1 Physik der Informationsverarbeitung

1.1 Einführung

1.1.1 Das Moore'sche Gesetz

Die Entwicklung der Mikro-und Optoelektronik und die damit verbundenen Digitalisierung von Information basiert auf Verbesserungen bei der Herstellung von Halbleitern, welche dazu geführt haben, dass immer kleinere und schnellere Komponenten auf einer gegebenen Fläche untergebracht werden können. Schon 1965 bemerkte Gordon MooreMoore [2], damals Forschungsdirektor bei Fairchild Semiconductor, später Mitgründer von Intel, dass die Zahl der Komponenten, welche auf eine gegebene Fläche gepackt werden konnten, exponentiell mit der Zeit zunahm, und dies im Wesentlichen konstant über viele Jahre.

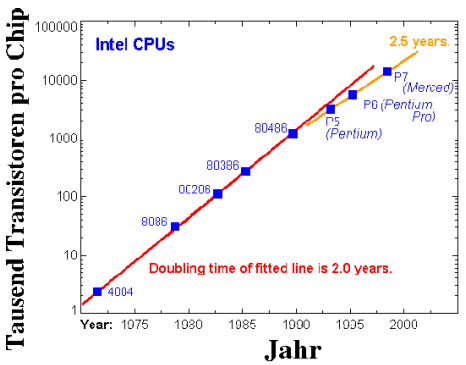

Abbildung 1.1: Das Moore'sche Gessetz: Entwicklung der Strukturgrößen über die Zeit von 1970 bis 2000.

Die bedeutete eine entsprechende Reduzierung der Strukturgrößen. Dieser Trend setzte sich auch in den 40 Jahren seit Moore's Publikation fort, nur mit geringer Abschwächung. Aktuell liegt die Strukturgröße der Halbleiterchips bei etwa 60 nm, und sie nimmt pro Jahr um etwa 12 % ab.

Wenn wir diesen Trend in die Zukunft extrapolieren, so könnte er sich noch rund 40 Jahre weiter fortsetzen, bis die ultimative Grenze erreicht ist, bei der die einzelnen Transistoren die Größe eines Atoms erreicht haben. Allerdings werden schon wesentlich früher die Schaltelemente der Halbleiterindustrie nicht mehr so funktionieren wie heute, sondern wir werden einen Bereich erreichen, wo die Funktionsweie durch die Gesetze der Quantenmechanik bestimmt wird.

1.1.2 Quantisierung der Ladung

Aufgrund der Reduktion der Größe muss auch die Betriebsspannung reduziert werden, da sonst die internen Felder $E = V/d$ die Durchbruchspannung überschreiten würden. In den nächsten Jahren wird voraussichtlich die interne Betriebsspannung der Halbleiterelektronik auf weniger als 1 V absinken. Dadurch sinkt auch die Zahl der Ladungen, welche jeweils bewegt werden. Wir nehmen als Beispiel einen Kugelkondensator. Dessen Kapazität ist

$$C = 4\pi\epsilon_0 r\,.$$

Für eine Kugel mit 50 nm Radius beträgt die Kapazität somit $C = 5 \cdot 10^{-18}$ F. Eine Spannungsänderung von 0.1 V bewegt in einem solchen System eine Ladung von $5 \cdot 10^{-19}$ C. Die Elementarladung beträgt $e = 1,6 \cdot 10^{-19}$ C, d.h. unter diesen Bedingungen würden nur noch etwa 3 Elektronen bewegt.

Die Grenze, bei der nur noch einzelne Elektronen bewegt werden, wurde in Labor-Experimenten bereits erreicht (siehe Fig. 1.2), allerdings bei sehr tiefen Temperaturen. Die Kapazität von wirklichen Strukuren ist zwar wesentlich höher als die eines Kugelkondensators. Trotzdem wird man sich auch dort anstrengen müssen, da bald

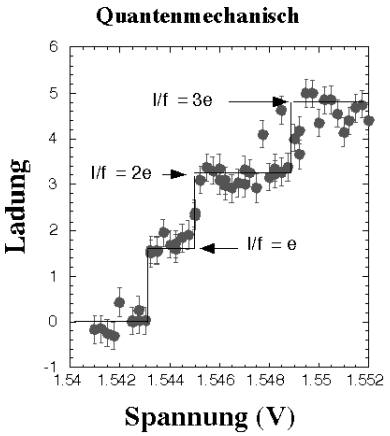

Abbildung 1.2: Bewegung einzelner Elektronen auf einem Kondensator.

nur noch wenige Elektronen pro Schaltzyklus bewegt werden.

