One Way Quantum Computer

Bakkalaureatsarbeit von
Michael F. KRENN

Betreuer: Univ.-Prof. Dr.rer.nat. Enrico ARRIGONI
Datum: 5. Dezember 2007

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Prolog

In dieser Bakkalaureatsarbeit wird das Konzept der theoretischen und praktischen Ausführung des 'One Way Quantum Computers' beschrieben. Die einführenden Kapitel geben jedoch vorerst einen Überblick über die Funktionalität des 'klassischen Computers' und des 'Quantencomputers', um die divergierenden Unterschiede ersichtlich darzustellen. Da die Verschränkung nicht nur eine grundlegende Eigenschaft der Quantenmechanik, sondern auch eine elementare Eigenschaft der Quantenrechnung - ohne die der Quantencomputer nicht effizienter als der klassische Computer sein kann - ist, soll im Zuge dieser Arbeit näher auf dieses physikalische Phänomen eingegangen werden. Die Arbeitsweise des 'One Way Quantum Computers' wird in weiterer Folge nicht nur durch die Beschreibung des Aufbaus, sondern auch durch die Angabe von Beispielen dargestellt. Das Kapitel 'Experimentalaufbau' weist auf die bis dato am häufigsten verwendeten praktischen Aufbauten hin und in 'Tomografie eines Quantenzustands' wird aufgezeigt, welche Mittel zur Überprüfung des Ausganges der Experimente möglich sind. Mit Anwendungen und einer kleinen Zukunftsaussicht schließt diese Arbeit.

An dieser Stelle möchte ich mich bei meinem Betreuer, Herrn Prof. Enrico Arrigoni herzlichst für die gute Zusammenarbeit bedanken.

2 Der klassische Computer

Der klassische Computer basiert auf der Booleschen Algebra, wobei die logischen Informationen aus Bits zusammengesetzt sind. Der Informationsinhalt eines solchen Bits wird aus 0 (nein) oder 1 (ja) gebildet. Physikalisch kann dieser zum Beispiel mit Hilfe einer Spannung oder einer magnetischen Ausrichtung beschrieben werden. Die Boolesche Algebra verwendet dazu die elementaren Operatoren NOT, AND und OR.

Der Operator NOT (Abb. 1) steht für die Invertierung der Eingangsvariable. Ist diese logisch 1 wird der Ausgang auf logisch 0 gesetzt (v.v.).

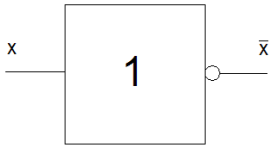


Abbildung 1: Symbolische Beschreibung eines NOT-Gatters

Sind beide Eingangsvariablen des Operators AND (Abb. 2) logisch 1 ergibt der logische Ausgang der Operation auch eine 1, ansonsten ist dieser stets 0.

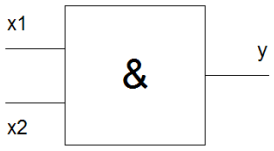


Abbildung 2: Symbolische Beschreibung eines AND-Gatters

Nun bleibt noch die Beschreibung des OR-Operators (Abb. 3) als dritter und letzter Elementaroperator der Booleschen Algebra. Sind hier beide Eingänge 0 gibt der Ausgang logisch 0 und sonst logisch 1.

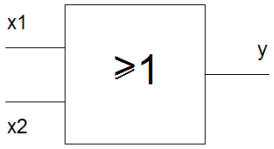


Abbildung 3: Symbolische Beschreibung eines OR-Gatters

Damit ist das Grundprinzip des klassischen Computers bereits beschrieben. Jede noch so komplexe Informationsverarbeitung kann durch eine Aneinanderschaltung der obigen Elementaroperatoren (Gatter) umgesetzt werden.

3 Der Quantencomputer

Im Gegensatz zum klassischen Computer treten in der Anwendung der Quantenmechanik nun nicht nur die Zustände [0,1] sondern auch deren Superposition auf. Dieser superponierte Zustand wird in der Quanteninformatik als Quantenbit oder kurz Qubit bezeichnet und mathematisch wie folgt beschrieben:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{mit} \qquad |\alpha|^2 + |\beta|^2 = 1: \quad \alpha, \beta \in \mathbb{C} \tag{1}$$

Genau dieser Umstand führt zur Stärke des Quantencomputers gegenüber dem klassischen Computer. Muß ein heutiger Computer der Reihe nach mit Eingaben gefüttert werden, kann der Quantencomputer mit der Überlagerung der Informationen Berechnungen gleichzeitig durchführen.

Die Darstellung eines Qubits erfolgt am anschaulichsten mit Hilfe der Bloch-Kugel (Abb.: 4).

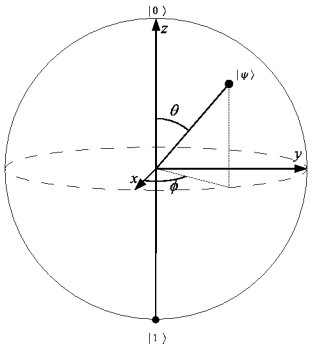


Abbildung 4: Bloch-Kugel mit dargestelltem Zustand ψ aus [1]

Dabei beschreibt der Nordpol der Bloch-Kugel den Zustand $|0\rangle$ und der Südpol den Zustand $|1\rangle$. Jeder andere Punkt auf der Oberfläche der Kugel bezeichnet eine komplexe Quantensuperposition von $|0\rangle$ und $|1\rangle$. Vielleicht auch besser ersichtlich durch die Zustandsschreibweise: $|\psi\rangle = e^{i\gamma}(cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle)$.
Physikalisch kann der Zustand $|0\rangle$ bzw. $|1\rangle$ z. B. durch unterschiedliche Polarisation oder durch den Grundzustand bzw. einen metastabilen Anregungszustand eines Ions realisiert werden. Man könnte nun meinen, dass der Informationsinhalt eines Qubits mit hinreichend genauer Längen-/Breitengrad-Beschreibung auf der Oberfläche der Bloch-Kugel ins Unendliche geht. Dies widerspricht jedoch der Quantenmechanik. Der Informationsgehalt eines Qubits kann erst durch eine Messung bestimmt werden, die mit einer bestimmten Wahrscheinlichkeit (je nach 'Breitengrad' auf der Bloch-Kugel) 0 oder 1 ergibt - also dem Informationsgehalt eines klassischen Bits entspricht. So ergibt, entgegen Einsteins Aussage 'Gott würfelt nicht', eine Messung (nach Gleichung 1) mit der Wahrscheinlichkeit $|\alpha|^2$: 0 und mit $|\beta|^2$: 1. Dabei muß die Summe der beiden Wahrscheinlichkeiten 1 ergeben.

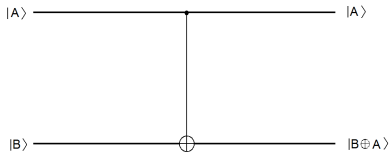
Zur Realisierung quantenmechanischer Operatoren, welche analoge Wirkungen der klassischen Elementaroperatoren aufzeigen, ist die Verwendung von zwei- oder mehrere-Qubit-Systemen entscheidend. Schwierigkeiten treten hier mit der Handhabung der Korrelation zwischen den Qubits auf, die für die Verwirklichung der Operatoren absolut notwendig ist, beispielsweise können Verschränkungen (siehe Kap. 4) nur in mehrere-Qubit-Systemen erzeugt werden.

In einem zwei-Qubit-System sieht eine Linearkombination wie folgt aus:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle^1 \qquad \sum_{x\in[0,1]^2} |\alpha_x|^2 = 1 \tag{2}$$

Die Messung des ersten Qubits ergibt 0 mit der Wahrscheinlichkeit $|\alpha_{00}|^2 + |\alpha_{01}|^2$. Die Zustände - auch 'computational basis states' - genannt spannen dabei wie in Gleichung 1 einen zweidimensionalen oder in Gleichung 2 einen vierdimensionalen Hilbertraum auf. Der Zustand eines zwei- bzw. höheren Qubit-Systems ist nicht mehr mit der anschaulichen Form der Bloch-Kugel darstellbar.

Um nun Operatoren analog zum klassischen Computer zu entwickeln soll beachtet werden, dass nur unitäre Zeitentwicklungsoperatoren verwendet werden können, damit sich die Norm von $|\psi\rangle$ zeitlich nicht ändert. Baut man den quantenmechanischen Operator analog zum klassischen Computer auf (z.B.: $AND = |0\rangle\langle 00| + |0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 11|$), würde sich durch die folgende Berechnung der Hilbertraum reduzieren und damit wäre der Prozess irreversibel.
Dieses Problem der Irreversibilität wurde von Tommaso Toffoli durch den nach ihm benannten Gatteraufbau gelöst. Für diesen Aufbau eines reversiblen AND-Gatters (TOFFOLI-Gatter) benötigt man das Konzept des C_{NOT}-'Controlled NOT'-Gatters. Hierbei handelt es sich um einen zwei-Qubit-Operator mit der Aufgabe, den zweiten Qubit nur dann zu invertieren, wenn der erste den Zustand 1 aufweist.

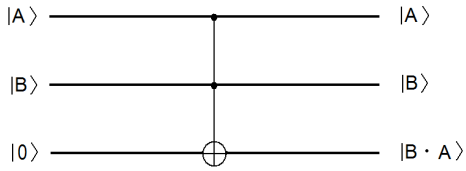


in	out
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Abbildung 5: Darstellung eines 'Controlled NOT'-Gatters

Dabei symbolisieren die Linien in quantenmechanischen Schaltungsdarstellungen so genannte 'wires'. Hierbei muß es sich nicht um klassische Drahtverbindungen handeln, sondern es kann auch einen Ortswechsel von quantenmechanischen Teilchen aufzeigen.

