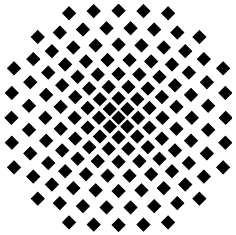
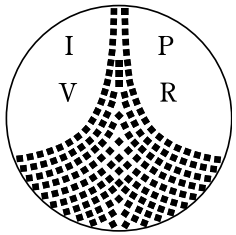




Universität Stuttgart

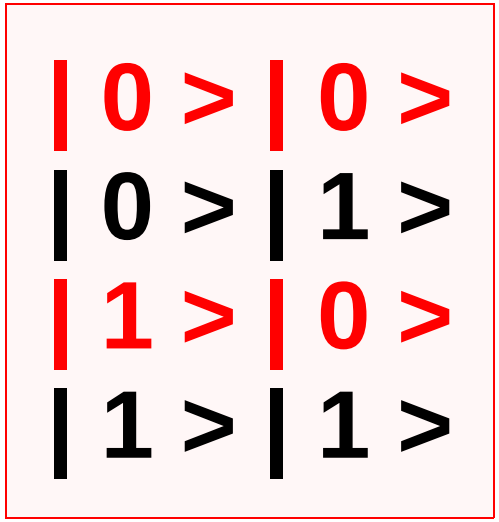
Institut für Parallele und
Verteilte Systeme (IPVS)

Universitätsstrasse 38
D-70569 Stuttgart

Quanten-Computer

Dr.rer.nat. Rainer Böhm / IPVS
Universität Stuttgart

Zusatz-Folien zur Vorlesung „Periphere Geräte“
WS 2003/04



Inhaltsverzeichnis

1.1 Die Idee des Quantums

- Die alten Griechen: Demokrit und die Idee des ατομοσ (das Unteilbare)
- Euklid und Ptolemaios: „Irgend etwas geht von meinem Auge zum Objekt und damit sehe ich“. Aristoteles und die „Atomisten“: Nein, es ist umgekehrt
- Die Araber: „Wenn ich lange genug in die Sonne sehe, dann sind meine Augen kaputt, also kommt der Strahl von der Sonne und nicht umgekehrt“ (Abu Ali al-Hasan Ibn al-Haytam = Al Hassan, Basra 956 n.Chr.)
- 1672: Newton gegen Huygens und Hooke, Welle oder Teilchen?
- 1801 Thomas Young: Doppelspalt-Experiment mit Licht = Wellennatur nachgewiesen
- 1900 Max Planck: Strahlungsgesetze, erster Hinweis auf Quantennatur. Planck liebt trotzdem das Kontinuum!
- 1905 Einstein: Photoelektrischer Effekt, Licht ist kein Kontinuum, es ist in Päckchen (= Quanten) aufgeteilt
- 1925/26: Schrödinger (Differentialform), Heisenberg: Matrizen-Ausdrücke, beide Formen gleichwertig

1.2 Erste Ansätze: Feynman, Deutsch, Shor

- **1982**: Erste Ideen für Quantum Computing durch Feynman (Caltech): Simulation von quanten-mechanischen Objekten durch andere Quantensysteme
- **1985**: David Deutsch (University of Oxford): Theoretische Arbeit, wie ein Quanten-Computer aufzubauen wäre. Daraufhin Jagd, was man denn so rechnen könne mit QC, ausser alles, was mit Quantenmechanik zusammenhing, keine konkreten Vorschläge. QC ist also mehr eine akademische Kuriosität.
- **1994**: Peter Shor (AT&T Bell Labs) veröffentlicht den ersten effizienten Quanten-Algorithmus zur Faktorisierung, dies war die „killer application“. Nun geht es auch dem beliebten RSA-Krypto-Code an den Kragen (bisher unknackbar)

Universität Stuttgart
Institut für Parallele und
Verteilte Systeme (IPVS)