Wenn die Dimensionen der Schaltelemente in den Bereich von wenigen nm reduziert werden, beginnt sich auch bemerkbar zu machen, dass Elektronen keine Punktteilchen sind. In diesem Bereich werden z.B. die Welleneigenschaften der Elektronen relevant.

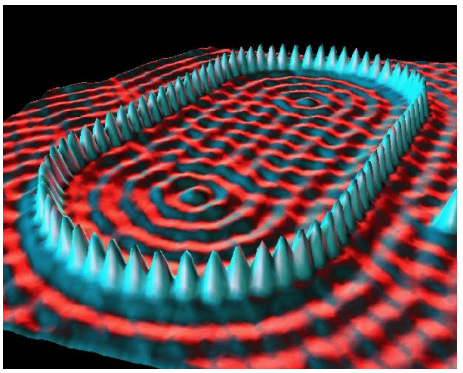

Abbildung 1.3: Der Quanten-Korall von Crommie, Lutz & Eigler (IBM).

Dies kann man z.B. in Figur 1.3 sehr schön beobachten. Hier wurden Eisenatome auf eine Kupferoberfläche aufgebracht und mit Hilfe eines Raster-Tunnelmikroskop in der Form eines Ovals angeordnet. Die resultierende Struktur wurde anschließend ebenfalls mit Hilfe des Rastertunnelmikroskops abgebildet. Im Bereich zwischen den Eisenatomen sieht man deutlich, wie die Elektronen wellenförmige Strukturen bilden.

1.1.3 Energieverbrauch

Entwicklungen, die dem Moore'schen Gesetz ähneln gibt es in unterschiedlichen Bereichen. Eine besonders eindrückliche Version davon ist die Entwicklung des Energieverbrauchs pro Schaltzyklus, wie sie in Figur 1.4 dargestellt ist.

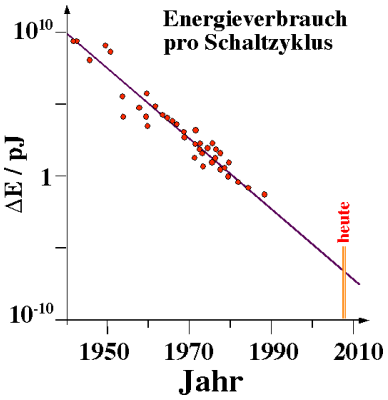

Abbildung 1.4: Entwicklung des Energiverbrauchs pro Schaltzyklus in Mikroprozessoren.

Wie in der Figur gezeigt, hat der spezifische Energieverbrauch in den letzten Jahrzehnten um 15 Größenordnungen abgenommen. Dies ist eine der wichtigsten Entwicklungen: würden unsere heutigen Rechner die Effizienz eines Rechners von 1945 haben, so würden sie statt rund 100 W etwa 100.000.000 GW an elektricher Leistung benötigen. Dies entspricht 100 Millionen Großkraftwerken. Auch wenn diese Leistung zur Verfügung stehen würde, wäre es nicht möglich den Rechner zu betreiben: bei dieser Leistung wird ein Liter Wasser in $4,2\,\mathrm{ps}$ zum Kochen gebracht, oder ein Mikroporzessor in weniger als einer ps (=1 Millionstel Mikrosekunden) verdampft. Auch bei der heutigen Effizienz ist die Wärmeentwicklung häufig ein limitierender Faktor.

Für eine weitere Steigerung der Leistungsfähigkeit der Computer muss diese Entwicklung deshalb weiter gehen. Allerdings wird dies nicht mehr lange möglich sein: In etwa 10 Jahren wird

eine fundamentale Grenze erreicht, welche durch den Ausdruck $k_B T \ln 2$ gegeben ist. Dies entspricht der thermischen Energie eines beliebigen Freiheitsgrades. Sie beschreibt die thermische Bewegung von Molekülen in einer Flüssigkeit oder Elektronen in einem Halbleiter. In diesem Bereich könnten somit Schalter durch die thermische Bewegung ausgelöst werden. Außerdem müssen alle Rechner, welche nach den Gesetzen der Boole'schen Logik arbeiten (und das umfasst alle heutigen Rechner) mindestens diese Energie pro Schaltzyklus freisetzen. Dies gilt unabhängig davon, welches Material diese Rechner verwenden (Halbleiter, mechanische Rechner oder Supraleiter).

Diese Grenze kann jedoch überschritten werden, wenn der entsprechende Rechner nicht boole'sche Logik verwendet, sondern reversible Logik. Es gibt Möglichkeiten, reversible logische Operationen mit klassischen mechanischen Systemen zu implementieren, aber auch die Quantenmechanik ermöglicht eine reversible Implementation der Informationsverarbeitung. Sowohl die Reduzierung der Dimensionen, wie auch die Reduktion des Energieverbrauchs deuten darauf hin, dass zukünftige Generationen von Schaltkreisen direkt den Gesetzen der Quantenmechanik gehorchen werden.