Mit Hilfe zweier Control-Qubits kann auf folgender Weise ein C^2_{NOT}-(Toffoli)-Gatter realisiert werden. Der C^2_{NOT}-Operator wirkend auf den dritten Zustand des drei-Qubit-Gatters, ändert nur dann diesen Zustand, wenn sowohl $|A\rangle$ als auch $|B\rangle$ den Zustand $|1\rangle$ aufweist. Ist der Eingangszustand es dritten Qubits mit $|0\rangle$ präpariert, erhält man das reversible, quantenmechanische AND-Gatter.



in	out
$\|000\rangle$	$\|000\rangle$
$\|010\rangle$	$\|010\rangle$
$\|100\rangle$	$\|100\rangle$
$\|110\rangle$	$\|111\rangle$

Abbildung 6: Darstellung eines quantenmechanischen AND-Gatters

[1] mehrere, hier zwei Qubits werden als Tensorprodukt $|ab\rangle = |a\rangle \otimes |b\rangle$ dargestellt, mit dem Skalarprodukt $\langle ab|a'b'\rangle = \delta_{a,a'}\delta_{b,b'}$

4 Verschränkung

Eine wichtige Eigenschaft der Quantenmechanik mit Verwendung im Quantencomputer und speziell im 'One Way Quantum Computer' ist die Verschränkung, eine Konsequenz aus dem Superpositionsprinzip. Zustände gelten als verschränkt, wenn der Gesamtzustand eines zusammengesetzten Systems nicht in Teilsysteme separiert werden kann, also wenn der Gesamtzustand z. B. zweier Systeme A, B mit den Hilberträumen H_A, H_B und dem zusammengesetzten System $H_A \otimes H_B$ nicht als $|\psi\rangle_A|\psi\rangle_B$ geschrieben werden kann.
Als berühmtes Beispiel soll an dieser Stelle die Messung eines verschränkten Zustandes von Alice und Bob (als Synonym für Sender und Empfänger einer Information) erklärt werden. Die Information besteht aus den Basisvektoren $(|0\rangle, |1\rangle)$ des jeweiligen Systems A und B. Daraus ergibt sich der verschränkte Gesamtzustand $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$. Alice soll hier die Beobachterin des Systems A und Bob der Beobachter des Systems B sein. Durch eine folgende Messung kann Alice mit gleicher Wahrscheinlichkeit 1 oder 0 als Ergebnis erhalten. Misst sie 1, kollabiert der Zustand zu: $|\psi\rangle = |1\rangle_A|0\rangle_B$, wodurch Bob als Messergebnis 0 erhalten muss. Ergibt Alice's Messung 0, reduziert sich der Zustand zu $|\psi\rangle = |0\rangle_A|1\rangle_B$ und Bob wird zugleich 1 als Messresultat erhalten.
Da das Messergebnis von Alice vollkommen zufällig ist, kann das Resultat von Bob nicht beeinflusst werden[2], womit keine Informationsübertragung stattfindet. Die Kausalität ist nicht verletzt [3] - die Information kann somit auch nicht schneller als Licht übertragen werden.
Die experimentelle Generierung von verschränkten Photonen (dessen Polarisation) erfolgt meist via 'parametric down-conversion' (genauere Beschreibung siehe Kapitel 5.4.1) oder durch Laseranregung bestimmter Atomarten, die bei Rückkehr in den Grundzustand verschränkte Photonen emittieren. Weiters können auch zweiatomige Moleküle mit Eigendrehimpuls S = 0 experimentell genutzt werden, indem man mittels Laser diese dissoziiert und damit zwei Atome mit verschränktem Spin ($S = +\frac{1}{2}$ bzw. $S = -\frac{1}{2}$) erhält.

Außer der Verwendung verschränkter Teilchen als Basis des Quantencomputers soll die Anwendung in Zukunft das sichere Austauschen von Schlüsseln in der Kryptografie zwischen zwei Kommunikationspartnern ermöglichen. Dabei[4] werten Alice und Bob verschränkte Photonen mittels Polarisationsfilter aus, die von Alice, Bob bzw. Charlie (einem dritten Glied in der Kommunikationskette) emittiert worden sind. Dies wird in gleicher Wahrscheinlichkeit mit horizontalen, vertikalen und diagonalen Polarisationsmessungen durchgeführt. Über einen ungesicherten Kanal werden anschließend die Filtereinstellungen ausgetauscht. Waren diese gleich, kennt jeder der beiden den Polarisationszustand des Photons seines Gegenübers. Die erhaltenen Bits können für die Kodierung verwendet werden. Waren jedoch die Filtereinstellungen verschieden, können diese Messungen zur Abschätzung der Bellschen-Ungleichung verwendet werden. Die Bellsche-Ungleichung geht von einem lokalen Realismus aus, womit besagt wird, dass physikalische Objekte von der Messung unabhängige, eindeutige Eigenschaften haben. Wird diese Ungleichung verletzt, waren die Photonen verschränkt. Wurde die Kommunikation durch einen Lauschangriff gestört, sind die Photonen nicht mehr verschränkt. Dieser Umstand wird bei der Auswertung der Bellschen-Ungleichung bemerkt und Gegenmaßnahmen, wie Übertragungskanal- und Schlüsselwechsel können eingeleitet werden (detailreiche Beschreibung unter [2]).

[2] Das verschränkte System wechselwirkt nicht über große räumliche Distanzen - vielmehr ist der Zustand des Systems nicht lokalisiert (Quanten-Nichtlokalität). Nach der 'Kopenhagener Interpretation' kommt es bei einer Messung zu einem instantanen Kollaps der Wellenfunktion, so verursacht die Messung von Alice am Ort von Bob einen Kollaps der Wellenfunktion und damit eine Art 'Fernwirkung'.

[3] die Zustände können auch nicht statistisch überprüft werden: No-Cloning-Theorem!

[4] von Artur Ekert (1991) beschriebenes Protokoll

5 One Way Quantum Computing

Die Idee eines 'One Way Quantum Computers (O.W.Q.C.)' von R. Raussendorf und H. Briegel [3] basiert auf die Verschränkung von Qubits, deren Gruppenzustand als 'cluster state' bezeichnet wird. Der unterliegende Algorithmus wird einzig durch die Einzel-Qubit-Messungen bestimmt, damit können durch unterschiedliche Messsequenzen mit ausreichender Gruppenzustandsgröße unterschiedliche Algorithmen realisiert werden. Womit alle Operationen eines herkömmlichen Quantencomputers auch mit einem O.W.Q.C. realisiert werden können. Durch die Korrelation wird die Information zwischen den Qubits 'weitergeleitet' (feedforward), wobei am letzten Qubit die Messung des Ergebnisses erfolgt.[5] Diese Art der Berechnung ist im Gegensatz zur unitären Entwicklung nicht zeit-reversibel, also 'one way'. Der Grund dafür ist die sequenzielle Zerstörung der Verschränkung, verursacht durch den Messeingriff.

5.1 Vergleich: 'Standard'/One-Way Quantum Computer

'Standard' Quantum Computer	One-Way Quantum Computer
Der Anfangszustand ist **nicht** verschränkt.	Unabhängig von der Art der Berechnung ist der Anfangszustand ('Cluster') stets '**maximal** verschränkt'.
Abhängig vom Problem, das berechnet werden muss, müssen verschiedene 1- und insbesondere 2-Qubit-Gates angewandt werden.	
Am Ende werden Messungen gemacht.	Lediglich Messungen müssen durchgeführt werden.

5.2 Clusterbildung

Um einen kurzen Einblick in die Verschränkung zu Clustern zu erhalten werden nachfolgend einige mathematische Beispiele gezeigt, wir folgen hier den Beschreibungen der Gruppe A. Zeilinger [4], worin in einem Experiment vier Qubits einen Cluster bildeten[6].
Zuerst werden die einzelnen Qubits in Superposition, also $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$[7] und danach mit dem CPhase-Gate in den verschränkten Zustand gebracht, mit:

$$\text{CPhase}|j\rangle|k\rangle \rightarrow (-1)^{jk}|j\rangle|k\rangle \qquad \text{mit } j,k \in 0,1 \ . \tag{3}$$

In der nachfolgenden Clusterdarstellung soll die Indizierung des Operators die Wirkung auf das jeweilige Qubit zeigen.