Zum Dualismus Welle-Teilchen

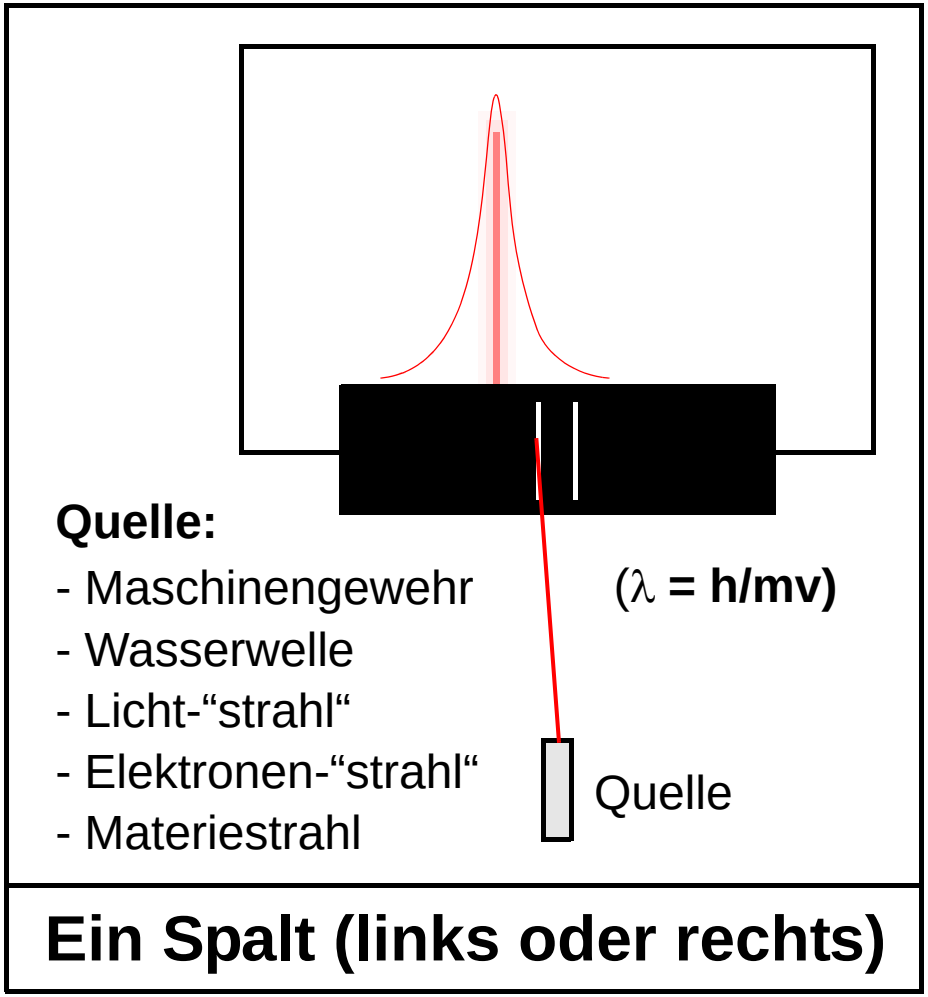
$\lambda = h/mv$

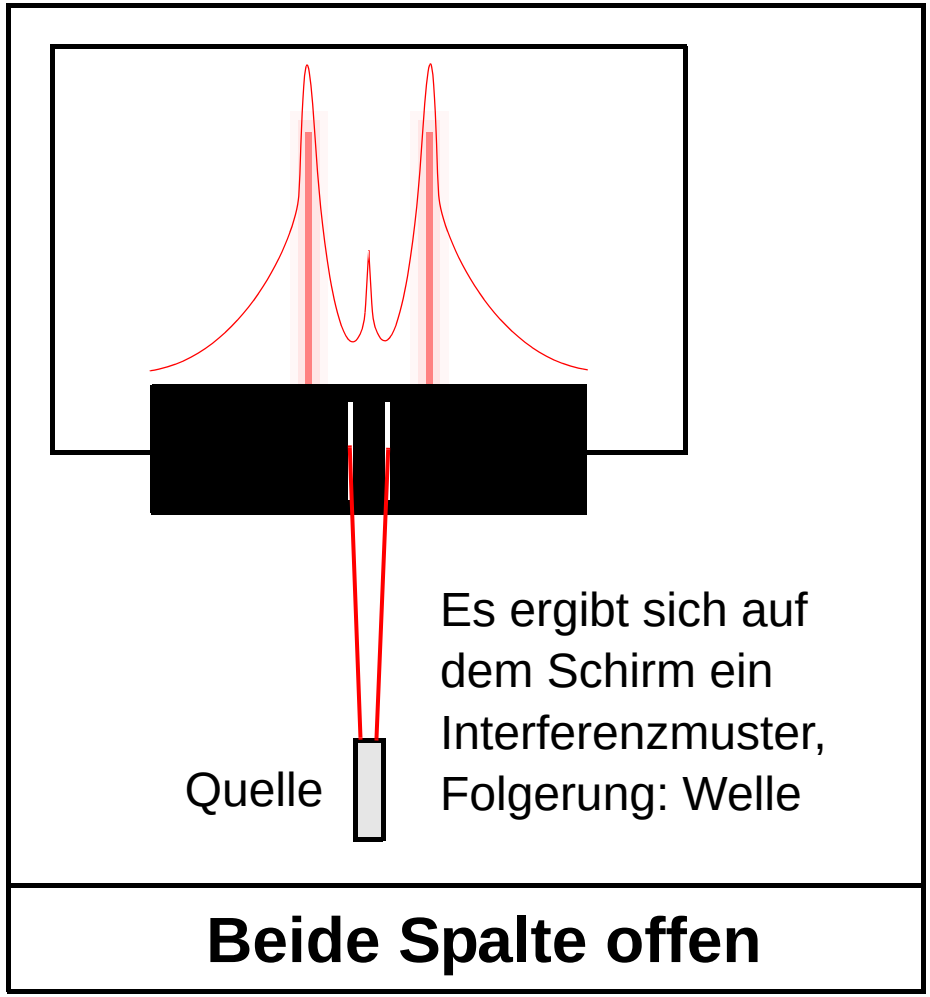
$h = 6.62*10^{-34}$ [kgms^{-1}]

Wasserstoffatom: Masse aus Atomgewicht/Zahl der Teilchen je Mol, Geschwindigkeit aus Wärmebewegung, h ist das Planck´sche Wirkungsquantum, man erhält $\lambda = 10^{-8}$ cm, somit ist das Wasserstoff-Atom als Teilchen zu behandeln

