierten Vektor dar. Kombiniert man $\langle x|$ und $|y\rangle$, geschrieben als $\langle x|y\rangle$, so ist damit das innere Produkt dieser beiden Vektoren gemeint.

Zur einfachen Visualisierung von Transformationen hat sich eine derartige Notation erprobt:

$$X : |0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$$

Dies beschreibt eine Transformation X, die $|0\rangle$ und $|1\rangle$ austauscht auf eine sehr intuitive Weise.

Quantum Bits

Ein quantum bit, auch qubit genannt, ist ein Einheitsvektor in einem 2-dimensionalen komplexen Vektorraum, für den eine Basis in der Form $\{|0\rangle, |1\rangle\}$ festgelegt wurde. Wichtig ist nur, dass die Basis orthonormal ist, ansonsten ist sie frei wählbar. So könnte statt dem Paar $\{|0\rangle, |1\rangle\}$ durchaus $\{|\nearrow\rangle, |\nwarrow\rangle\}$ oder auch $\{|\uparrow\rangle, |\rightarrow\rangle\}$ als Repräsentation ihre Verwendung finden. Wie in der Informatik gängig wird jedoch meist die 0/1 Schreibweise verwendet, was den Eindruck von konventionellen Bits widerspiegelt. Hierbei muss jedoch

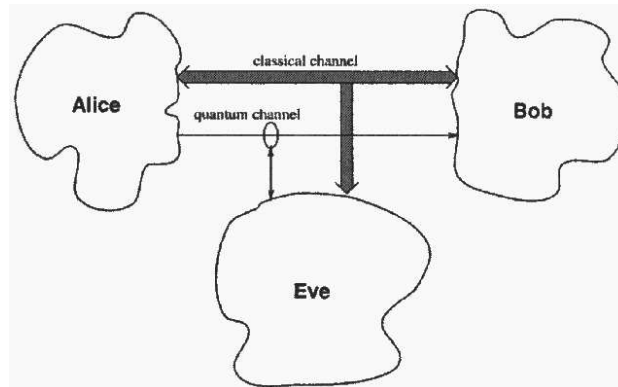


Abbildung 4: Quantum Key Distribution Versuchsaufbau

ganz klar betont werden, dass qubits auch in einer sogenannten Superposition (superposition) von $|0\rangle$ und $|1\rangle$ sein können, wenn man die Definition aus dem Kapitel Das Photon Polarization Experiment beachtet. So kann sich das qubit in einer beliebigen Kombination aus $a|0\rangle + b|1\rangle$ befinden, mit der Einschränkung, dass $|a|^2 + |b|^2 = 1$ gelten muss, wobei a und b komplexe Zahlen sind. Analog zum Photon Polarization Experiment gilt: $|0\rangle$ wird mit einer Wahrscheinlichkeit von $|a|^2$ gemessen, $|1\rangle$ mit der Wahrscheinlichkeit von $|b|^2$ gemessen.

Dennoch ist zu beachten, dass man nur eine Information pro qubit erhalten kann, obwohl sich ein qubit in einer theoretisch unendlich großen Vielfalt an Möglichkeiten von Superpositionen befinden kann. Das Problem ist die Messung, da sich die Information nur aufgrund jener aus dem qubit extrahieren lässt. Eine derartige Messung liefert nur eine Information, gewichtet nach den Wahrscheinlichkeiten der zugrundeliegenden Linearkombination. Hinzu kommt, dass bei jeder Messung der Originalzustand zerstört wird und somit kein öfteres Auslesen möglich ist.

Quantum Key Distribution

Mittels mehreren einzelnen Qubits ist es möglich private Schlüssel über nicht gesicherte Kanäle zu übertragen. Dies soll an einem Beispiel illustriert werden: Angenommen Alice und Bob wollen sich auf einen geheimen Schlüssel einigen, um danach sicher kommunizieren zu können. Verbunden seien sie über einen bidirektionalen offenen Kanal und einen einseitigen, also unidirektionalen Quantenkanal. Beide Kanäle können von einer dritten Person, nennen wir sie Eve, abgehört werden (Abbildung 4). Alice kann nun über den Quantenkanal Photonen zu Bob schicken, der dann deren Zustand messen kann.