[5] Offen bleiben noch Fragen zum O.W.Q.C., ob Auswirkungen (Fehlertoleranzen) in realen Betriebsbedigungen (z.B. Rauschen) gegenüber dem Quantencomputer verstärkt auftreten.
[6] Im Labor wurde bis dato bereits ein Quantenbyte (8 Qubits) miteinander verschränkt.
[7] im Folgenden auch in Verwendung: $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- $$\begin{aligned}\underline{|\psi\rangle_2} &= \tfrac{1}{2}\cdot \mathbf{CPhase_{1,2}}(|\mathbf{0}\rangle + |\mathbf{1}\rangle)(|\mathbf{0}\rangle + |\mathbf{1}\rangle)\\ &= \tfrac{1}{2}\cdot(|0\rangle|0\rangle + |1\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|1\rangle)\\ &= \underline{|0\rangle|+\rangle + |1\rangle|-\rangle} \qquad \text{(2 Qubit-Cluster: 'Bell - state')}\end{aligned}$$

- $$\begin{aligned}\underline{|\psi\rangle_3} &= \tfrac{1}{\sqrt{2}}\tfrac{1}{2}\cdot \mathbf{CPhase_{2,3}}(|0\rangle|\mathbf{0}\rangle + |1\rangle|\mathbf{0}\rangle + |0\rangle|\mathbf{1}\rangle - |1\rangle|\mathbf{1}\rangle)(|\mathbf{0}\rangle + |\mathbf{1}\rangle)\\ &= \tfrac{1}{\sqrt{2}}\tfrac{1}{2}\cdot(|0\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle - |1\rangle|1\rangle|0\rangle + |0\rangle|0\rangle|1\rangle\\ &\quad -|0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|1\rangle)\\ &= \underline{|+\rangle|0\rangle|+\rangle + |-\rangle|1\rangle|-\rangle} \qquad \text{(3 Qubit-Cluster: 'GHZ}^8\text{ - state')}\end{aligned}$$

- $$\begin{aligned}\underline{|\psi\rangle_4} &= \tfrac{1}{2}\tfrac{1}{2}\cdot \mathbf{CPhase_{3,4}}(|0\rangle|0\rangle|\mathbf{0}\rangle + |0\rangle|1\rangle|\mathbf{0}\rangle + |1\rangle|0\rangle|\mathbf{0}\rangle - |1\rangle|1\rangle|\mathbf{0}\rangle\\ &\quad +|0\rangle|0\rangle|\mathbf{1}\rangle - |0\rangle|1\rangle|\mathbf{1}\rangle + |1\rangle|0\rangle|\mathbf{1}\rangle + |1\rangle|1\rangle|\mathbf{1}\rangle)(|\mathbf{0}\rangle + |\mathbf{1}\rangle)\\ &= \tfrac{1}{2}\tfrac{1}{2}\cdot(|0\rangle|0\rangle|0\rangle|0\rangle + |0\rangle|1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|0\rangle|0\rangle - |1\rangle|1\rangle|0\rangle|0\rangle\\ &\quad +|0\rangle|0\rangle|1\rangle|0\rangle - |0\rangle|1\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle|0\rangle\\ &\quad +|0\rangle|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle|1\rangle + |1\rangle|0\rangle|0\rangle|1\rangle - |1\rangle|1\rangle|0\rangle|1\rangle\\ &\quad -|0\rangle|0\rangle|1\rangle|1\rangle + |0\rangle|1\rangle|1\rangle|1\rangle - |1\rangle|0\rangle|1\rangle|1\rangle - |1\rangle|1\rangle|1\rangle|1\rangle)\\ &= \underline{|0\rangle|+\rangle|0\rangle|+\rangle + |0\rangle|-\rangle|1\rangle|-\rangle + |1\rangle|-\rangle|0\rangle|+\rangle + |1\rangle|+\rangle|1\rangle|-\rangle} \qquad \text{(4 Qubit-Cl.)}\end{aligned}$$

$$\vdots$$

In Abbildung 7 (linker Teil) folgt eine Übersicht über einige Clusterarten. Dabei handelt es sich bei a) und b) um eindimensionale (erzeugt durch 1-Qubit-Gatter), c), d) und e) hingegen zeigen zweidimensionale Cluster (erzeugt durch 2-Qubit-Gatter). Zur Realisierung dieser Cluster werden die Qubits stets auf $|0\rangle + |1\rangle$ präpariert und durch Anwendung des CPhase-Operator jeweils mit den durch einen Strich gekennzeichneten Nachbarqubit verschränkt, siehe Abbildung 7 (mitte).
Mit der Wahl der Clusterdimension und der miteinander verschränkten Qubits wird also auch die Basis für die folgende Messung (Algorithmus) fixiert. Die Erfolgsaussichten immer mehr Qubits miteinander zu verschränken sinken dabei mit steigender Anzahl und auch die 'Qualitätskontrollen' der Korrelationen (siehe Kapitel 5.5) nehmen immer größere Ausmaße an. Dies ist wohl auch der Grund, warum viele Forscher in der Welt der Physik behaupten, dass ein Quantencomputer innerhalb der nächsten 50 Jahre nicht in der Lage sein wird mehr als 100 Rechenschritte zu tätigen.
Diese Aussage ist für die Zukunft schwer einzuschätzen, als Gedankenanstoß möchte ich zwei ebenfalls pessimistische Einschätzungen aus anderen technologischen Errungenschaften unserer Zeit einfach nur in den Raum stellen, die sich heute als absolut falsch erwiesen haben. Aus dem Memo der Western Union Financial Services (1876):'... Dieses Telefon hat so viele Mängel, dass es nicht ernsthaft als Kommunikationsmittel taugt. Das Ding hat für uns an sich keinen Wert ...' und ein Zitat des Chairmans von IBM, Thomas J. Watson (1943): '... I think ther's a world market for about five computers ...'.

[8] GHZ-State: benannt nach den Physikern: Greenberger, Horne und Zeilinger

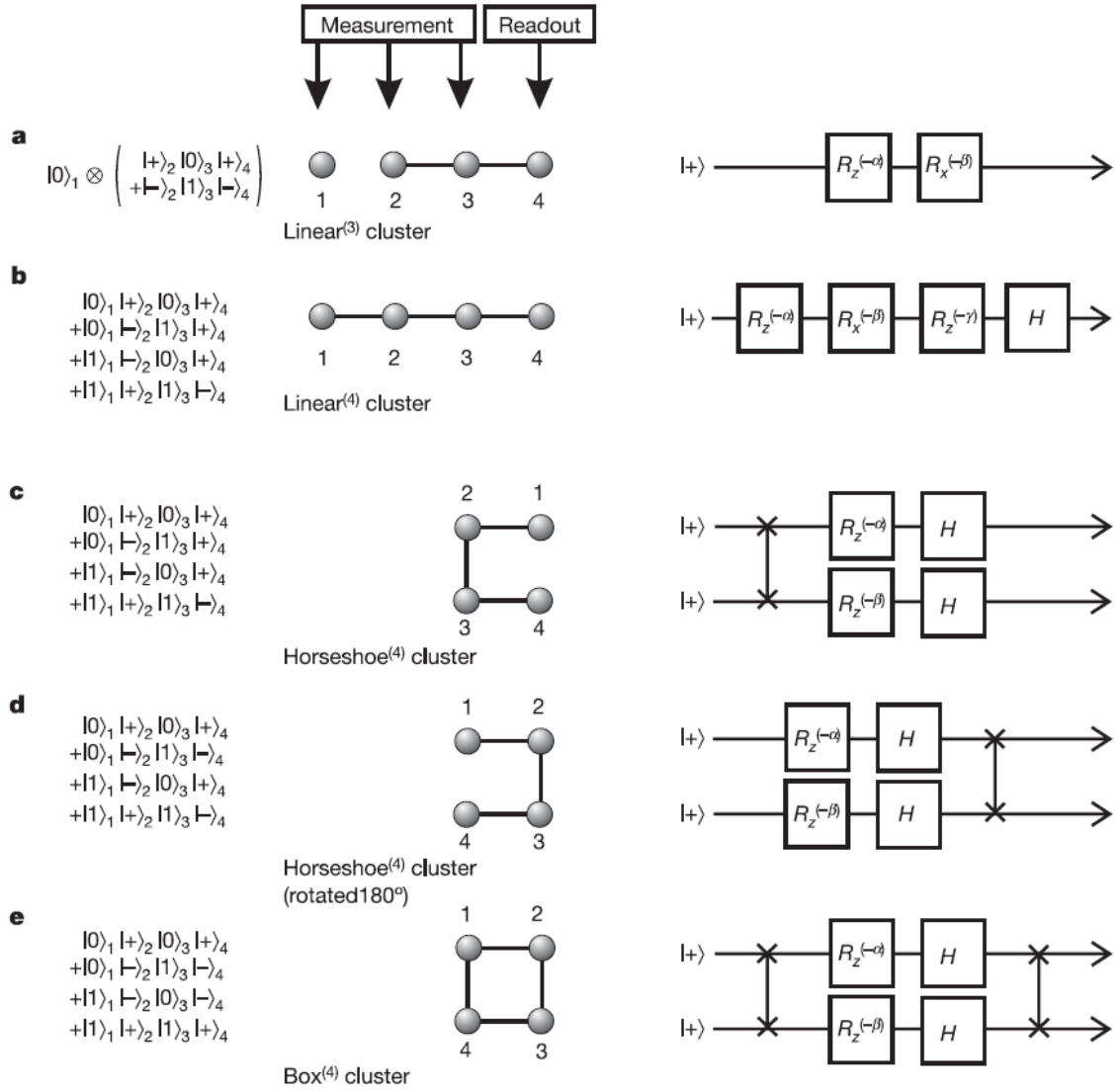


Abbildung 7: Eine Auflistung von einigen Cluster-Zuständen (aus [4] entnommen)

5.3 Realisierte Gates

Auf der rechten Seite der Abbildung 7 erfolgt eine Auflistung der Folge von Gates, die durch geeignete Messungen[9] realisiert werden, wobei $R_n(\theta)$ die Rotation des Zustandes beschreibt, mit:

$$R_n(\theta) \equiv e^{-i\theta\frac{\sigma_n}{2}} = cos\frac{\theta}{2}\ I - i\ sin\frac{\theta}{2}\ \sigma_n$$

mit σ_n den Paulimatrizen ($n \in x, y, z$) und H den Hadamard-Operator[10]

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

Das Hadamard-Gatter bewirkt eine Zustandsdrehung um 90° bezüglich der x-Achse (mit Phasenverschiebung) und hat im Klassischen, ebenso wie die Rotation des Zustandes kein Äquivalent. Weiters bedeuten gekreuzte Verbindungen in der Schaltsymbolik eine CPhase-Operation.