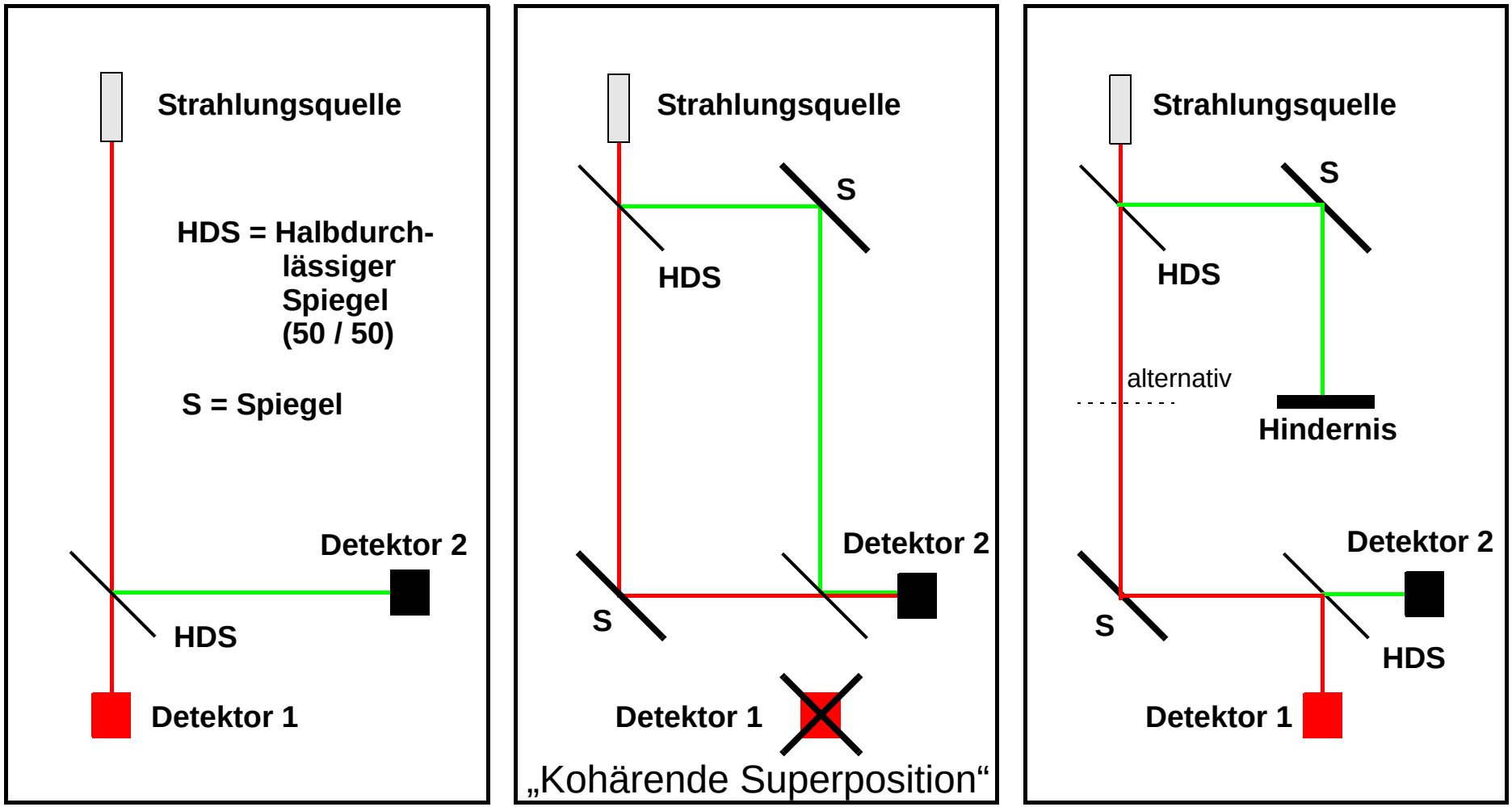
Elektron: Masse kleiner, Geschwindigkeit wesentlich grösser, somit sowohl als Welle, als auch als Teilchen zu behandeln (λ = 7 nm für v = 0.1*c)

2.2 Doppelspaltversuche





2.3. Grundlegende Versuche zur Quantennatur



Mach-Zehnder-Interferometer (schon über 100 Jahre alt, auch heute noch verwendet)

2.4 Begriffe: Verschränkung

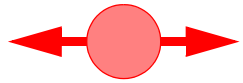
- Verschränkung = Zwei Teilchen (Elektronen, Photonen, Protonen, aber keine Neutronen wg. WW) sind mit einander verbunden. Wenn eines verändert wird, betrifft dies auch den Partner.
- Schickt man beispielsweise ein Photon durch einen Kristall, so können zwei Photonen mit jeweils der halben Energie entstehen. Allerdings bewegen sich beide Photonen in entgegengesetzte Richtungen, wobei ihre Polarisation zunächst unbekannt bleibt. Durch Messung wird die Polarisationsrichtung eines Teilchens festgestellt, das andere hat dann die entgegengesetzte.
- Diese Erscheinung wurde durch Einstein, Podolsky und Rosen entdeckt und trägt daher den Namen „EPR-Paradoxon“.
- Und jetzt wird es spannend: Die Entfernung beider Teilchen spielt keinerlei Rolle, ohne eine messbareZeit geschieht die Veränderung. Folgerung: Die Information zwischen den verschränkten Teilchen kann nicht durch Photonen (mit Lichtgeschwindigkeit) übermittelt werden, wobei wir wieder bei der Frage wären: „Was ist das V a k u u m ?“

2.5 Begriffe: Superposition und Dekohärenz

- Klassisch: Ein Teilchen kann zwar verschiedene Zustände haben, aber nur **einen** zu einem Zeitpunkt.
- Ein Photon hat somit nur eine der beiden Polarisationen.
- Quantenmechanisch: Ein Teilchen kann eine Aufenthaltswahrscheinlichkeit zwischen verschiedenen Zuständen haben, dies wird (kohärende) Superposition genannt. Will man den momentanen Zustand wissen, dann muss gemessen werden, dadurch wird der Zustand des Teilchens „eingefroren“ auf einen der beiden möglichen Zustände und auch konserviert. Dies wird Dekohärenz genannt.
- Eine Messung ist immer eine Interaktion mit der „Umwelt“, auch wenn ein Photon ins Auge trifft.
- Zusätzlich ist jedes „Klonen“ (= Verdoppelung von beliebigen Quantenzuständen) eine Messung und wegen der Dekohärenz eine Zerstörung der Superposition, somit nicht möglich

Verschränkung

Klassisch: Reine Zustände



Superposition

2.6 Verbotener Eingriff in die Messung

Geschlossener Kasten mit folgendem Inhalt:

Eine lebende Katze

radioaktive Substanz

Zählrohr

Hammer

Giftgas

Wenn das Zählrohr einen radioaktiven Zerfall misst, dann betätigt es einen Hammer, dieser zerschlägt eine Ampulle mit Giftgas und die Katze stirbt.

Da der Kasten geschlossen ist (während der laufenden Messung), ist nicht bekannt, ob die Katze lebt oder tot ist (Zwischenzustand). Erst wenn die Messung beendet ist, kann der Kasten geöffnet werden: Katze lebt oder ist tot.