Während diese Entwicklung für Ingenieure zunächst Schwierigkeiten bereitet, stellt sie auch eine große Chance dar, weil diese zukünftigen Schaltkreise nicht nur die weitere Entwicklung des Moore'schen Gesetzes ermöglichen, sondern darüber hinaus einen qualitativen Sprung in der Leistungsfähigkeit. Schaltkreise, welche nach den Gesetzen der Quantenmechanik funktionieren, sind in der Lage Quantenalgorithmen auszuführen. Damit ist es möglich, Probleme zu lösen, welche auf klassischen Computern nicht effizient lösbar sind. Auch wenn die Herstellung dieser Schaltkreise noch große Herausforderungen stellt, hat dieses Potenzial doch schon ein erhebliches Interesse für diese Zukunftstechnologie erzeugt, nicht nur unter Wissenschaftlern.

1.1.4 Historisches

Die Wurzeln der Quanteninformationsverarbeitung sind fast so alt wie die Quantenmechanik selbst. Wir sind überzeugt, dass die Quantenmechanik die fundamentale Theorie ist, mit deren Hilfe wir z.B. die eigenschaften der Materie erklären können. Damit ist sie automatisch die Grundlage für jeden Computer. Allerdings sind in den meisten Fällen klassische Mechanik, Optik, Elektrondynamik etc. ausgezeichnete Näherungen und völlig ausreichend, um die Funktionsweise der Rechner zu verstehen,

Die passendere Frage ist somit, was geschieht, wenn die Funktionsweise des Computers nur noch mit Hilfe der Quantenmechanik beschrieben werden kann und die klassischen Näherungen versagen. Eine explizite Diskussion dieser Frage begann 1982, als Benioff zeigte, dass quantenmechanische Systeme in der Lage waren, klassische Computer zu simulieren.

Im gleichen Jahr stellte Richard Feynman die gegenteilige Frage: Können klassische Computer quantenmechanische Systeme effizient simulieren? Her realisierte, dass die Zahl der Variablen, welche benötigt werden, um das System zu beschreiben, exponentiell mit der Systemgröße zunimmt. Als Beispiel betrachten wir ein System aus N Spins $1/2$. Die Dimension des zugehörigen Hilbertraums beträgt 2^N und eine darstellung des Zustandes benötigt $2 \cdot 2^N - 1$ reelle Zahlen. Jeder Rechner, der ein solches System simulieren soll, muss somit 2^N komplexe Zahlen verfolgen. Schon bei wenigen hundert Teilchen übersteigt die Zahl 2^N die Zahl der Atome im Universum und damit die Speicherfähigkeit jedes vorstellbaren Computers. Gleichzeitig wächst die Rechenzeit, die eine Simulation benötigt, exponentiell mit der Größe des Systems. Feynman kam zum Schluss, dass klassische Computer niemals in der Lage sein werden, quantenmechanische Systeme mit mehr als ein paar wenigen Teilchen zu somulieren. Natürlich beziehen sich diese Überlegungen nur auf den allgemeinen Fall. Falls die Teilchen (oder wenigstens die meisten davon) nicht wechselwirken, ist es immer möglich, die Berech-

nungen in einem kleineren Hilbertraum durchzuführen und damit die Anforderungen an die Rechenzeit erheblich zu reduzieren.

Nachdem er das Problem dargelegt hatte, bot Feynman sogleich eine mögliche Lösung an: “Quantencomputer - universelle Qunten Simulatoren”. Er zeigte, dass der drastische Anstieg des Speicherbedarfs als Konsequenz der Informationsmenge gesehen werden kann, welche in einem Quantensystem enthalten ist. Die Tatsache, dass Quantensysteme sich selber simulieren können, könne als Indiz gewertet werden, dass Quantensysteme sehr effiziente Informationsspeicher sind. Er sagte “Ich glaube, dass ein geeignetes Quantensystem in der Lage ist, ein beliebiges Quantensystem zu simulieren - einschließlich der physikalischen Welt. Er lief die Frage offen, welche Systeme wirklich simuliert werden können, und welche Simulationen nützlich sein könnten.

Ein erster Beweis dieser Vermutung wurde 1993 von Bernstein und Vazirani geliefert. Sie zeigten, dass eine quantenmechanische Turingmaschine jedes andere Quanensystem in polynomialer Zeit simulieren kann. Dies impliziert, dass Quantencomputer leistungsfähiger sind als klassische Computer. Dies war ein nicht-konstruktiver Beweis, d.h. es wr noch kein Algorithmus bekannt, der dieses Potenzial realisiert hätte.