Ausgehend von jeweils vier-Qubit-Cluster zeigt Abb. 7a) die Bildung eines linearen drei-Qubit-Clusters. Durch eine vorhergehende Messung des ersten Qubits in der σ_z-Eigenbasis (und der damit resultierenden Aufhebung der Verschränkung) wurde der lineare vierer Cluster auf einen linearen drei-Qubit-Cluster reduziert. Damit soll gezeigt werden, dass im Aufbau von komplexen Cluster-Schaltungen redundante Qubits eines Clusters nicht physikalisch, sondern durch Messung in σ-Eigenbasis 'entfernt' werden.
Mittels Messungen an den Qubits 2 ($|\psi_{in}\rangle$)und 3 wird am Qubit 4 schließlich der Zustand $|\psi_{out}\rangle = R_x(-\beta)R_z(-\alpha)|\psi_{in}\rangle$ realisiert.
Diese Folge (Beschrieben durch einen Operator F) wird auf jeweils dem (den) Qubits (Qubit) auf der linken Spalte angewandt ($|\psi_{in}\rangle$) und das Ergebnis auf der rechten (ψ_{out}) übertragen.
In Schema b) können aufgrund der Clustergröße (linearer 4-Qubit-Cluster) drei Messungen erfolgen und damit kann der Zustand $|\psi_{out}\rangle = HR_z(-\gamma)R_x(-\beta)R_z(-\alpha)|\psi_{in}\rangle$ an Qubit 4 erzeugt werden.
Im Horseshoe-Cluster (benannt nach seiner 'hufeisenförmigen Form') dienen in c) Qubit 2 und 3 als Input der Messung. Damit ergibt sich an den Qubits 1 und 4: $|\psi_{out}\rangle = (H_1 \otimes H_4)[R_z(-\alpha) \otimes R_z(-\beta)]\ CPhase|\psi_{in}\rangle$.
Den Endzustand von d) erhält man an den Qubits 2 und 3 mit $|\psi_{out}\rangle = CPhase\ (H_1 \otimes H_4)[R_z(-\alpha) \otimes R_z(-\beta)]|\psi_{in}\rangle$, während 1 und 4 als Input-Qubits dienen.
Im Box-Cluster (Abb. 7e) dienen analog zu d) Qubit 1 und 4 als Input-, Qubit 2 und 3 als Output-Qubits. Dabei ergibt sich aus den Messungen $|\psi_{out}\rangle = CPhase\ (H_1 \otimes H_4)[R_z(-\alpha) \otimes R_z(-\beta)]\ CPhase|\psi_{in}\rangle$.

Am Ausgang von 2-dimensionalen Clusterzuständen können verschränkte Zustände auftreten. Hierfür entscheidend ist der jeweilige Anfangszustand. So bewirkt der Eingangszustand $|+\rangle_1|+\rangle_4$ mit der Rotation $[\alpha = \pi, \beta = 0]$ den Ausgangszustand $|+\rangle_2|+\rangle_3$, der wie leicht zu sehen ist keinen verschränkten Zustand aufweist. Hingegen bewirkt der Eingangszustand $|+\rangle_1|+\rangle_4$ am Horseshoe-Cluster mit der Messung $[\alpha = 0, \beta = 0]$ immer eine maximale Verschränkung. So tritt am Ausgang der Zustand $\frac{1}{\sqrt{2}}(|0\rangle_2|+\rangle_3 + |1\rangle_2|-\rangle_3)$ auf.

Die dargestellten Schaltungen (Cluster) bilden ein universelles Set von logischen Gattern. Mit ihnen kann die volle Funktionsfähigkeit des Quantencomputers beschrieben, d.h. jeder weitere logische Aufbau durch die Zusammensetzung der universellen Cluster erklärt werden. Dabei muß immer

[9] experimentell z.B. durch den Aufbau von Stern-Gerlach realisiert
[10] nach dem Mathemaiker Jacques Salomon Hadamard

der Output des Clusters mit dem Input des Folgeclusters durch eine CPhase-Operation verbunden sein.

5.3.1 Beispiel

Als Beispiel, ausgehend von einem 5-Qubit-Cluster-Zustand, soll an dieser Stelle gezeigt werden, wie eine beliebige Rotation des Input-Qubits $|\psi_{in}\rangle$ auf $|\psi_{out}\rangle$ einzig durch Messungen realisiert werden kann. Man erhält damit $|\psi_{out}\rangle = U_R(\xi,\eta,\zeta)|\psi_{in}\rangle$ mit $U_R(\xi,\eta,\zeta) = U_x(-\gamma)U_z(-\eta)U_x(-\xi)$[11].

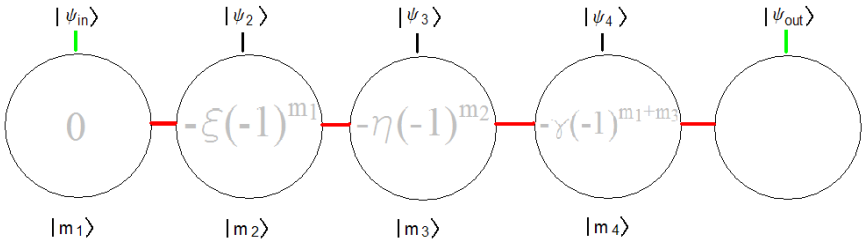


Abbildung 8: Beispiel: Qubit-Rotation

Für die anschließende Diskussion wird der folgende Hadamard-Operator und die folgenden Rotationsoperatoren benötigt:

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

$$R_x(\theta) = \begin{pmatrix} cos\frac{\theta}{2} & -i\ sin\frac{\theta}{2} \\ -i\ sin\frac{\theta}{2} & cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = \begin{pmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$$

1. Für ein Paar von Qubits (i,j) kommutiert der $CPhase(i,j)$-Operator, wobei die Konfigurationsbasis $|m_1, m_2, ..., m_N\rangle$ die Eigenbasis ist.
2. Der CPhase-Operator vertauscht mit jeden nicht wirkenden Operator für i und j (äquvivalent zur Identität)
   Allgemeiner: Operatoren, wirkend auf unterschiedlichen Qubits kommutiern
3. Definition:
   $\forall i \leq j : S^{(i-j)} \equiv CPhase(i,i+1)CPhase(i+1,i+2)\cdots CPhase(j-1,j)$ (wobei die Reihenfolge nach (1) nicht wichtig ist)
4. Wir präparieren den Zustand:
   $|\psi_0\rangle = S^{(1-5)}|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes |\psi_4\rangle \otimes |\psi_5\rangle$
   mit $|\psi_1\rangle = |\psi_{in}\rangle$ und $\otimes_{i=2}^{5}|+\rangle_i$ (siehe Abb. 8)

[11] mit $U_x(\alpha) = e^{-i\alpha\frac{\sigma_x}{2}}$ und $U_z(\alpha) = e^{-i\alpha\frac{\sigma_z}{2}}$

5. Die Messung erfolgt in der jeweiligen Basis $B_j(\alpha_j) = |^0_1, \alpha_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle_j \pm e^{\imath\alpha_j}|1\rangle_j) = e^{(\imath\frac{\alpha_j}{2})}R_z(\alpha)H|^0_1\rangle$[12] und löst damit jedes Mal eine Verschränkung auf (symbolische rote Linie in Abb.: 8). Als Resultat der Messung ergibt sich $|m_j\rangle$ mit $m_j \in \{0,1\}$, wobei $m_j = 0$ ($m_j = 1$)bedeutet, dass Qubit j in den ersten (zweiten) Zustand der Basis $B_j(\alpha_j)$ projiziert wurde. Die Inversion der Basis ergbit: $|^0_1\rangle = \frac{1}{\sqrt{2}}(|0,\alpha_j\rangle_j \pm e^{-\imath\alpha_j}|1,\alpha_j\rangle_j)$.

6. Wird die Messung in der Basis $B(\alpha_j)$ auf das Qubit $|\psi_i\rangle$ angewandt, vertauscht diese mit allen $CPhase(j,l)$, mit $j,l \neq i$ (siehe ②).

7. Für den linearen Cluster können wir uns dies zu Nutze machen und somit zwei benachbarte Qubits verschränken.
$CPhase(|\psi_{in}\rangle \otimes |+\rangle)$ $\quad\|$ mit dem Ansatz: $|\psi_{in}\rangle = a|0\rangle + b|1\rangle$ und unter Verwendung von ⑤
$= \frac{a}{\sqrt{2}}(|0,\alpha_j\rangle + |1,\alpha_j\rangle) \otimes |+\rangle + e^{-\imath\alpha_j}\frac{b}{\sqrt{2}}(|0,\alpha_j\rangle - |1,\alpha_j\rangle \otimes |-\rangle)$
$= |0,\alpha_j\rangle \otimes (a|+\rangle + e^{-\imath\alpha_j}b|-\rangle) + |1,\alpha_j\rangle \otimes (a|+\rangle - e^{-\imath\alpha_j}b|-\rangle)$
globale Konstanten können vernachlässigt werden, da sie für uns keine Rolle spielen
$= |0,\alpha_j\rangle \otimes e^{-\imath\frac{\alpha_j}{2}}HR_z(-\alpha_j)(a|0\rangle + b|1\rangle) + |1,\alpha_j\rangle \otimes e^{-\imath\frac{\alpha_j}{2}}HR_z(-\alpha_j)(a|0\rangle - b|1\rangle)$
$= |0,\alpha_j\rangle \otimes HR_z(-\alpha_j)|\psi_{in}\rangle + |1,\alpha_j\rangle \otimes HR_z(-\alpha_j)\sigma_z|\psi_{in}\rangle$
Nach der Messung wird die rechte Seite mittels der Relation $H\sigma_z = \sigma_x H$ transformiert zu:
$= |0,\alpha_j\rangle \otimes HR_z(-\alpha_j)|\psi_{in}\rangle + |1,\alpha_j\rangle \otimes \sigma_x^m HR_z(-\alpha_j)|\psi_{in}\rangle$ mit $m \in [0,1]$ als das Ergebnis der Messung.