Schrödingers Katze (1935)

2.7 Zusammenfassung

In der Quantenmechanik ist es möglich, dass sich ein Teilchen in einem sogenannten **Überlagerungszustand** (Superposition) befindet. Betrachten wir zum Beispiel den Ort: So kann es sein, dass sich das Teilchen an keinem bestimmten Ort befindet. Das liegt nicht an unserer Unkenntnis des Systems, sondern daran, dass sich das Teilchen "gleichzeitig" an mehreren Orten aufhält. Messen wir nun allerdings den Ort eines Teilchens, so stellen wir fest, dass es sich dann nur an einem einzigen Ort aufhält. Wie kann das sein? Wie kann ein Teilchen, das sich erst in einem Überlagerungszustand befand, nach der Messung einen konkreten "Ortszustand" einnehmen?
Ende der 20er Jahre entstand um den dänischen Wissenschaftler Niels Bohr die bis heute verbreitete **Kopenhagener Deutung**. Danach führt die Messung durch einen "bewussten" Beobachter dazu, dass das Teilchen, das sich zuvor in einem Überlagerungszustand befand, abrupt in einen der möglichen Zustände "springt" (**Kollaps der Wellenfunktion**). Diese Deutung führte zu dem paradoxen und immer noch häufig zitierten Gedanken-Experiment von Schrödinger aus dem Jahr 1935 - der Ortszustand wird durch die Messgröße "tot" oder "lebendig" ersetzt: In einer nicht einsehbaren Kiste ist eine Katze eingesperrt (**Schrödingers Katze**), die einem Überlagerungszustand aus "lebend" und "tot" ausgesetzt ist. Erst die Messung durch einen **bewussten Beobachter** führt dazu, dass die Katze entweder lebendig oder tot ist.
In den letzten Jahren wurde die Kopenhagener Deutung mehr und mehr von der Theorie der **Dekohärenz** verdrängt. Demnach kollabiert die Wellenfunktion nicht erst durch einen Beobachter, sondern durch Wechselwirkungen des Systems mit der Umgebung. Der Mechanismus der Dekohärenz kann quantenmechanisch beschrieben werden. Die Dekohärenz-Zeit, also die Zeit, die das System zum Kollabieren benötigt, ist umso kürzer, je größer die Masse des Systems ist. Für Schrödingers Katze schafft das Klarheit: Sie muss nur noch unmerklich kurz in einem Überlagerungszustand aus lebendig und tot verharren. Je wohlgenährter sie ist, desto schneller fällt die Entscheidung. Sie braucht keinen Beobachter mehr, der sich ihrer erbarmt und nach ihr sieht.
Zurek, einer der Entwickler dieser Theorie, hat in einer neulich veröffentlichten Rechnung [W.H. Zurek, Nature **412**, 712-717 (2001)] die Empfindlichkeit eines Quantensystems gegenüber Wechselwirkungen mit der Umwelt und damit die Effektivität der Dekohärenz ermittelt. Er zeigte unter anderem, dass chaotische Systeme eine besonders kurze Kohärenz-Zeit besitzen. Heißt für die Katze: Je fetter und chaotischer, desto schneller ist sie hin.
Nach: www.quanten.de/schroedingers_katze.html

3.1 Klassisch: Von Neumann / Turing

- Hier findet sich alles, was ein Informatiker so im Laufe des Studiums lernt, aber immer auf der Basis von zweiwertigen Bits. Ausserdem ist alles deterministisch.
- Das Bit als kleinste Informationseinheit ist entweder „NULL“ oder „EINS“
- Bei einem klassischen Computer ist die Operation fest verdrahtet und die Bits fliessen als Strom zu den Operationen

- Beim Quantencomputer dagegen sind die Bits an einer „festen“ Stelle und die Operationen kommen als Energie-Impulse zu den Bits. Daher muss die erforderliche Programmierung gänzlich anders verlaufen

3.1 Das Qubit, Notationen

- Ein Quantenbit (Qubit) hat nicht nur den Zustand „NULL“ oder „EINS“, sondern es kann beide Zustände gleichzeitig einnehmen. Normalerweise geht man von einer Wahrscheinlichkeit von 50% für beide aus. Wahrscheinlichkeitswerte werden in der Quantenmechanik mit folgender (Teil)-Notation geschrieben:
- **|0> und |1>**

- Ein Quantenregister mit zwei Qubits kann somit folgende Information gleichzeitig repräsentieren:
- Binär: **|0>|0>, |0>|1>, |1>|0>, |1>|1>** oder
- Dezimal: **|0>, |1>, |2>, |3>** , Klassisch wird nur ein Wert durch Messung ausgelesen, keine Superposition mehr
- Bei zwei Qubits beträgt die Wahrscheinlichkeit für jeden Zustand 1/4 = 25%

3.2 Register mit 4 Qubits

$$a_0|0000> + a_1|0001> + a_2|0010> + a_3|0011> + a_4|0100> + a_5|0101> + a_6|0110> + a_7|0111> + a_8|1000> + a_9|1001> + a_{10}|1010> + a_{11}|1011> + a_{12}|1100> + a_{13}|1101> + a_{14}|1110> + a_{15}|1111>$$

alle 16 Zustände sind

mit einer Wahrschein-

lichkeit von 1/16

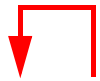
g l e i c h z e i t i g

darstellbar.

3.3 Gatter

- Ein Gatter ist klassisch eine Elementar-Operation. Schafft man es, eine solche Operation auf ein Qubit-Register anzuwenden, dann sind aufgrund der Superposition a l l e Zustände gleichzeitig ansprechbar, bzw. änderbar.
- Das einfachste Gatter, auch in der Quantencomputerei ist das NOT-Gatter, man könnte auch sagen, der Inverter.
- **Einbit-NOT-Gatter:** **|0> → |1> und |1> → |0>**

- **Zweibit-Gatter** (kontrolliertes NOT). Es ist weder ein XOR, noch ein XNOR!!
- Hier bestimmt das zweite Qubit, das sog.Kontrollbit, mit seiner Wertigkeit die Wahrscheinlichkeitsbesetzung des ersten Qubits (das zweite Qubit wird also auf das erste Qubit „angewendet“)