1.2 Quantencomputer Grundlagen

1.2.1 Quantenmechanik

Die Grundlagen der Quantenmechanik wurden vor etwa hundert Jahren gelegt. Max Planck fand, dass Licht scheinbar nicht kontinuierlich ausgestrahlt wird, sondern in diskreten Paketen (=Quanten). Albert Einstein kam bei der Diskussion des Photoeffekts (d.h. bei der Absorption von Licht) zum gleichen Ergebnis. Während diese beiden Physiker die Photonen noch nicht direkt beobachten konnten, ist dies heute leicht möglich.

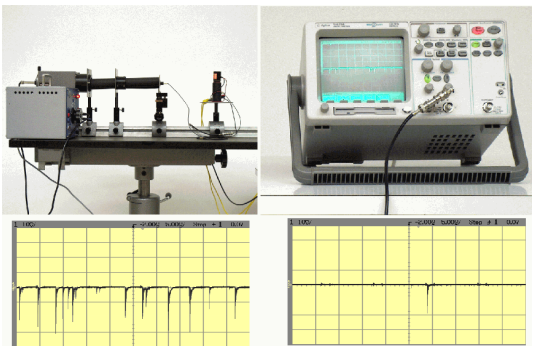

Abbildung 1.5: Messunge einzelner Photonen beim Nachweis von Licht.

Fällt nur wenig Licht auf den Detektor, so findet man keinen kontinuierlichen Strom, sondern einzelne diskrete Pulse. Jeder dieser Pulse entspricht der Absorption eines Photons. Jedes Photon besitzt eine Energie

$$E_{\text{Photon}} = h\nu\,,$$

wobei $h = 6,63 \cdot 10^{-34}$Js die Planck’sche Konstante darstellt und ν die Frequenz des Lichtes. Diese liegt im Bereich von $5 \cdot 10^{14}$Hz für sichtbares Licht, etwas höher für blaues Licht, etwas niedriger für rotes. Der Grund, weshalb wir diese diskreten Energiepakete üblicherweise nicht sehen, liegt in der großen Zahl: Bei Tageslicht fallen pro Sekunde etwa $4 \cdot 10^{21}$Photonen auf einen Quadratmeter.

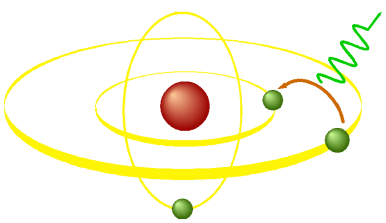

Abbildung 1.6: Aufbau eines Atoms.

Auch Atome sind Quantensysteme. Ein Atom besteht aus einem positiv geladenen Atomkern und negativ geladenen Elektronen, die sich um den Kern bewegen. Man findet, dass die Elektronen nicht auf beliebigen Bahnen um das Atom kreisen können, sondern nur auf bestimmten Bahnen, welche durch eine “Quantisierungsbedingung” bestimmt sind. Deshalb ist auch die

Energie des Atoms quantisiert: es kann nur diskretet Werte annehmen.

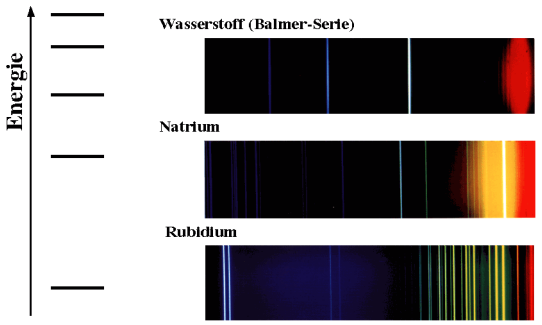

Abbildung 1.7: Linienspektren einiger unterschiedlicher Atome.

Dies führt dazu, dass Atome auch Energie nur in diskreten Quanten abgeben. Aufgrund der Beziehung zwischen Energie, Frequenz und Wellenlänge der Photonen führt dies dazu, dass die Spektren von Atomen aus wenigen scharfen Linien bestehen. So emittiert atomares Natrium bevorzugt bei 589 nm, im gelben Bereich des Spektrums, wie man von den entsprechenden Straßenlampen gewohnt ist.