8. Nach der Messung von $|\psi_1\rangle$ in der Basis $B(\alpha_1 = 0)$ transformiert sich der Zustand $|\psi_0\rangle$ zu:
$|\psi\rangle = |m_1,\alpha_1\rangle \otimes S^{(2-5)}|\tilde{\psi_2}\rangle \otimes |\psi_3\rangle \otimes |\psi_4\rangle \otimes |\psi_5\rangle$
mit m_1 dem Messergebnis der ersten Messung und $|\tilde{\psi_2}\rangle = \sigma_x^{m_1}H|\psi_{in}\rangle$ aus ⑦

9. Analog zu ⑦ erfolgt die Messung von $|\tilde{\psi_2}\rangle$ in der Basis $B(\alpha_2 = -\xi(-1)^{m_1})$. Daraus ergibt sich mit m_2 dem Messergebnis dieser zweiten Messung:
$|\psi_2\rangle = |m_1,\alpha_1\rangle \otimes |m_2,\alpha_2\rangle \otimes S^{(3-5)}|\tilde{\psi_3}\rangle \otimes |\psi_4\rangle \otimes |\psi_5\rangle$
mit $|\tilde{\psi_3}\rangle = \sigma_x^{m_2}HR_z((-1)^{m_1}\xi)|\tilde{\psi_2}\rangle$
Unter Verwendung der Fortpflanzungsrelation $HR_z(\xi)\sigma_x = \sigma_z HR_z(-\xi)$ und $HR_z(\xi)H = R_x(\xi)$ erfolgt:
$= \sigma_x^{m_2}H\sigma_x^{m_1}R_z(-\xi)H|\psi_{in}\rangle$
$|\tilde{\psi_3}\rangle = \sigma_x^{m_2}\sigma_z^{m_1}R_x(-\xi)|\psi_{in}\rangle$

10. Die Messung von $|\tilde{\psi_3}\rangle$ mit dem Ergebnis m_3 erfolgt in der Basis $B(\alpha_3 = -\eta(-1)^{m_2})$:
$|\psi_3\rangle = |m_1,\alpha_1\rangle \otimes |m_2,\alpha_2\rangle \otimes |m_3,\alpha_3\rangle \otimes S^{(4-5)}|\psi_4\rangle \otimes |\psi_5\rangle$
mit $|\tilde{\psi_4}\rangle = \sigma_x^{m_3}HR_z((-1)^{m_2}\eta)|\psi_3\rangle$
mit der Fortpflanzungsrelation $HR_z(-\eta)\sigma_z = \sigma_x HR_z(-\eta)$ erhält man:
$|\tilde{\psi_4}\rangle = \sigma_x^{m_3}\sigma_z^{m_2}\sigma_x^{m_1}HR_z(-\eta)R_x(-\xi)|\psi_{in}\rangle$

11. Schließlich ergibt die Messung von $|\tilde{\psi_4}\rangle$ in der Basis $B(\alpha_4 = -\gamma(-1)^{m_1+m_3})$ als Resultat m_4.
$|\psi_4\rangle = |m_1,\alpha_1\rangle \otimes |m_2,\alpha_2\rangle \otimes |m_3,\alpha_3\rangle \otimes |m_4,\alpha_4\rangle S^5|\psi_5\rangle$
mit $|\tilde{\psi_5}\rangle = HR_z((-1)^{m_1+m_3}\gamma)|\tilde{\psi_4}\rangle$
mit den Relationen $H\sigma_x = \sigma_z H$, $H\sigma_z = \sigma_x H$, $HR_z(-\gamma)H = R_x(-\gamma)$ und $H^2 = \mathbb{1}$ ergibt sich:
$|\psi_{out}\rangle = \sigma^{m_4+m_2}\sigma^{m_1+m_3}R_x(-\gamma)R_z(-\eta)R_x(-\xi)|\psi_{in}\rangle$

[12] mit α_j als jeweiliger Winkel des Basiszustandes (Basiszustände liegen auf dem Schnitt der Blochkugel mit der x/y - Fläche)

Durch die Zufälligkeit der jeweiligen Messung ergibt sich ein unerwünschter Nebenproduktoperator ('random byproduct operator'), womit **nicht** $|\psi_{out}\rangle = U_R(\xi,\eta,\zeta)|\psi_{in}\rangle$, sondern durch die Messungen eigentlich $|\psi_{out}\rangle = U_{\sum,R}U_R(\xi,\eta,\zeta)|\psi_{in}\rangle$ realisiert wird, mit (im allgemeinen Ansatz) $U_{\sum,R} = \otimes_{j=1}^{n}(\sigma_x)^{m_j+\lambda_{x,j}}(\sigma_z)^{\lambda_{z,j}}$ [13].

Der Nebenproduktoperator $U_{\sum,R}$ entspricht einer Korrektur und muß damit im erhaltenen Ausgangszustand $|\psi_{out}\rangle$ berücksichtigt werden, oder kann gegebenenfalls durch die Anwendung eines Korrekturoperators ('local correction operator') kompensiert werden (weitere Erläuterungen in [3]).

5.3.2 C_{NOT}-'controlled NOT'-Operator

Um an die Kapitel 'Der klassische Computer' und 'One Way Quantum Computing' (siehe Kapitel 3) anschließen zu können soll an dieser Stelle die Clusterbildung und Messung zur Erstellung eines C_{NOT}-'controlled NOT'-Gatters besprochen werden.
Die einfachste Realisierung eines C_{NOT}-Gatters besteht aus vier-Qubits (siehe Abb. 9 bzw. Ref. [3]). Hierzu müssen zuerst die Qubits in den Zustand $|i_1\rangle_{z,1}\otimes|i_4\rangle_{z,4}\otimes|+\rangle_2\otimes|+\rangle_3$ (mit $|i_1\rangle_{z,1}$ und $|i_4\rangle_{z,4}$ den Inputzuständen) gebracht und anschließend mit Hilfe des CPhase-Operators (siehe Def. Gl. 3) verschränkt werden.

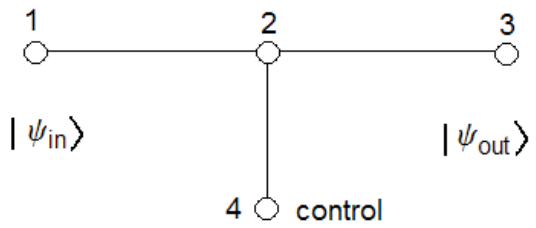


Abbildung 9: Darstellung der einfachsten Form eines C_{NOT}-Gatters

Nach der Verschränkung der Qubits erfolgt die Messung des ersten und zweiten Qubits in der σ_x-Eigenbasis. Das Messresultat $m_j \in [0,1]$ ergibt - analog zu Kap. 5.3.1 - die Projektion des j-ten Qubits in den Zustand $|m_j\rangle$, mit $j = 1,2$ und damit $|m_1\rangle_{x,1}\otimes|m_2\rangle_{x,2}$.
An dem Kontroll-Qubit 4 bleibt vorerst der Eingangszustand $|i_4\rangle_{z,4}$ erhalten. Durch die Verschränkung dieses Qubits mit dem Qubit 2 bildet sich nach dessen Messung, im Gegensatz zu einem linearen Cluster an Qubit 3 der Zustand: $|(i_1+i_4)mod2\rangle_{z,3}$. Durch die Modulo2-Funktion ist gewährleistet, dass der Zustand $|i_1\rangle$ immer kippt, sollte $|i_4\rangle = 1$ sein und damit ist die Schaltlogik eines C_{NOT}-Gatters hergestellt.
Auch hier tritt - analog zu Kap. 5.3.1 - der Nebenproduktoperator auf. Damit ergibt sich an den Outputqubits $(3,4)$ der Zustand: $|\psi_{out}\rangle = U_{\Sigma}^{(34)}|i_4\rangle_{z,4}\otimes|(i_1+i_4)mod2\rangle_{z,3}$ mit dem Nebenproduktoperator $U_{\Sigma}^{34} = \sigma_z^{m_1+1}\sigma_x^{m_2}\sigma_z^{m_1}$
Die Zustände der Output-Qubits können nun ohne Beschränkung der Allgemeinheit in der σ_z-Eigenbasis ausgelesen werden.

[13] mit n der Qubitanzahl
Der Cluster erfüllt dabei das Theorem, die Eigenwertgleichungen (aus [3]), die λ-Werte werden daraus bestimmt: $\sigma_x^{C_I}(U\sigma_xU^\dagger)^{C_O}|\psi\rangle_C = (-1)^{\lambda_{x,j}}|\psi\rangle_C$ und $\sigma_z^{C_I}(U\sigma_zU^\dagger)^{C_O}|\psi\rangle_C = (-1)^{\lambda_{z,j}}|\psi\rangle_C$, mit U als unitärer Operator und C_I, C_O, C als Menge der Input-, Output- und der gesamten Clusteranteile

5.4 Experimentalaufbau

5.4.1 Optical parametric down conversion (OPDC)

Zur experimentellen Herstellung von Clustern mit 4 verschränkten Qubits bediente sich A. Zeilinger der sogenannten 'optical parametric down conversion' (OPDC), siehe [4]. In Abbildung 10 ist der entsprechende schematische Aufbau zu sehen.