1.	↺	↑	↻	↔	↑	↑	↔	↔	↻	↺	↑	↻	↺	↺	↑
2.	+	○	○	+	+	○	○	+	○	+	○	○	○	○	+
3.	↑		↻		↑	↺	↺	↔		↑	↻	↻		↺	↑
4.	+		○		+	○	○	+		+	○	○		○	+
5.			✓		✓			✓				✓		✓	✓
6.			↻		↑			↔				↻		↺	↑
7.			1		1			0				1		0	1

Abbildung 5: Bennetts Protokoll

Eve hat die nötige Ausstattung und kann nun versuchen das Teilchen abzufangen, zu messen und danach an Bob weiterzuschicken. Alice beginnt nun eine Sequenz von Bits zu Bob zu senden, wobei sie die einzelnen qubits nach folgendem Schema kodiert: Für jedes Bit nimmt Alice zur Kodierung eine der zwei Basen:

$$0 \rightarrow |\uparrow\rangle, 1 \rightarrow |\rightarrow\rangle$$

oder

$$0 \rightarrow |\swarrow\rangle, 1 \rightarrow |\nearrow\rangle.$$

Bob misst jetzt den Zustand der Photonen, indem er zufällig jeweils eine der zwei Basen auswählt. Sobald alles fertig übertragen wurde, schicken sich Bob und Alice über den offenen Kanal die Basis, die sie fürs Kodieren bzw. fürs Dekodieren verwendet haben. Durch diese Information können sie bestimmen, welche Bits richtig übertragen wurden. Das sind nämlich die Bits, für die die Basen von Bob und Alice übereinstimmen. Genau jene Bits verwenden sie als Schlüssel. Wichtig anzumerken ist, dass die beiden sich auf im Durchschnitt 50% aller geschickten Bits einigen. Sobald Eve versucht ein Photon zu messen, wird sie mit einer Wahrscheinlichkeit von $\frac{1}{2}$ eine falsche Basis verwenden. Dadurch wird Eve auch die Daten mit der falschen Basis an Bob weiterleiten, was eine hohe Fehlerrate verursacht. Alice und Bob müssen nun von einer Person, die den Datenverkehr abhört, ausgehen.

Im Vergleich zu der zugrundeliegenden Arbeit von Rieffel/Polak [10] soll im Rahmen dieses Artikels noch auf die Sichtweise von Charles Bennett et al. [3] eingegangen werden. Bennetts quantum key distribution Protokoll verwendet zwei konjugierte (conjugate) Basen, wobei er einerseits eine geradlinige (rectilinear) Basis (also horizontale vs vertikale Polarisation) und andererseits eine kreisförmige (circular) (also left-circular vs right-circular) verwendet. Diese benennt er kanonische Basen (canonical bases). 2 Basen heißen konjugiert in diesem Zusammenhang, wenn die Messung einer Basis eines Photons die anderen komplett willkürlich anordnet. Eine kanonische Polari-

sation ist dann per definitionem nach Bennett entweder horizontal, vertikal, left-circular oder right-circular.

Eine wichtige Anmerkung von Bennett ist, dass das Protokoll, das sowohl Rieffel/Polak als auch er verwenden, sogar sicher ist gegen einen Gegner, der unbegrenzte Rechenkraft (also sogar wenn $\mathcal{P} = \mathcal{NP}$ gelten würde) besitzt.