1.2.2 Simulation von Quantensystemen

Versucht man, quantenmechanische Systeme auf einem klassischen Rechner zu simulieren, so stellt man fest, dass dies eine sehr schwierige Aufgabe ist. Die Grundlagen dafür sind gut bekannt, es handelt sich um die Schrödingergleichung

$$\frac{d}{dt}|\psi\rangle \;=\; -i\,\mathcal{H}\,|\psi\rangle\,.$$

Hier stellt $|\psi\rangle$ den quantenmechanischen Zustand dar und $\mathcal{H}$ den Hamiltonoperator (=Energieoperator).

Wenn man aber versucht, diese Gleichung zu lösen, stellt man fest, dass die Menge der Zahlen, die man speichern muss, exponentiell mit der Größe des Systems zunimmt. Wir betrachten dies kurz anhand des einfachsten Beispiels, eines Systems von Teilchen mit Spin 1/2. Jedes dieser Teilchen kann 2 mögliche Zustände einnehmen, welche wir z.B. mit $|\uparrow\rangle$ und $|\downarrow\rangle$ bezeichnen. Ein System aus zwei Teilchen kann danach die Zustände $|\uparrow\uparrow\rangle$,$|\uparrow\downarrow\rangle$,$|\downarrow\uparrow\rangle$,$|\downarrow\downarrow\rangle$ einnehmen, und bei 3 Teilchen gibt es die Zustände $|\uparrow\uparrow\uparrow\rangle$, $|\uparrow\uparrow\downarrow\rangle$, $|\uparrow\downarrow\uparrow\rangle$, $|\uparrow\downarrow\downarrow\rangle$, $\downarrow\uparrow\uparrow\rangle$, $|\uparrow\uparrow\downarrow\rangle$, $|\downarrow\downarrow\uparrow\rangle$, $|\downarrow\downarrow\downarrow\rangle$. Für N Teilchen gibt es 2^N unterscheidbare Zustände, also eine exponentiell wachsende Zahl. Wie man zeigen kann wächst jedoch nicht nur die Zahl der Zustände, sondern auch die benötigte Rechenzeit exponentiell mit der Anzahl Teilchen.

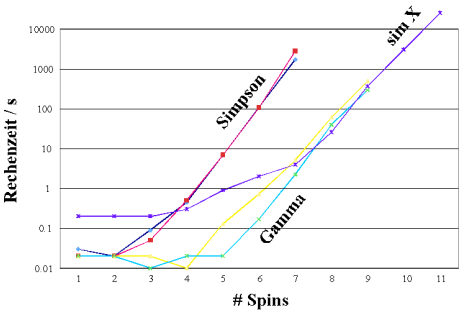

Abbildung 1.8: Rechenzeit für die Simulation von Spinsystemen als Funktion der Anzahl Spins.

Figur 1.8 zeigt ein Beispiel dafür: Dargestellt sind die Rechenzeiten, welche benötigt werden, um ein Spinsystem zu simulieren. Die horizontale Achse stellt die Anzahl der Spins dar, auf der vertikalen Achse ist die Rechenzeit auf einem logarithmischen Maßstab aufgetragen. Es wurden unterschiedliche Softwarepakete auf handelsüblichen Rechnern getestet. In allen Fällen stieg pro zusätzlichem Spin die Rechenzeit um etwas mehr als eine Größenordnung (außer für kleine Systeme, wo der Overhead wie z.B. Initialisierung und Ausgabe dominiert).

Diese Problem wurde erstmals 1982 von Richard Feynman explizit formuliert. Er schlug auch gleich eine Lösung vor: Wenn Quantensysteme sich selber “berechnen” können, sind sie vielleicht auch in der Lage, andere Systeme zu berechnen. Dies würde bedeuten, dass Quantensysteme die Basis für leistungsfähigere Rechner sein könnten als unsere heutigen klassischen Rechner.

1.2.3 Quanteninformation

Information esistiert in sehr unterschiedlichen Formen. Wir beschränken uns hier auf digitale Information. Klassisch wird digitale Information in einer Sequenz von binären Werten (=bits) dargestellt. Jedes Bit kann zwei mögliche Zustände einnehmen, welche üblicherweise mit 0 und 1 bezeichnet werden. In elektronischen Geräten werden diese meist durch unterschiedliche Spannungen dargestellt. Im TTL Standard, z.B., entspricht die logische 0 einer Spannung von $< 0{,}8$ V, die logische 1 einer Spannung $> 2{,}4$ V.

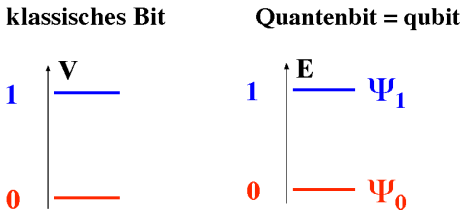

Abbildung 1.9: Darstellung von digitaler Information in einem klassischen Computer (links) und einem Quantencomputer (mitte). Der Spin 1/2, welcher zwei mögliche quantenmechanische Zustände besitzt, und damit das prototypische Qubit darstellt, ist rechts gezeigt.