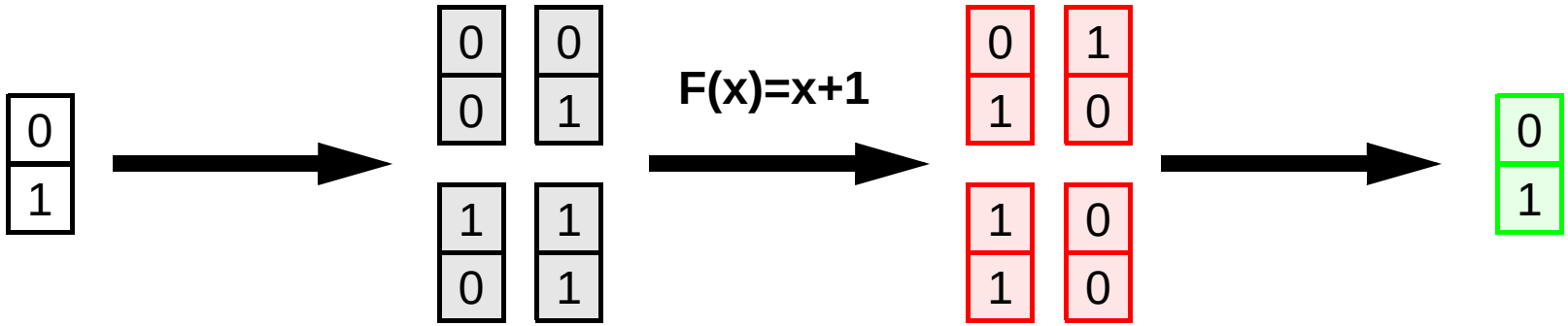
|0>|0> → |0>|0>
|1>|0> → |1>|0>
|0>|1> → |1>|1>
|1>|1> → |0>|1>

„Wirkt“ nur, wenn das Kontrollbit = 1 gesetzt ist

Dies erinnert sehr an das MRAM mit 4 Anschlüssen

4.1 Funktionen 1,

In Anlehnung an die aus ADD und KOMPLEMENT zusammensetzbaren vier Grundrechenarten beim Von-Neumann-Rechner lassen sich auch beim Quantencomputer durch Hintereinanderschalten von Elementargattern („Anwenden“ der Grundfunktionen) mathematische Funktionen realisieren.Die Superposition bleibt dabei erhalten, das „bearbeitete“ Register enthält nach der Anwendung nicht mehr die ursprünglichen Wahrscheinlichkeitswerte, sondern die zugehörigen Ergebnisse. **Vergleichbar einem Ein-Adress-Befehl**



Schritt 1:

Das Register ist im klassischen Grundzustand mit **|0>|0>**

Schritt 2:

Superposition aller möglichen Zustände alle Zustände mit gleicher Wahrscheinlichkeit

Schritt 3:

Die Funktion F(x)=x+1 wurde auf das Register angewendet. Dadurch wird der Inhalt verändert.

Schritt 4

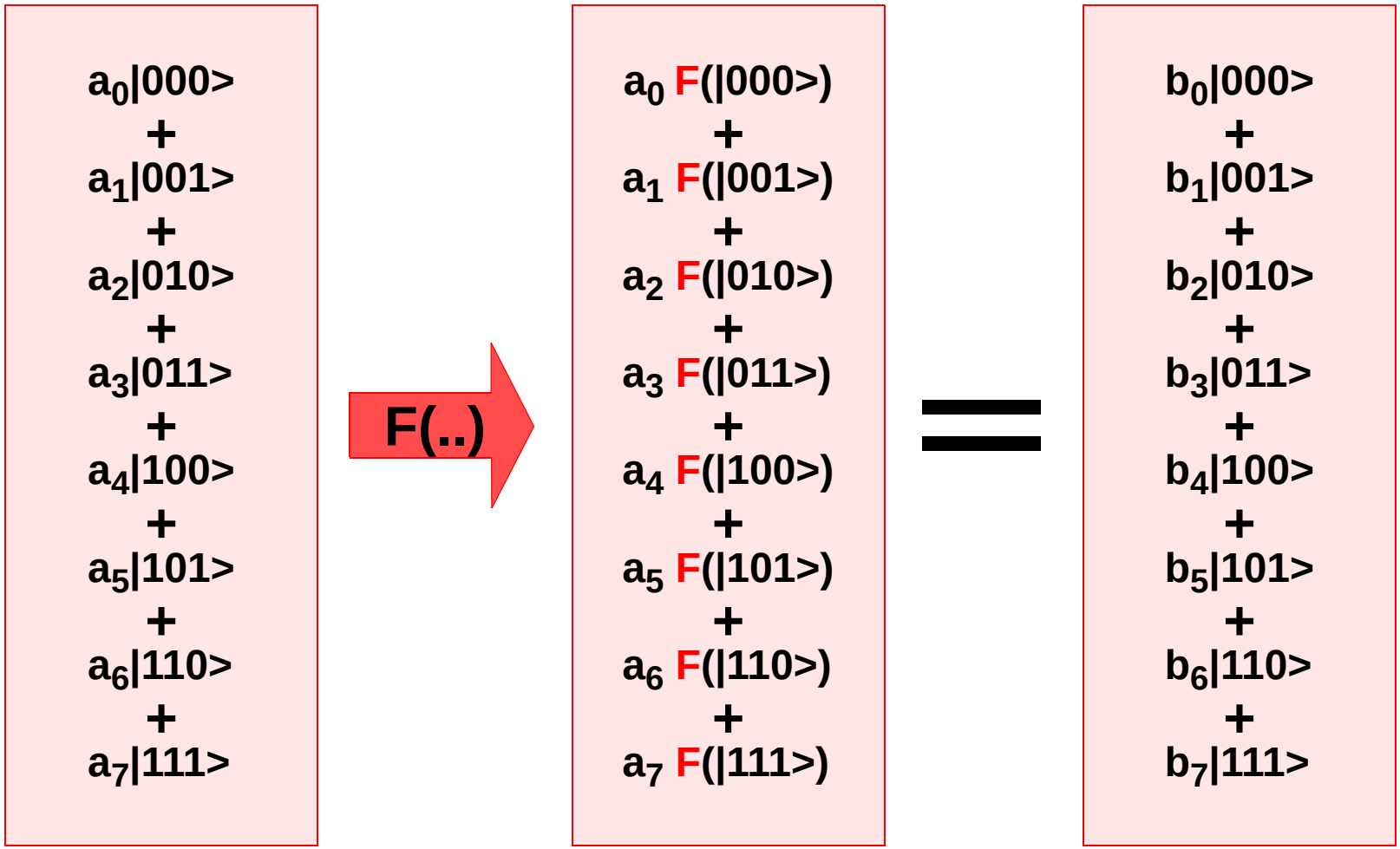
Das Register ist wieder im klassischen Grundzustand und enthält das Ergebnis

4.1.1 Funktionen 2, Mehrregister-Prinzip

Zwei-Adress-Prinzip: |x> ist für die Eingangswerte, |y> ist für die Ausgangswerte. Wegen der durch die Berechnung erfolgende Verschränkung wird bei Messung des einen Register auch das andere verändert. Nach der Messung enthält das zweite Register nur noch die Werte, die der Messung des anderen Registers entsprechen

- $|x\rangle|0\rangle \rightarrow |x\rangle|y = f(x)\rangle$ Im ersten Register stehen die zu berechnenden Werte, ins zweite werden die Ergebnisse geschrieben
- $|x\rangle|y\rangle \rightarrow |j\rangle|y = f(j)\rangle$ Das erste Register mit |x> wird gemessen, dadurch enthält das zweite Register nur noch Werte, die von |f(x)> für j zurückgeliefert werden.