Analog zu Rieffel/Polak wollen wieder Alice und Bob sich auf einen geheimen Schlüssel einigen, den sie später für eine gesicherte Kommunikation nutzen können. Dazu sendet Alice eine beliebige Folge von Photonen, die entweder horizontal (\leftrightarrow), vertikal (\updownarrow), right-circular oder left-circular polarisiert sind (Abbildung 5 Schritt 1). Bob misst unabhängig die Polarisation der Photonen nach dem Zufallsprinzip, indem er entweder die geradlinige (+) oder die kreisförmige (\circ) Basis verwendet, natürlich ohne Abstimmung mit Alice, weil er ja zu diesem Zeitpunkt die von ihr gesendeten Photonen nicht kennt (Schritt 2). Dabei kann es vorkommen, dass manche Photonen überhaupt nicht ankommen und somit nicht gemessen werden (Schritt 3).

Dies ist ein wesentlicher Unterschied zu Rieffel/Polak, bei denen das Protokoll unter Idealbedingungen arbeitet, wo grundsätzlich immer alles ankommt und auch keine Messfehler entstehen. Bennett sieht dies von einem realistischeren Standpunkt, indem er auch auf physikalische Messgeräte, Fehler etc. achtet. Rieffel/Polak können dies jedoch leicht rechtfertigen, da ihr Artikel als Einführung von für das Verständnis der Materie selbst unwichtigen Details abstrahiert.

Bob teilt nun Alice mit, welche Basis er für jedes Photon, das er erhalten hat, benutzt hat (Schritt 4). Alice muss ihm darauf antworten, welche seiner Basen korrekt waren, das heißt welche Basen bei Bob und Alice übereingestimmt haben (Schritt 5). Beide dieser Tätigkeiten sind öffentlich, das heißt eine dritte Person, nennen wir sie Eve wie bei Rieffel/Polak, kann diese Informationen leicht abhören.

An dieser Stelle macht Bennett eine fundamentale Anmerkung, die bei Rieffel/Polak nur implizit in deren Artikel angenommen wird: Eve darf diesen öffentliche Kanal nur abhören, jedoch darf sie keinesfalls Informationen ändern können, weil sonst eine Man-in-the-middle-attack leicht zum Erfolg führen könnte. So könnte Eve Bob vortäuschen, sie wäre Alice, und Alice vortäuschen, sie wäre Bob, womit dieses Verfahren nutzlos wäre.

Bob und Alice verwenden diese Photonen, bei denen die Basen übereingestimmt haben (Schritt 6), und ordnen den Basen horizontal und left-circular 0 zu, und ordnen vertikal und right-circular 1 zu (Schritt 7). Somit haben sie einen Schlüssel bestimmt. Die restlichen Bits können verworfen werden, da sie nicht mehr gebraucht werden. Wie bei Rieffel/Polak können sich Alice und Bob das Problem der Messung zu Nutze machen, da Eve bei etwaigen Abhörversuchen durch die Messung eine Reihe von Basen falsch polarisiert.

Die beiden können nun wieder Abhörversuche feststellen, sobald sie sich nicht im Durchschnitt auf 50% der gesendeten Daten einigen.

Multiple Qubits

Einer der erstaunlichen Tatsachen ist der Fakt, dass ein Quantensystem, welches aus mehreren Teilchen besteht, nicht immer aus einer Sicht von einzelnen Teilchen betrachten werden kann, um quasi aus den einzelnen Komponenten ein ganzheitliches System zu konstruieren. Die Größe des Zustandsraums eines Quantensystems mit n Qubits hat 2^n Dimensionen — genau dieses exponentielle Wachstum des Zustandsraums legt auch eine mögliche exponentielle Beschleunigung der Rechenzeit auf Quantencomputer im Vergleich zu herkömmlichen Computern nahe.

Normalerweise errechnet sich der Zustandsraum von n Teilchen über ein kartesisches Produkt. Der Zustandsraum von Quanten muss jedoch über ein Tensorprodukt berechnet werden. Es sollen nun die wesentlichen Unterschiede zwischen dem kartesischen und dem Tensorprodukt, die für den Bereich der Quantencomputer relevant sind, verglichen werden.