Das gleiche Prinzip gilt bei Quantensystemen, welche Information darstellen: Um ein einzelnes Bit von Information darzustellen, benötigt man zwei unterscheidbare Zustände. "Unterscheidbar" bedeutet in der Quantenmechanik, dass es sich um unterschiedliche Eigenzustände eines geeigneten Operators handeln muss. Ein typisches Beispiel ist ein Spin 1/2, welcher zwei unterscheidbare Zustände besitzt: der Spin kann parallel oder entgegengesetzt zu einem äußeren Magnetfeld ausgerichtet sein. Ein anderes Beispiel ist ein Photon, welches horizontal oder vertikal polarisiert sein kann. Diese Zustände können jeweils als logische 0 oder 1 identifiziert werden.

Der wichtigste Unterschied zwischen quantenmechanischer und klassischer Information liegt darin, dass Quanteninformaiton nicht notwendigerweise im Zustand 0 oder 1 sein muss. Statt dessen kann sie sich auch in einem beliebigen "Überlagerungszustand", d.h. einer Linearkombination der beiden Basiszustände, befinden. Um diesen Unterschied herauszustreichen, verwendet man den Ausdruck "Qubit" (als Abkürzung für "quantum bit") für die quantenmechanische Informationseinheit.

Die Leistungsfähigkeit der Quantencomputer kann direkt auf diese Möglichkeit zurückgeführt werden, Überlagerungszustände zu bilden und darauf logische Operationen anzuwenden. Ein system aus N Qubits besitzt 2^N orthogonale, d.h. unterscheidbare Basiszustände, und es ist möglich, ein solches System in einen Überlagerungszustand aller dieser Basistzustände zu bringen. Logische Operationen können direkt auf diese Überlagerungszustände angewendet werden. In diesem Falle werden prinzipiell alle 2^N Zustände gleichzeitig verarbeitet. Man bezeichnet dies als Quanten-Parallelismus.

Formal wird die Information, welche in einem quantenmechanischen System dargestellt wird, in einem quantenmechanischen Zustand codiert. Sie stellt damit einen Vektor in einem Hilbertraum dar. Für den einfachsten Fall eines einzelnen Qubits ist der Zustand

$$|\psi\rangle \;=\; a|\psi_0\rangle \;+\; b|\psi_1\rangle\,.$$

Die beiden Koeffizienten a und b sind beides komplexe Zahlen, mit der Normierungsbedingung $|a|^2 + |b|^2 = 1$. Somit wird der Zustand durch drei reelle Variablen parametrisiert.

Die Tatsache, dass der Zustand durch drei reelle Variablen codiert wird, bedeutet nicht, dass er eine unendliche Menge von Information enthalten kann. Um den Informationsgehalt zu berechnen, muss man den Messprozess mit berücksichtigen, d.h. das Auslesen der Information. Es ist niemals möglich, den Quantenzustand eines einzelnen Photons exakt zu bestimmen. Eine einzelne Messung (präziser: eine ideale QM Messung im Sinne von Neumanns) kann nie den gesamten Quantenzustand bestimmen, sondern nur einen

Freiheitsgrad, und damit ein bit an Information liefern.

Eine Bestimmung des vollständigen Zustandes würde wiederholte Messungen benötigen. Dies ist dann möglich, wenn es einem gelingt, viele identische Teilchen in den gleichen Zustand zu präparieren. Für einen unbekannten Quantenzustand ist dies nicht möglich, wie mit Hilfe des "No-Cloning" Theorems gezeigt werden kann. Ohne die Details zu diskutieren kann man zeigen, dass es aber möglich ist, in einem einzelnen Photons bis zu zwei klassische bits an Information zu übertragen. Dies kann man sich dadurch plausibel machen, dass es möglich ist, zwei unabhängige Messungen durchzuführen, z.B. die Messung der Polarisation des Lichtes senkrecht / horizontal oder $\pm 45°$.

1.2.4 Quantenkommunikation

Zu den aktivsten Bereichen der Quanten-Informationsverarbeitung gehört die Quantenkommunikation, d.h. die Übertragung von Information, welche in quantenmechanischen Freiheitsgraden gespeichert ist. Dazu wird diese meist im Zustand von Photonen codiert. Neben der Grundlagenforschung bietet die Quantenkommunikation auch eine Reihe von interessanten Anwendungen. So sollte es möglich sein, unter Berücksichtigung der Quantenmechanik die Übertragungskapazität von Kommunikationskanälen zu erhöhen.