4.2 Funktionen 3



Klassisch:
8 Register für 8 Werte

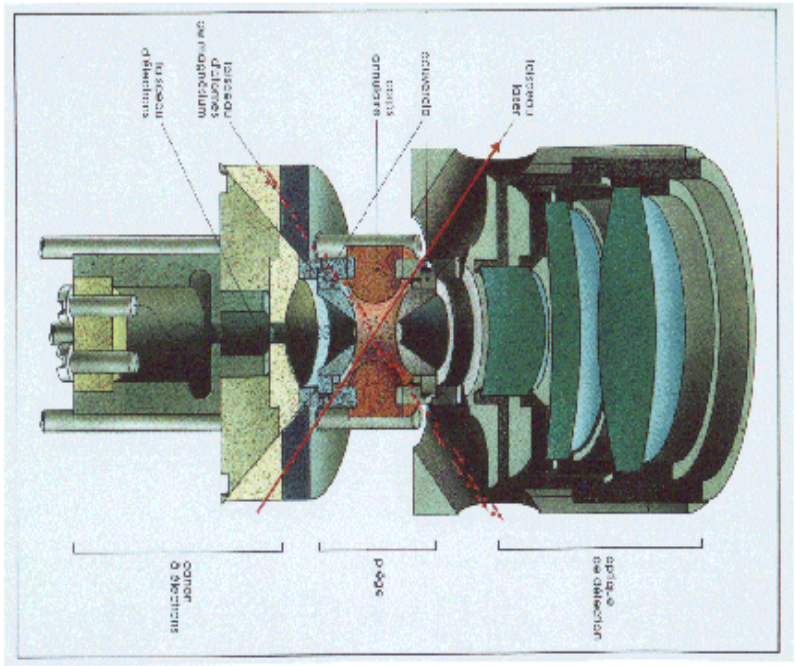
Qubits:
1 Register gleichzeitig für 8 Werte

Allgemein:
1 Register der Länge L kann 2^L Operationen gleichzeitig ausführen

Input-Register **Output-Register**

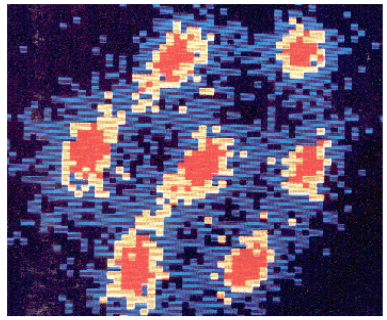
4.3 Praxis: Die Ionenfalle (Paulfalle)

Walther: Falle

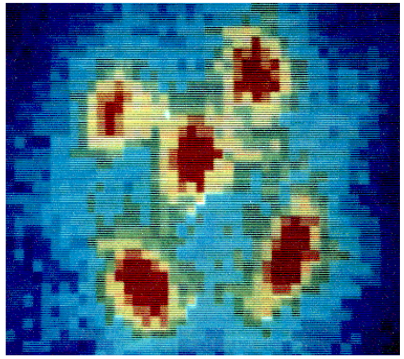


Othmar Marti, Experimentelle Physik, Universität Ulm

Walther: 7 Ionen in Paul-Falle



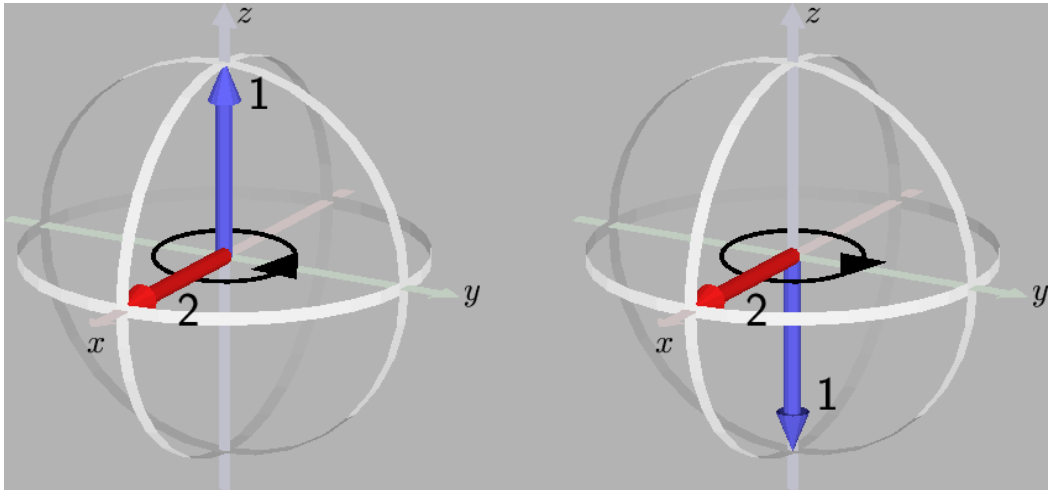
Walther: Phasenübergänge von 5 Ionen in Paul-Falle



Othmar Marti, Experimentelle Physik, Universität Ulm

4.4 Kernspin-Resonanz

Tatsächlich konnte die deutsch-amerikanische Forschergruppe, der Steffen Glaser (Garching) angehört, im letzten Jahr die Kapazität von Quantencomputern von bisher drei auf jetzt **fünf** Qubits erhöhen. Für die Realisierung ihres Quantencomputers haben die Wissenschaftler die kernmagnetische Resonanz einer eigens für diesen Zweck aus seltenen Isotopen synthetisierten Verbindung mit fünf gekoppelten Kernspins ausgenutzt. Im starken Magnetfeld eines NMR-Spektrometers richten sich die Kernspins der Verbindung ähnlich wie Kompassnadeln im Erdmagnetfeld aus. Die (quantisierten) Orientierungen der Spins (parallel bzw. entgegengesetzt zum Magnetfeld) entsprechen den Zuständen 0 und 1 der Qubits, die durch die Einstrahlung von Radiofrequenzen gezielt manipuliert werden können. Das »Computerprogramm« des Quantencomputers besteht demnach aus einer bestimmten Abfolge definierter Radio-frequenz-Impulse, die das Ergebnis der Rechnung festschreibt.