Seien V und W zwei zwei-dimensionale komplexe Vektorräume mit der Basis $\{v_1, v_2\}$ beziehungsweise $\{w_1, w_2\}$. Das kartesische Produkt ist dann $\{v_1, v_2, w_1, w_2\}$. Anzumerken ist, dass die Dimension des Zustandsraum von mehreren Teilchen beim kartesischen Produkt linear anwächst, das heißt $\dim(X \times Y) = \dim(X) + \dim(Y)$. Das Tensorprodukt von V und W hat folgende Basis: $\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\}$. So kann festgestellt werden, dass ein System aus n Qubits 2^n Basisvektoren besitzt, was einem exponentiellen Wachstum entspricht. Die Dimension eines Tensorprodukts $X \otimes Y$ ist daher $\dim(X) \times \dim(Y)$.

Wie im ersten Satz dieses Kapitels angedeutet, gibt es Zustände, die nicht durch die Zustände der einzelnen Komponenten beschrieben werden können. Ein Beispiel hierfür ist $|00\rangle + |11\rangle$. So kann man keine a_1, a_2, b_1, b_2 finden sodass $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$ gilt. Derartige Zustände, die nicht zerlegt werden können, nennt man verschränkte Zustände (entangled states).

Das Problem der Messung

Bereits der Versuch im Kapitel "Das Photon Polarization Experiment" zeigte, wie das Ergebnis von dem verwendeten Messgerät abhängt, weil der Zustand des qubits auf eine der Basen des Messgeräts mit einer gewissen Wahrscheinlichkeit abgebildet wird. Hinzu kommt, dass durch jede Messung der Zustand

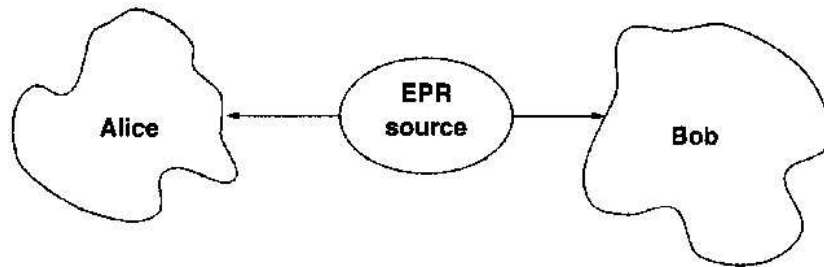


Abbildung 6: Alice, Bob und eine EPR-Quelle

des qubits verändert wird. So kann nicht etwa durch Kopieren oder wiederholtes Messen eine Lösung gefunden werden. Eine mögliche Vorgehensweise soll auf einem 2-qubit-System erläutert werden.

Bei einem System bestehend aus nur 2 qubits kann jeder Zustand als $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ beschrieben werden, wobei gilt dass $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. Will man nun das erste qubit mit der Standardbasis $\{|0\rangle, |1\rangle\}$ messen, ist folgende Umformung angebracht:

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = u|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right) + v|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right)$$

Für $u = \sqrt{|a|^2 + |b|^2}$ und $v = \sqrt{|c|^2 + |d|^2}$ sind $\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle$ und $\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle$ von der Einheitslänge. Die Messung für das erste Bit wird entweder mit der Wahrscheinlichkeit $u^2 = |a|^2 + |b|^2$ $|0\rangle$ zurückliefern oder mit der Wahrscheinlichkeit $v^2 = |c|^2 + |d|^2$ $|1\rangle$ liefern. Im ersteren Fall wird der Zustand des Systems nach der Messung auf $|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right)$ abgebildet, im zweiten auf $|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right)$.

Das Messen eines Systems mit mehreren Bits kann als Folge von Messungen der einzelnen Bits bewerkstelligt werden.