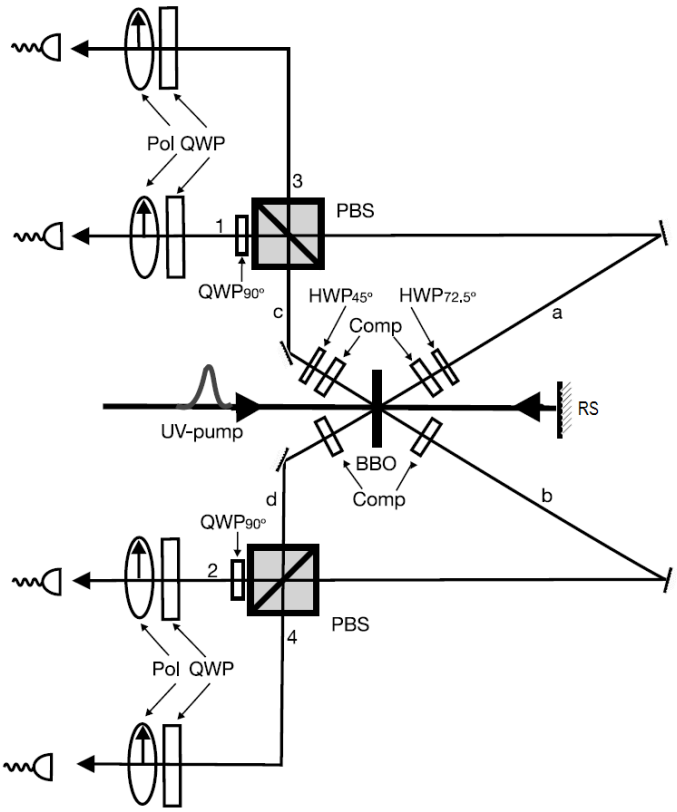


Abbildung 10: Experimenteller Aufbau zur Clustererzeugung aus Ref. [4] entnommen

Dazu passiert ein frequenzverdoppelter Laserpuls (795 nm) zweimal einen BBO-Kristall[14], wobei jedes Mal zwei Photonen mit doppelter Wellenlänge emittiert werden (Strahlengang [a,b] bzw. [c,d] in Abb. 10). Die Emissionsrichtungen der Photonen (gegeben durch Impuls- und Energieerhaltung) liegen dabei bei geeigneter Kristallausrichtung auf zwei sich überschneidenden Kegelmänteln (siehe Abb. 11). Liegen die emittierten Photonen mit dem eingehenden Photon auf einer Ebene, sind die Zustände dieser Teilchen miteinander antisymmetrisch verschränkt.

Quantenmechanisch wird die Wechselwirkung im optisch doppelbrechenden Kristall durch den konstruierten Hamilton-Operator beschrieben (nach [5]):

$$H(x,t) = \epsilon_0 \int_V d^3\vec{x}' \cdot \chi \cdot E_p(\vec{x}',t) E_{ao}(\vec{x}',t) E_o(\vec{x}',t)$$

[14] β-Bariumborat-Kristall ($\beta - Ba_3(B_3O_6)_2$) ist ein optisch doppelbrechender Kristall - mit hoher optischer Nichtlinearität und transparent im Wellenlängenbereich [189 - 3500 nm]

mit ϵ_0 der Dielektrizitätskonstante in Vakuum, χ dem Suszeptibilitätstensor des Kristalls, der Feldstärken E_p des Pumpstrahls und der im optisch nichtlinearen Kristall auftretenden außerordentlichen (E_{ao}) und ordentlichen Feldstärke (E_o). Durch die hohe Intensität des Laserpuls-Pumpstrahls kann diese Feldkomponente (E_p) des Integrals als klassische monochromatische Welle dargestellt werden, mit $E_p(\vec{x}', t) = E_p e^{i(\vec{k}_p \vec{z} - \omega_p t)}$.
Die Felder des außerordentlichen bzw. ordentlichenen Strahls hingegen unterliegen einem quantenmechanischen Ansatz mit den Photonenerzeugungsoperatorn $a(\vec{k}_{ao})$ für den außerordentlichen und $a(\vec{k}_o)$ für den ordentlichen Strahlenanteil. Daraus ergibt sich für die Feldstärke des außerordentlichen $E_{ao}(\vec{x}', t) = \int d^3\vec{k}_{ao} E_{ao} a(\vec{k}_{ao}) e^{-i(\vec{k}_{ao}\vec{x} - \omega_{ao} t)}$ und des ordentlichen Strahlengangs $E_o(\vec{x}', t) = \int d^3\vec{k}_o E_o a(\vec{k}_o) e^{-i(\vec{k}_o \vec{x} - \omega_o t)}$, wobei k_i den jeweiligen Wellenzahlvektor und ω_i die dazugehörige Frequenz angibt.
Die Integralschreibweise von E_{ao} und E_o ist auf die Impulserhaltung zurückzuführen, so ist zwar der Gesamtimpuls des Pumpphotons bekannt, jedoch sind nicht die zwei Einzelimpulse nach der parametrischen Fluoreszenz bestimmt.
Der Zustandsvektor der erhaltenen Photonen wird mit Hilfe der Störungstheorie erster Ordnung mit dem konstruierten Hamiltonoperator berechnet, daraus ergibt sich, basierend auf den Vakuumzustand $|0\rangle$:

$$|\psi(t)\rangle = |0\rangle - \frac{i}{\hbar} \int_0^t dt' H(\vec{x}, t')|0\rangle \tag{4}$$

Die Ausbreitungsrichtung des Pumpstrahls liegt im Koordinatensystem in z-Richtung. Unter Beachtung der Impulserhaltung resultiert daraus, dass sich die orthogonalen Impulsanteile der emittierten Photonen aufheben ($\vec{k}_o^\perp = -\vec{k}_{ao}^\perp = \vec{k}^\perp$) und dessen Parallelanteile sich zum Gesamtimpulsvektor summieren ($\vec{k}_o^z + \vec{k}_{ao}^z = \vec{k}_p^z$). Mit der Energieerhaltung $\omega_p = \omega_o + \omega_{ao}$ und der Deltafunktion reduziert sich das Integral (Gl.4) auf:

$$|\psi\rangle = |0\rangle - C \int dk_o^z dk_{ao}^z d^2\vec{k}^\perp \delta(\omega_p - \omega_o - \omega_{ao}) \delta(k_p^z - k_o^z - k_{ao}^z) a(k_o^z + \vec{k}^\perp) a(k_{ao}^z - \vec{k}^\perp)|0\rangle$$

Betrachtet man nur die Schnittpunkte der Kegelmäntel der möglichen Emissionsrichtungen, muss das Integral mit der Funktion $\frac{1}{\sqrt{2}}(\delta(\vec{k}^\perp - \vec{k}_1^\perp) + \delta(\vec{k}^\perp - \vec{k}_2^\perp))$ mit den Richtungsvektoren ($\vec{k}_1$, $\vec{k}_2$ und $\vec{k}_1^\perp = \vec{k}_2^\perp$) der Schnittpunkte, multiplikativ ergänzt werden. Durch anschließende Integration ergibt sich der Zustand:

$$|\psi\rangle = |0\rangle - \frac{C}{\sqrt{2}} \left(a(\vec{k_o})_1 a(\vec{k_{ao}})_2 + a(\vec{k_{ao}})_1 a(\vec{k_o})_2 \right)$$

Der Koinzidenzterm ergibt schließlich den verschränkten Zustand der beiden Photonen und sieht in gewohnter Angabe der Polarisationsrichtung wie folgt aus:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 + e^{i\phi} |V\rangle_1 |H\rangle_2)$$

Physikalisch sollen daher nur Photonen der Schnittpunkte den Experimentalaufbau passieren, dies kann durch den Einsatz von Filtern bzw. Lochmasken relativ einfach realisiert werden.

Das Auftreten der Doppelbrechung durch die starke Anisotropie des BBO-Kristalls wirkt sich in der Ausbreitungsrichtung der außerordentlichen/ordentlichen, polarisierten Konversionsmode in Form einer Strahlablenkung (transversaler walk-off) ebenso, wie in der unterschiedlichen Gruppengeschwindigkeit der Wellenpakete der Konversionsphotonen (longitudinaler walk-off) aus. Beide Effekte müssen so gut als möglich im Kompensationsaufbau (Comp) entschärft werden, da sie dem Grad der Verschränkung (Qualität) nicht dienlich sind.
Die Halbwellenplättchen (HWP) dienen schließlich zur Generierung der vier möglichen Bell-Zustände,

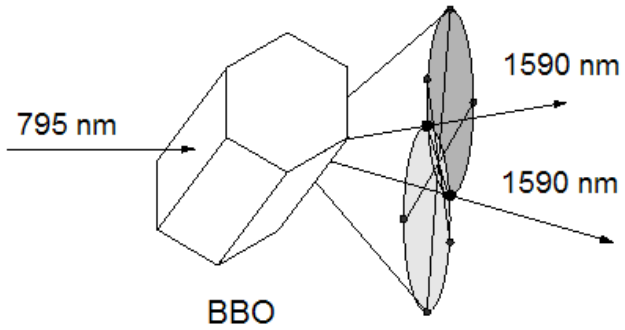


Abbildung 11: Emission der 'down-conversion'-Photone [4]

dies geschieht wie folgt:
Das in Rückwärtsrichtung emittierte Photonenpaar trifft durch Justierung des Reflektionsspiegels (RS) des UV-Pumpstrahls zeitgerecht mit dem in Vorwärtsrichtung emittierten Photonenpaar im jeweiligen Strahlteiler (PBS) ein. Der Strahlteiler ist als Kombination zweier Prismen zu verstehen, mit Unterscheidung im Transmissionsverhalten zwischen horizontaler (Transmission) und vertikaler Polarisation (Brechung/Reflexion). Nach dem PBS wird an zwei Stellen zur Kompensation doppelbrechender Eigenschaften ein Viertelwellenplättchen eingesetzt.
Der Clusterzustand kann schließlich nur bei gleichzeitiger Emission der Photonen/Qubits zustande kommen. Ohne Einsetzen weiterer HWPs kommt der Zustand $|\psi\rangle = |H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$[15] zustande. Eine weitere Möglichkeit ist das sogenannte Zusammenfallen von Zuständen, die schlussendlich zum hoch verschränkten Clusterzustand
$|\phi_{cluster}\rangle = \frac{1}{2}(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 + |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4)$
superponieren. Dazu muss das Vorzeichen des Zustands, erzeugt vom 'vorwärts'-Photonenpaar $|\phi_{a,b}\rangle = -|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$ durch einen π-shift geändert werden - dies wird durch eine Polarisationsdrehung größer $\varphi = 22,5°$ erreicht, theoretische Berechungen ergeben ein $\varphi = 27,5°$ (HWP 72,5°). Der 'rückwärts'-Zustand $|\phi_{c,d}\rangle = |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4$ ergibt damit den letzten Teil der Superposition und damit wäre der Bell-Zustand realisiert.