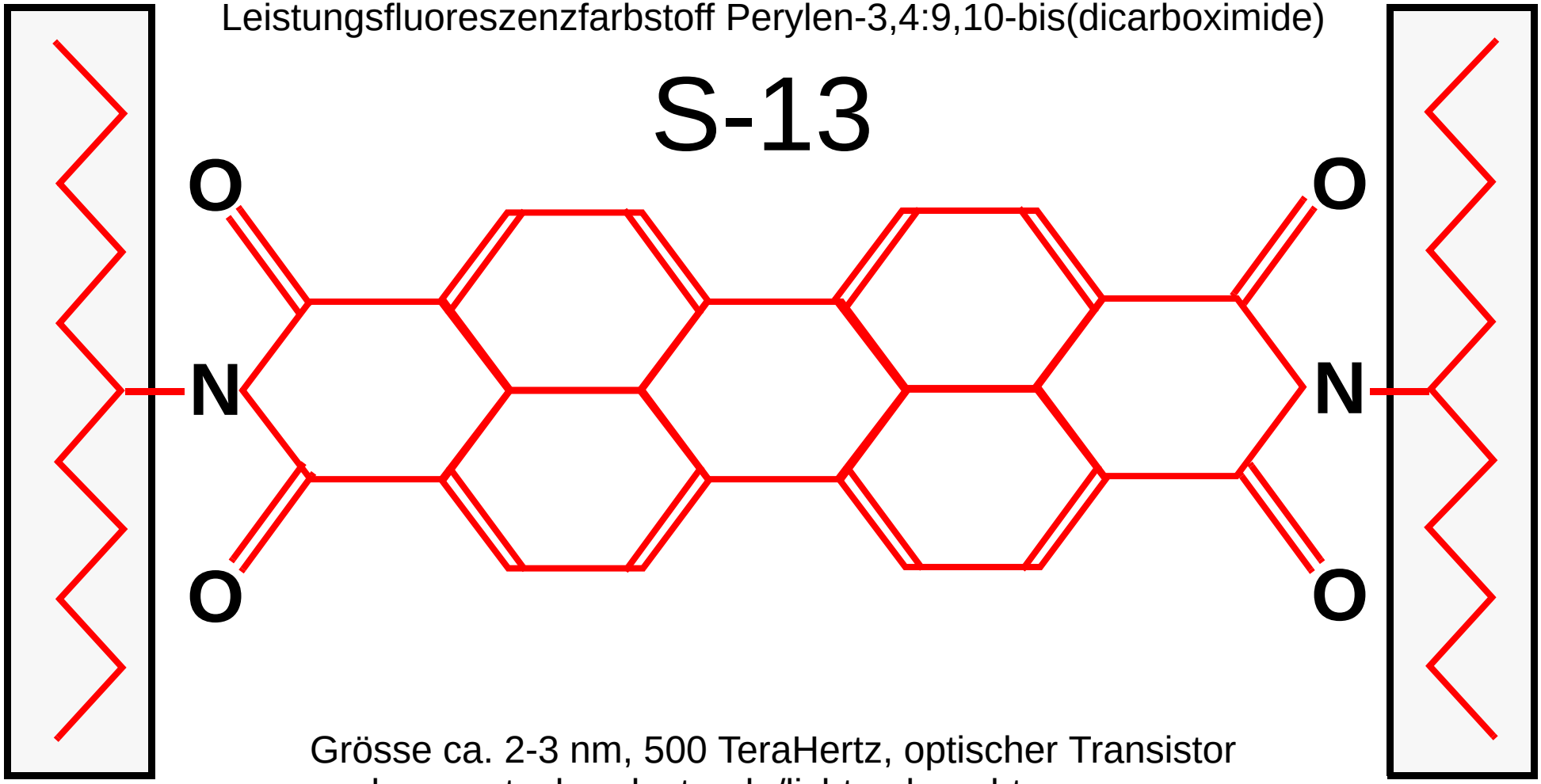


Der aus fünf Qubits bestehende NMR-Quantencomputer hat als Beispiel für einen Quantenalgorithmus den »Deutsch-Josza-Algorithmus« erfolgreich ausgeführt. Im Gegensatz zu konventionellen Rechenverfahren erlaubt dieser Algorithmus, konstante und ausgeglichene Funktionen in einem Schritt zu unterscheiden, wie ein Beispiel aus der Mustererkennung verdeutlicht: Um die Echtheit einer Münze zu erkennen, müsste ein normaler Computer beide Seiten der Münze nacheinander testen. Ein Quantencomputer könnte diese Aufgabe mit Hilfe des Algorithmus' in einem Schritt und damit wesentlich schneller bewältigen.

4.5 Optical Computing als Konkurrenz?

Leistungsfluoreszenzfarbstoff Perylen-3,4:9,10-bis(dicarboximide)

S-13



Grösse ca. 2-3 nm, 500 TeraHertz, optischer Transistor
nach: www.technodoctor.de/lichtrechner.htm

4.6 Simulationen Bottom up / Top down

- Man kann gegenwärtig bereits Quanten-computer auf von Neumann-Rechnern simulieren, wenn auch mit langen Lauf-zeiten.
- Umgekehrt geht es selbstverständlich auch, auf einem Quantencomputer einen Von-Neumann-Rechner zu simu-lieren, ob das noch Sinn macht, bleibt offen.