Hinzufügend kann man noch anmerken, dass die Messung auch eine alternative Definition der verschränkten Teilchen, wie sie im Kapitel Multiple Qubits erwähnt wurden, liefert. So gelten Teilchen als nicht verschränkt, wenn eine Messung einzelner Teilchen keinen Einfluss auf die restlichen Teilchen hat. Trifft dies zu, so spricht man von verschränkten Teilchen.

Das EPR Paradoxon

Einstein, Podolsky und Rosen [7] beschäftigten sich im Rahmen eines Gedankenexperiments 1935 mit einem Paradoxon: Gegeben sei eine Energiequelle, die zwei maximal verschränkte Teilchen $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, ein sogenanntes EPR-Paar, ausstrahlt (Abbildung 6). Jeweils eines wird an Alice und Bob

gesandt, wobei die zwei beliebig weit auseinander sein können. Angenommen Alice misst ihr Partikel und erhält $|0\rangle$. Das impliziert, dass der kombinierte Zustand nun $|00\rangle$ ist. Wenn Bob nun sein Partikel misst, erhält er ebenfalls $|0\rangle$. Dasselbe gilt für $|1\rangle$. Dies gilt immer und unabhängig wie weit die beiden auseinander sind. Im ersten Moment wirkt dies, als wäre eine Kommunikation schneller als das Licht möglich. Es gibt zwei Theorien, wie viele Personen meinen sich das erklären zu können, die sind beide aber inkorrekt und führen leicht zu Missverständnissen. Deshalb sollen sie genauer behandelt werden.

Einstein, Podolsky und Rosen stellten sich vor, dass jedes Teilchen eine internen Zustand hat, der ganz und vollständig bestimmt, wie das Ergebnis einer jeden Messung sein wird. Für den Betrachter ist dieser Zustand jedoch unsichtbar und kann nur durch Wahrscheinlichkeitsvorhersagen erörtert werden. Diese Theorie wurde unter dem Namen "local hidden variable theory" bekannt. In dem genannten Experiment seien eben beide Zustände jeweils auf $|0\rangle$ bzw. auf $|1\rangle$ gesetzt. John Bell [1] konnte jedoch im Jahre 1964 durch sein "inequality principle" beweisen, dass diese Theorie nicht möglich war.

Die zweite Theorie beruht auf dem Prinzip von Ursache und Wirkung. So könne die eine Messung von Bob eine Auswirkung auf die andere Messung von Alice haben, was zur Kommunikation zwischen den beiden benutzt werden könne. Eine derartige Theorie steht aber im strikten Widerspruch zu Einsteins Relativitätstheorie [6].

Das Ergebnis der Versuchs kann derart erklärt werden, dass Bob zuerst misst und eine Veränderung im Teilchen von Alice verursacht, und gleichzeitig Alice zuerst misst und eine Veränderung im Teilchen von Bob hervorruft. Dies wiederum zeigt, dass die beiden das EPR Paar nicht zur Kommunikation verwenden können, was das Paradoxon auflöst, nach dem Kommunikation schneller als Licht möglich gewesen wäre.

Verwandte Arbeiten

In diesem Abschnitt soll vermehrt auf Arbeiten, die mit diesem Artikel inhaltlich verwandt beziehungsweise als weiterführende Literatur vorhanden sind, eingegangen werden.

So ist hier etwa "Quantum Computing" von Andrew Steane [11] zu nennen. Der Artikel zielt zwar auf Physiker ab, dennoch ist die Sicht auf dieses Thema von Andrew Steane auch für interessierte Informatiker lesenswert. Etwa beschreibt er Verbindungen zwischen der Informationstheorie und dem Bereich Quantencomputer. Hinzu kommen auch die Erörterungen über die Fehlerkorrektur, wo er einer der wichtigsten Entwickler war. Hinzu gewährt er dem Leser einen Überblick über die physikalischen Schwerpunkte, die zum

Bau eines Quantencomputers relevant sind, wozu er Untersuchungen führt, was bis zum Jahr 1997 bereits alles getan wurde. Sein Artikel beinhaltet eine detaillierte geschichtliche Aufzählung über die Ideen bezogen auf die Quantencomputer.