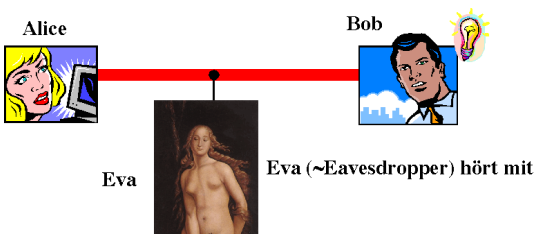

Abbildung 1.10: Eine Kommunikation zwischen Alice und Bob wird von Eva abgehört.

Außerdem kann die Quanteninformationsübertragung abhörsicher gemacht werden, d.h. es ist nicht möglich, die Information, welche über einen Quanten-Kanal übertragen wird, abzuhören, ohne dass die eigentlichen Nutzer dies bemerken. Dies ist eine direkte Konsequenz des "no-cloning" Theorems: während es möglich ist, dass jemand die Leitung anzapft und die Information erhält, welche übertragen wird, und er die Möglichkeit hätte, die detektierten Photonen wieder zu erzeugen und weiter zu senden, können diese nicht im gleichen Zustand sein wie die abgehörten Photonen. Dadurch gelingt es den beiden Parteien, welche die Information austauschen möchten, dies zu detektieren, nicht anhand der Messungen an einzelnen Photonen, aber durch statistische Analyse der empfangenen Daten.

Dies ist jedoch kein Automatismus. Würde das Kommunikationsprotokoll das Vorhandensein oder Fehlen eines Photons als logische 1 und 0 verwenden, so könnte der Abhörende eine QND Messung verwenden (QND = Quantum NonDemolition). Dabei handelt es sich um eine Art von Messung, bei denen bestimmte quantenmechanische Variablen (wie z.B. Zahl der Photonen) gemessen werden, ohne dass sie beeinflusst werden. Das Heisenberg'sche Unschärfenprinzip besagt jedoch, dass in diesem Fall eine sogenannte konjugierte Variable verändert werden muss. Im Falle der Intensität ist die konjugierte Variable die Phase des Lichts.

Daraus kann man ein sicheres Protokoll entwickeln: Der eine Partner (meist als Alice bezeichnet) stellt Paare von verschränkten Photonen her. Diese sind anti-korreliert, d.h. ihre Polarisation is entgegengesetzt, hat aber keinen bestimmten Wert bevor er gemessen wird. Von jedem Paar von Photonen sendet Alice eines zu ihrem Partner Bob. Die beiden Partner führen dann Messungen der Polarisation dieser Photonen durch, wobei die Richtung der Polarisationsache, mit der gemessen wird, stochstisch zwischen zwei vorher bestimmten Richtungen gewechselt wird. Falls die beiden Polarisatoren in die gleiche Richtung ausgerichtet waren, kennt nun jeder Partner das Resultate der Messung beim anderen Partner. Dazu tauschen sie zunächst die Information über die verwende-

te Richtung des Polarisators aus (aber nicht das Resultat der Messung !!) Sie verwerfen jetzt die Daten, bei denen sie unterschiedliche Polarisationsrichtungen gewählt hatten und benutzen die verbleibenden Daten als geheimen Schlüssel für ihre Datenübertragungen.

Versucht eine andere Person, diese Datenübertragung abzuhören, so verändert er die Polarisation und damit die Messresultate. Um diese Möglichkeit zu eliminieren, tauschen A und B einen Teil der Daten aus und überprüfen ihn anhand statistischer Kriterien. Diese Möglichkeit der sicheren Datenübertragung ist inzwischen mehrfach getestet, sowohl bei er Übertragung mit Hilfe von Glasfasern wie auch im freien Raum.

1.2.5 Quantenbits

Ein Quantencomputer, d.h. ein programmierbarer Rechner, welcher Quanteninformation verarbeiten kann, codiert die Informationen in einem Quantenregister. Dieser besteht aus einer numerierten Reihe von Qubits. Jedes Qubit stellt ein quantenmechanisches Zweiniveausystem dar, wie z.B. ein Spin 1/2. Der wesentliche Unterschied zwischen klassischen und Quantenbits ist, dass ein Qubit nicht nur die Zustände$|0\rangle$ und $|1\rangle$ annehmen kann, sondern auch einen Superpositionszustand

$$|\psi\rangle \;=\; c_0|0\rangle \;+\; c_1|01\rangle\,.$$

Das System ist somit in einem gewissen Sinn an 2 Orten gleichzeitig.