5.1 Knödel / Zemanek ca. 1955

Prof. Knödel hat einmal folgende Episode erzählt: Er war Assistent beim grossen Mathematiker Zemanek in Wien. Eines Tages brachte er seinem Chef voller Stolz die neuesten Listings von bis dahin noch nicht berechneten höheren Funktionen und äusserte gleichzeitig den Wunsch, auch einen solchen Rechner in Wien zu haben. Darauf Zemanek: „Wieso brauchen wir denn noch selbst einen Computer, es ist doch jetzt alles wesentliche tabellarisch berechnet“.

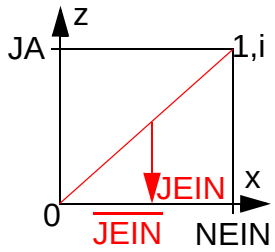
In einer ähnlichen Lage befindet man sich gegenwärtig beim Rechnen mit dem Quantencomputer.

5.2 Quantenalgorithmen

Die Babbage „Differential Engine“ konnte dasselbe wie z.B. eine moderne Connection Machine, nur eben sehr viel langsamer.

Ein Quanten-Algorithmus kann nicht korrekt auf klassischen Maschinen laufen wegen der geforderten Superposition.

Veranschaulichung nach Prospiech: Man berechne SQRT(NOT) in der komplexen Ebene:



Eingang		Ausgang	
| 0 >	JA	½((1+i)|0> + (1-i)|1>)	JEIN
| 1 >	Nein	½((1-i)|0> + (1+)|1>)	$\overline{\text{JEIN}}$

Koordinaten-Transformation von der Basis <(1,0),(0,1)>

in die Basis <½(1+i,1-i),½(1-i,1+i)>

5.3 Shor, Fourier-Transformation

? * ? = 960.391 (hattu Zeit ?)

977*983 = ? (hattu Bleistift, ca. 1 min)

RSA-Code: Basis ist eine 129-stellige Primzahl. Angeblich unknackbar, da 40 Billiarden Jahre (=$4*10^{13}$ Jahre) Rechenzeit erforderlich. Letztes Jahr durch Zusammenschalten von 600 PC´s dummerweise geknackt!!

Übliche Methode: Gegeben N. Man dividiert durch alle Werte zwischen 1 und $N^{½}$. Ein Rechner, der in der Sekunde 10^{10} Teilungen schaffen würde, bräuchte für eine 100-stellige Zahl länger als die Dauer des Universums. Dabei gibt es diesen schnellen Rechner noch gar nicht.

Nach Shor werden zuerst alle möglichen Werte aus einem Register in einer Superposition aller möglichen Werte 1, 2, 3, 4, ... errechnet. Das Ergebnis kann nicht durch eine Messung abgefragt werden, sondern muss mit den Methoden der „Quanten Fourier-Transformation“ ermittelt werden.

5.4 Grover´scher Such-Algorithmus

- Anschauliches Beispiel: In einem undurchsichtigen Sack mit weissen Kugeln ist eine rote Kugel versteckt. Man greift blind in den Sack und zieht eine Kugel nach der anderen heraus, bis man die rote endlich erwischt hat. Bei N Kugeln im Mittel N/2 Schritte.

- Grover nimmt einen durchsichtigen Sack (Superposition) und breitet ihn einlagig aus, damit kann man die Kugel sofort lokalisieren. Bei N Kugeln 1 Schritt (mit dem richtigen Quantencomputer)

5.5 Math. Nachbemerkung

Die Menge aller Superpositionen der zwei Basiszustände $|0\rangle$ und $|1\rangle$ ist ein zweidimensionaler Vektorraum (im Fachjargon: Hilbertraum). Die Menge $\{|0\rangle, |1\rangle\}$ bildet eine **Basis** dieses Raums (woher auch die Bezeichnung Basiszustände kommt). Die Koeffizienten a und b dürfen komplexe Zahlen sein. Manchmal werden diese beiden Zahlen in Form eines Spaltenvektors

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

zusammengefasst, um den Zustand zu repräsentieren. Die Basiszustände $|0\rangle$ und $|1\rangle$ werden dann durch die beiden Einheitsvektoren

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

dargestellt. Diese Form ist beim Rechnen mit Zuständen manchmal recht praktisch.

Nach: www.quanten.de/

5.6 Schwerkraft-Simulation mit dem QC

In einem geschlossenen Würfel befinden sich N identische Masse-Teilchen (z.B. 100*100*100). JedesTeilchen hat einen „randomized“ Impuls und prallt irgendwann mit einem anderen Teil-chen zusammen und tauscht mit diesem seinen Impuls aus. Dann fliegen beide mit geänderten Richtungen weiter. Gibt es eine Zusammenballung von Materie und wie wie lange muss man simulieren, um das nebenstehende Ergebnis zu erhalten?

Statt $N*10^6$ Schritten nur noch N*1 Schritte

6. Forschungsstätten (ganz kleine Auswahl)

- Universität Heidelberg
- Max Planck Institute
- Universität Innsbruck
- Los Alamos National Laboratory
- Mass. Institute Technology (MIT)
- Caltech
- Microsoft

7. Literatur zu Quantencomputern

1. D.Deutsch, A.Ekert: „Quantum Computation“, Physics World, March (1998)
2. D.Deutsch: Proc. Roy. Soc. London, Ser. A **400**, 97 (1985)
3. Richard P.Feynman, Int. J. Theor. Phys. **21**, 467 (1982)
4. P.W.Shor: „Algorithms for quantum computation: Discrete logarithms and factoring“, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press (1994)
5. Lov K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, p.212-219, May 22-24, 1996, Philadelphia, Pennsylvania, United States
6. J.Gruska: Quantum Computing, McGraw Hill, 1999
7. G.Prospiech: www.rz.uni-frankfurt.de/~prospiech/q_comp.html
8. www.ap.univie.ac.at/users/fe/quantencomputer
   www.ap.univie.ac.at/future.media/qu/quantentheorie.html (Animation zum Spiegelexp.)
   Bester zusammenfassender Beitrag auf dem Internet von Franz Empacher,