Charles Bennett et al. [2] gehen in "Strengths and weaknesses of quantum computing" der Frage nach, inwieweit Quantencomputern klassischen Computern in der Rechenleistung überlegen sind und ob und wie gut Quantencomputer ihre Vorteile bei \mathcal{NP} Problemen nutzen können. Nach den Resultaten von Shor, der zeigte, dass die Faktorisierung in quantum polynomialer Zeit möglich ist, stellt er die Frage ob vielleicht auch alle \mathcal{NP} Probleme effizient gelöst werden könnten. In diesem Artikel zeigt er, dass die Klasse \mathcal{NP} nicht auf einer Quantum Turing Maschine (QTM) in unter $O(2^{n/2})$ lösbar ist.

"Quantum Computation" von André Berthiaume [4] ist eine kurze und eine sehr lesenswerte Literatur, die kurz eine Einführung in die Welt der Quantencomputer gibt. Er gibt einen Überblick über ein paar wenige Ergebnisse der Forschung über Quantencomputer, unter anderem auch den Faktorisierungsalgorithmus von Shor.

Einen gerade zu diesem vorliegenden Artikel sehr passender Artikel ist "Experimental Quantum Cryptography" von Charles Bennett et al. [3], da in diesem vorliegenden Artikel im Abschnitt Quantum Key Distribution auch auf Teile davon eingegangen wurde, indem er mit der Arbeit von Eleanor Rieffel und Wolfgang Polak [10], auf den sich diese Arbeit wesentlich stützt, verglichen wurde. In Bennetts Artikel werden physikalische Geräte und Protokolle vorgestellt, um damit Quantum Key Distribution zu implementieren.

Schließlich soll noch auf Richard Feynmans "Lectures on Computation" hingewiesen werden [9], das einen "reprint" von dem Artikel "Quantum Mechanical Computers" [8] beinhaltet. Dieser Artikel gilt als die Begründung des ganzen Forschungsgebiets. So wird über die Thermodynamik der Berechnungen diskutiert, was sehr eng mit dem Gebiet der reversible Computerberechnungen und der Informationstheorie selbst verknüpft ist.

Fast als eigener Punkt muss der Artikel "An Introduction to Quantum Computing for Non-Physicists" von Eleanor Rieffel und Wolfgang Polak [10] bezeichnet werden. Wie bereits zuvor erwähnt, wäre dieser vorliegende Artikel nie ohne der Grundlage deren Arbeit entstanden. Gerade die zweite Hälfte deren Arbeit findet keinen relevanten Niederschlag in diesem vorliegenden Artikel und ist deshalb speziell geeignet, für den interessierten Leser als weitere Literatur empfohlen zu werden.

Zusammenfassung

Der Bereich der Quantencomputer ist ein Gebiet, das das Potential hat, die jetzigen Ansichten über Computer, Rechenverfahren und Komplexitätstheorie zu revolutionieren. Jedoch stecken die Quantencomputer noch in ihren Kinderschuhen und stellen ein riesiges und erfolgsversprechendes Forschungsgebiet dar.

So wurde in diesem Artikel versucht, einen ersten Kontakt mit diesem interessantem und zugleich neuem Teilaspekt der Informatik zu knüpfen. Nach einem ersten in die Materie einführenden Versuch "Das Photon Polarization Experiment" und dessen Erklärung wurde die Bra/Ket Notation von Dirac [5] vorgestellt, die sich als die Standardschreibweise in Bereich der Quantenmechanik etabliert hat. Danach wurde der Schwerpunkt auf Quantum Bits gelegt, wo auch ausführlicher die Problemstellung der Quantum Key Distribution diskutiert wurde. Zu diesem Thema haben etwa Bennett et al. weitaus ausführlichere Abhandlungen [3] geschrieben, die für den interessierten Leser weitere Literatur bilden.