Durch innere Eigenschaften (Rauschen, u.s.w.) nimmt die Schwierigkeit zur Bildung von Clustern höherer Qubit-Anzahl exponentiell zu.

5.4.2 Ionenfalle

Eine weitere Möglichkeit zur Clusterbildung ist die Manipulation von Kalzium-Ionen in einer Ionenfalle, siehe genauere Beschreibung [7]. Dazu wird Kalzium-Dampf mittels Laserbeschuss ionisiert und in einem Wechselfeld (Ionenfalle) eingeschlossen. Durch gegenseitige Abstoßung reihen sich die Ionen perlenartig an (siehe Abb.:12).

Mittels Doppler- und Ramankühlung (mit frequenzstabilem Laser) wird die Ausgangsbedingung nachfolgender Quantenoperationen definiert. Durch einen sehr genauen Laser erfolgt schließlich die Adressierung der Qubits. Durch die Coulomb-Abstoßung unter den einzelnen Ionen wirkt sich jede Bewegungsänderung eines einzelnen auf die Bewegung aller aus. Dieser Umstand kann für die Verschränkung genutzt werden. In einfachen Worten Dargestellt kann die Laser-Photonenenergie so

[15] mit $|H\rangle$ für horizontal, $|V\rangle$ für vertikal polarisierter Zustand und den jeweiligen Qubit Index

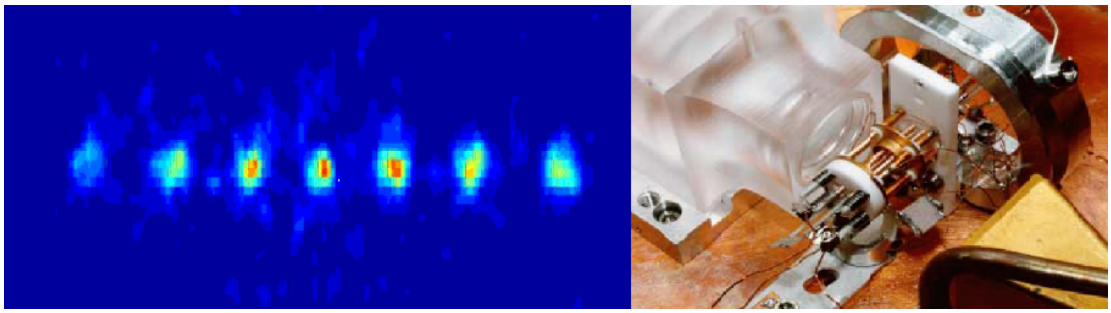


Abbildung 12: Ionenzustände als Informationsträger (aus Ref. [7]) in Ionenfalle (aus Ref. [8])

adjustiert werden, dass nach der Anregung ein Quantum an Bewegungsenergie ($E_{kin} = \hbar \cdot \omega_{Falle}$) übrig bleibt, womit die Bewegung mit dem internen Zustand gekoppelt ist. Wird jetzt der Bewegungszustand eines weiteren Ions geändert, wirkt sich dies auf das ganze System aus.

Diese Methode zeichnet sich durch die relativ einfache Adaptierung der Qubit-Anzahl - durch das Einbringen weiterer Ionen in die Falle - aus. Details können in [6] gefunden werden

5.4.3 Ultrakalte Atome im optischen Gitter

Aktuelles Forschungsgebiet ist auch die Anwendung ultrakalter Atome im optischen Gitter als Quantencomputer (aus Ref. [9] entnommen). Der zweidimensionale Clusterzustand wird dabei aus einem neu entdeckten Materienzustand - dem sogenannten Mott[16]-Zustand - nahe dem absoluten Nullpunkt gebildet.
In einer dreidimensionalen Gitteranordnung von Laserstrahlen befinden sich Atome - im superfluiden Bose-Einstein-Kondensat, also in einem 'wellenartigen Atomgaszustand' - auf den ganzen optischen Kristall (Lasergitter) gleichmäßig verteilt. Wird die Laserleistung erhöht, kommt es zu einem Quantenphasenübergang[17] in die Mott-Isolator-Phase (siehe Abbildung 13). Nun ist jeder Gitterplatz durch abstoßende Wechselwirkungen untereinander mit einer genau definierten Anzahl von Atomen besetzt, für die Anwendung des Quantencomputers idealerweise mit einem Atom.

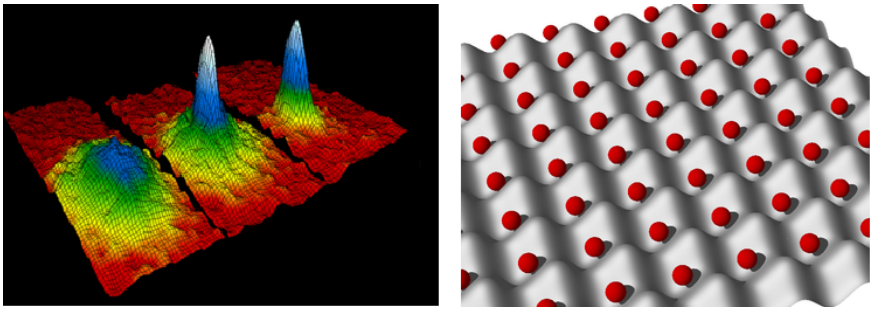


Abbildung 13: Bose-Einstein-Kondensat (aus Ref. [10]) und Mott-Isolator-Phase (aus Ref. [11]) nach Quantenphasenübergang im optischen Gitter

[16] von Sir Neville Mott erstmals beschrieben - erhielt dafür 1977 den Nobel Preis für Physik
[17] da keine thermische Fluktuation während des Quantenphasenübergangs am absoluten Nullpunkt vorhanden ist, wird dieser Übergang durch die Quantenfluktuation beschrieben

Nun hat man eine sehr große Anzahl gleich präparierter Atome zur Verfügung, die mittels Radioimpulse in den vorgesehenen Quantenzustand gebracht werden können. Mit einem Laserstrahl werden die Qubits verschoben und stoßen mit ihren nächsten Nachbarn zusammen (cold collisions), wodurch sich ihre Quantenzustände durch zustandsabhängige Wechselwirkung oder mittels Tunneleffekt miteinander verschränken. Per Laserstrahl werden die Qubits mit ihren neuen Eigenschaften wieder ins Potentialminimum des Lichtkristalls verschoben. Zur Realisierung des Quantengatters fehlen schließlich nur noch die Einzelmessungen. Eine sehr viel versprechende Methode ist geboren.

5.5 Tomografie eines Quantenzustands

Nach der experimentellen Präparierung der Zustände ist es wichtig auch diese zu überprüfen und im Speziellen den Erfolg der Verschränkung zu dokumentieren. Dies geschieht in der Quantenzustandstomografie - hier erklärt anhand eines Beispiels für vier Qubits (aus [4]). Dazu müssen unter gleichen Laborbedingungen wiederholt Zustände produziert und diesbezüglich die Dichtematrix ρ des vier-Photonen-Polarisationszustandes gemessen werden. Daraus ergibt sich für ρ eine 16x16-Matrix, dargestellt in Abbildung 14. Um diese 256 Messungen (16x16) vollziehen zu können, bildet man alle Kombinationen der Zustände: $|H\rangle$, $|V\rangle$, $\frac{|H\rangle+|V\rangle}{\sqrt{2}}$ und $\frac{|H\rangle-i\,|V\rangle}{\sqrt{2}}$. Damit werden sowohl die Haupt-, als auch die Nebendiagonalen der Dichtematrix bestimmt. Dabei muß jede Messung aus statistischen Gründen einige hundert Male durchgeführt werden. Die Hauptdiagonalelemente beinhalten die Zustände $|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4$, $|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$, $|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4$ und $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$. Da der letzte Term des Clusterzustands $|\phi\rangle = \frac{1}{2}(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 + |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4)$ negativ ist, treten auch in der Darstellung der Dichtematrix im Zusammenhang mit dem Zustand $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ negative Einträge auf.
Quantenmechanisch wichtig sind jedoch die Nebendiagonalen, beschreiben diese Elemente doch die Kohärenz und zeigen, dass es sich um eine echte Superposition handelt. Ist die Dichtematrix nicht separierbar:

$$H_{1\ldots n} = H_1 \otimes H_2 \otimes \ldots \otimes H_n, p_k \geq 0, \sum_k p_k = 1, \rho \neq \sum_k p_k \rho_1^k \otimes \ldots \rho_n^k$$

ist dies eine hinreichende Bedingung für eine vorliegende Verschränkung. Gerade dieser Umstand ist jedoch sehr schwer zu überprüfen.