Darauf folgend wurden Multiple Qubits genauer betrachtet, ein Abschnitt der für die Quantencomputik sehr wichtig ist, weil er einen ersten Eindruck liefert, was vielleicht mit Quantensystemen mit ihrem exponentiellen Zustandsraum in Zukunft alles möglich sein wird. Danach wurde noch kurz auf das Problem der Messung eingegangen, um kritische Aspekte zu erwähnen und grob zu erklären, wie man bei einer Messung von mehreren Qubits vorgehen kann, um eine vernünftige Messung zu bewerkstelligen.

Als Abschluss wurde das EPR-Paradoxon [7] betrachtet, dessen verblüffenden Ergebnisse auch wesentliche Grundlagen für Annahmen der weiteren Forschung auf dem Gebiet der Quantencomputer bildeten.

Literatur

- [1] J. S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, 1964. In 1964 stellte John Bell eine Theorie auf, mit der man nach der Existenz von "local hidden variables" testen kann. Darauf aufbauend entwickelte er sein "inequality principle", womit er zeigte, dass die "local hidden variable" Theorie nicht haltbar war.
- [2] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *Society for Industrial and Applied Mathematics Journal on Computing*, 26:1510–1523, 1997. Bennett et al. gehen der Frage nach, inwieweit Quantencomputer klassischen Computern in der Rechenleistung überlegen sind und ob

und wie gut Quantencomputer ihre Vorteile bei \mathcal{NP} Problemen nutzen können.

- [3] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Lecture Notes in Computer Science*, 473:253–265, Sep 1991. Bennett et al. beschreiben in diesem Artikel ein Gerät und Protokoll, um damit quantum key distribution zu implementieren.
- [4] André Berthiaume. *Quantum Computation*. Springer-Verlag, also to appear in Complexity Theory Retrospective II, 1996. Eine Einführung in die Welt der Quantencomputer.
- [5] Paul Adrien Maurice Dirac. *The Principles of Quantum Mechanics*. Oxford University Press, 4th edition, 1958. Dirac stellt seine Bra/Ket Notation vor.
- [6] A. Einstein. *Relativity: The Special and General Theory*. Methuen & Co Ltd, December 1964. Albert Einsteins grundlegende Überlegungen und Erkenntnisse über die Relativitätstheorie, wie sie von fundamentaler Bedeutung für die Physik waren.
- [7] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935. In diesem 1935 mit Podolsky und Rosen verfassten Artikel Can Quantum-Mechanical Description of Physical Reality be Considered Complete? führt Albert Einstein ein Gedankenexperiment über die Unzulänglichkeiten der Quantenmechanik.
- [8] Richard Feynman. Quantum mechanical computers. *Optics News*, 11:11–20, 1985. Feynman, quasi einer der "Erfinder" der Quantencomputer, beschreibt in diesem Artikel den Themenbereich über Quantencomputer.
- [9] A. J. Hey and R. W. Allen. *Feynman Lectures on Computation*. Addison-Wesley, 1996. Ein "reprint" Richard Feynmans Artikel "Quantum mechanical computers" aus dem Jahre 1985.
- [10] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32:300–335, Sep 2000. Die beiden Autoren geben eine Überblick über den Themenbereich der Quantencomputer. Hierzu wird der Leser stufenweise in die Materie eingeführt, indem ein Streifzug durch die wesentlichen Gebiete, die zum Verständnis notwendig sind, gegeben wird.

- [11] Andrew Steane. Quantum computing. *Reports on Progress in Physics*, 61:117–173, 1998. Dieser Artikel vereint Ideen der klassischen Informationstheorie, der Informatik und der Quantenphysik. Das Zielpublikum sind Physiker.