Um die Qualität des experimentell erlangten Zustands zu beurteilen wird dieser mit dem theoretisch geforderten ($\phi_{cluster}$) in Form der Güte F (fidelity), mit $F = \langle\phi_{cluster}|\rho|\phi_{cluster}\rangle$, verglichen. $F = 1$ würde einen exakt erzeugten Zustand beschreiben und F = 0 einen totalen Fehlschlag. Im Experiment von A. Zeilinger mit vier Qubits erlangte man eine Güte von F = $(0,63 \pm 0,01)$, welche den modellierten 'bi-separablen'-vier-Qubit-Zustand mit $F = 0,5$ um einiges übertrifft und es sich dadurch zwangsweise um einen erfolgreich verschränkten vier-Qubit-Cluster handeln muß.
Es ist anzunehmen, dass bei jeder weiteren Vergrößerung des Hilbertraums die Güte und damit die Qualität der Zustände bzw. der Verschränkungen sinken wird
Eine weitere Möglichkeit zur Überprüfung des Verschränkungsgrades ist die - zugegebenermaßen schwierige - Auffindung eines Zeugenoperators W. Für einen drei-Qubit-Zustand (also z.B. zur Überprüfung der Verschränkung nach einer Messung eines vier-Qubit-Clusters) hat dieser folgende Form: $W = \frac{1}{4}\mathbb{1}^{\otimes 3} - \frac{1}{2}(|H\rangle_2\langle H|_2 \otimes |\phi^+\rangle_{3,4}\langle\phi^+|_{3,4} + |V\rangle_2\langle V|_2 \otimes |\phi^-\rangle_{3,4}\langle\phi^-|_{3,4})$[18]

Die Dichtematrix ist demnach separierbar, wenn $tr(W\rho) \geq 0$ ist und steht für einen verschränkten Zustand, sollte die Spur negativ sein.

[18] mit I dem Einheitsoperator, den Indizes 2,3,4 der jeweiligen Qubits und $|\phi^+\rangle$,$|\phi^-\rangle$ für die vorwärts- bzw. rückwertsemittierten Photonenpaare aus Abb. 11

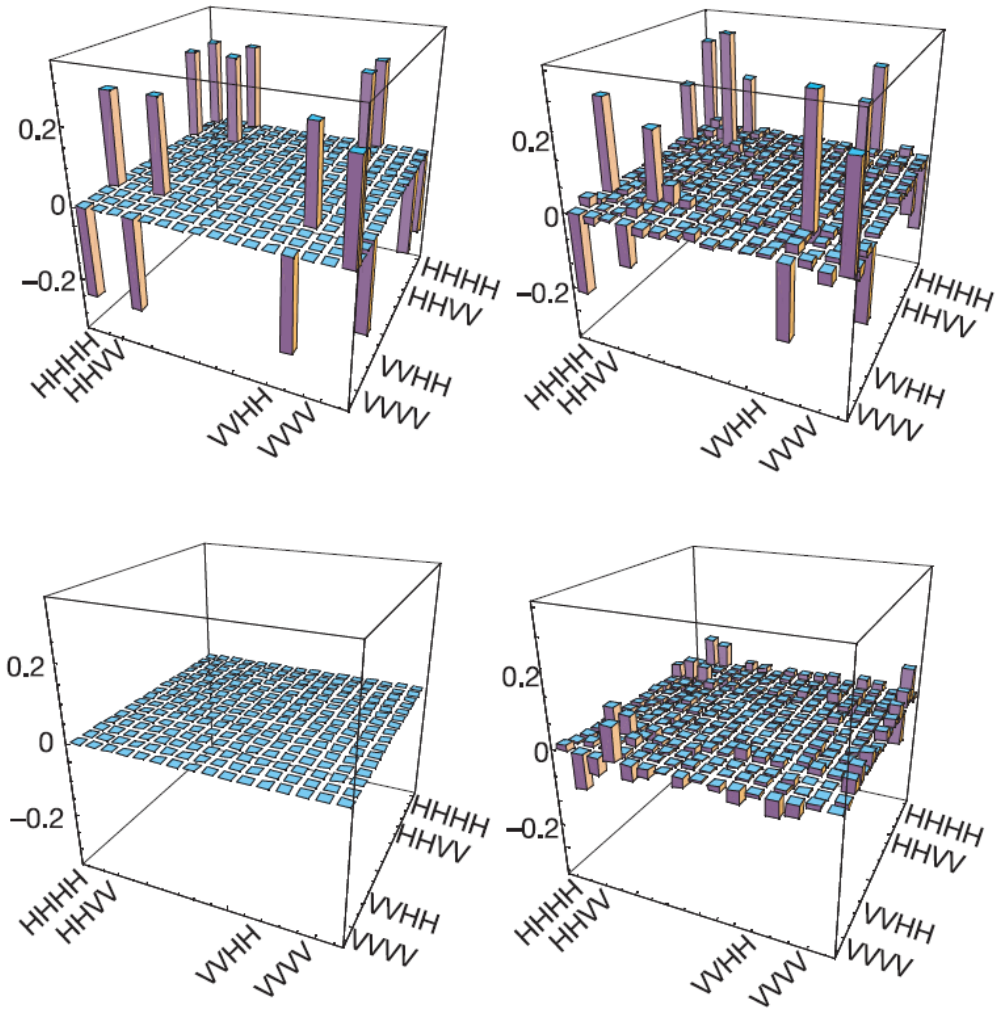


Abbildung 14: Dichtematrix eines 4-Qubit-Zustands in Laborbasis: a) theoretisch und b) experimentell. Die obere Darstellung gibt dabei den Real-, die untere den Imaginärteil an

6 Epilog

Die vorteilhafte Anwendung des Quantencomputers ist momentan auf einige wenige Algorithmen beschränkt. Am deutlichsten ersichtlich ist die Effizienzsteigerung bei der Suche in unsortierten Datenbanken mit N einträgen. Erhält man mit herkömmlichen klassischen Computern ein Ergebnis in $O(N)$-Schritten (O...Ordnung), so ist diese Suche mittels Grover-Algorithmus [12] durch einen Quantencomputer in $O(\sqrt{N})$-Schritten abgeschlossen. Bei steigender N-Anzahl eine beträchtliche (polynominale) Zeiteinsparung, doch dazu ist noch viel Forschung nötig - es besteht somit kein Grund, panikartig die Google-Aktien zu verkaufen.
Der erste Algorithmus, dessen zeitgewinn exponentiell ist wurde von P.W.Shor [13] entwickelt. Dieser spezialisiert sich auf die Faktorisierung, also auf die Berechung nichttrivealer Teiler von zusammengesetzten Zahlen. Im Gegensatz zur Berechnung mit klassischen Algorithmen (exponentieller Anstieg der Laufzeit, mit $L = log(N)$, wobei N die Zahl ist) tritt hierbei nur ein polynominaler Laufzeitanstieg bei steigendem N auf. Dieser Umstand hat starke Auswirkungen auf die Kryptografie, bauen doch heutige Verschlüsselungssysteme genau auf die Faktorisierung auf. Ein symbolisches Beispiel soll die immense Steigerung zeigen: wenn die Faktorisierung einer Zahl mit 300 Dezimalstellen berechnet werden soll, benötigt ein klassischer (1 GHz) Rechner dafür 6 Millionen Jahre. Ein Quantenrechner (1 MHz) mit Shor-Algorithmus würde hierfür lediglich $2\frac{1}{2}$ Tage benötigen.
Dieses Beispiel macht verständlich warum weltweit immer mehr Teams an der Entwicklung des Quantencomputers arbeiten und steigende Geldmittel von Fonds, der europäischen Kommission, aber auch von Militärs zur Verfügung gestellt werden.
Eine wichtige Zukunftsfrage ist auch die Bauartenverkleinerung von Quantencomputern, um bei steigender Algorithmus-Anzahl vielleicht einmal mit dem klassischen Computer konkurrieren zu können. Kleinere Aufbauten können jedoch steigende Dekohärenz bedeuten - also steigende Wechselwirkung von Zuständen mit der Umgebung und damit einen Fehlerratenanstieg. Mit diesen Fakten bleibt abzuwarten in welcher Form schließlich der Quantencomputer in Zukunft realisiert werden wird bzw. kann.

Literatur

[1] Grafik aus www.quantiki.org

[2] Nielsen, M.A., Chuang, I.L. Quantum Computation and Quantum Information, *Cambridge University Press*

[3] Raussendorf, R., Browne, D.E. & Briegel, H.J. Measurement-based quantum computation on cluster states *Physical Review A* **68** 1-32 (2003)

[4] Walther, P., Resch, K.J., Rudolph, T., Schenk, E., Weinfurter, H., Vedral, V., Aspelmayer, M. & Zeilinger, A. Experimental one-way quantum computing *Nature* **434**, 169-176 (2005)

[5] www.quantum.univie.ac.at/publications

[6] Ignacio, J., Zoller, P. Grundlagen des Quantencomputings mit quantenoptischen Systemen *Physik Journal* **4** 31-36 (2005)

[7] Homepage der Universität Innsbruck

[8] www.pi5.uni-stuttgart.de/lehre/hauptseminar2001/Quantencomputer

[9] www.weltderphysik.de/de/1072.php

[10] www.sciencedaily.com

[11] www.phys.uu.nl

[12] Grover, L.K. Quantum Mechanics helps in searching for a needle in a haystack, *Physical Review Letter* **79**, 325-328 (1997)

[13] Shor, P.W. Polynominal-Time Algorithmus for Prime Factorization and Discrete Logarithmus on a Quantum Computer, *SIAM Journal on Computing* **26** 1484-1509 (1997)