Figur 1.11 zeigt das Prinzip für einen symmetrischen Überlagerungszustand. Führt man eine Messung durch, welche entscheiden soll, an welchem der beien Orte das Teilchen sich aufhält, so erhält man mit jeweils 50% Wahrscheinlichkeit eines der beiden möglichen Resultate.

Der Zustand des Quantenregisters wird durch die Basistzustände$|0,0,0..0\rangle$, $|0,0,0..1\rangle$, .. aufgespannt. Er kann damit allgemein den Zustand

$$|\psi\rangle^{reg} \;=\; c_0|0,0,0..0\rangle \;+\; c_1|0,0,0,..1\rangle \\ +\,c_2|0,0,0,..1,0\rangle \;+\;\ldots\,.$$

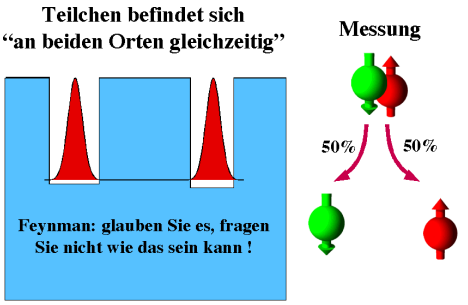

Abbildung 1.11: Ein quantenmechanischer Überlagerungszustand. Bei einer Messung erhält man beide möglichen Resultate mit gleicher Wahrscheinlichkeit.

annehmen.

Während heutige Quantenregister weniger als 20 Qubits enthalten, benötigt man für viele Anwendungen Quantenrechner mit mehreren tausend Qubits.

1.2.6 Rechnen mitQubits

Bevor man Rechenoperationen durchführen kann, muss der Quantenregister initialisiert werden, d.h. er muss in einen wohldefinierten Zustand gebracht werden. Typischerweise wählt man dafür den Zustand $|0,0,0...0\rangle$. Diese Initialisierung ist nicht-unitär, somit nicht-reversibel: die Werte, die hier hineingeschrieben werden, sollen nicht vom vorherigen Zustand des Quantenregisters abhängen. Solche Operationen werden auch als dissipativ bezeichnet, d.h. sie erzeugen Entropie und damit Wärme.

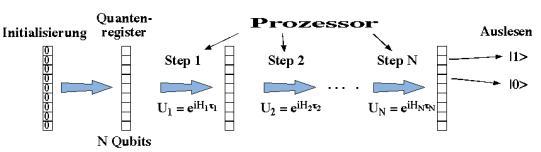

Abbildung 1.12: Schritte bei der Quanteninformationsverarbeitung.

Für die Verarbeitung der Information müssen logische Operationen darauf angewendet werden.

Man bezeichnet diese als Quanten-Gatter. Mathematisch werden sie durch unitäre Transformationen U_i beschrieben, welche auf den Quantenregister wirken:

$$|\psi_0\rangle \xrightarrow{\mathbf{U_1}} |\psi_1\rangle \xrightarrow{\mathbf{U_2}} |\psi_2\rangle ...$$

Die Reihenfolge dieser Gatteroperationen wird durch den Algorithmus bestimmt, welcher implementiert werden soll. Das Programm, welches die Reihenfolge definiert, kann auf einem klassischen Rechner gespeichert sein.

Jede Änderung im Zustand eines quantenmechanischen Systems wird durch einen entsprechenden Hamiltonoperator $\mathcal{H}$ getrieben, welcher auf den Zustand wirkt. Physikalisch bedeutet dies, dass man eine Wechselwirkung zwischen dem Qubit und einer äußeren Kontrolleinheit einführt, sowie Wechselwirkungen zwischen den einzelnen Qubits. Typische Beispiele sind Wechselwirkungen zwischen einem magnetischen Dipol (Spin) und einem externen Magnetfeld $\vec{B}$.

In den meisten Fällen ist es sehr schwierig, einen Hamiltonoperator zu finden, welcher die gewünschte Operation direkt durchführt, wie z.B. die Zerlegung einer Zahl in ihre Primfaktoren. Statt dessen teilt man die Gesamttransformation in viele elementare logische Operationen auf, welche einzelne Qubits oder Paare von Qubits in geeigneter Weise transformieren. Dabei hängt die Transformation vom Zustand der anderen Qubits ab. Man kann zeigen, dass es möglich ist, sämtliche benötigten logischen Operationen auf eine kleine Zahl von elementaren Operationen zurückzuführen.

1.2.7 Elementare Quantengatter

Man benötigt im Mimimum folgende elementaren Quantengatter, um beliebige Rechnoperationen durchzuführen:

- Operationen an einzelnen Qubits.
- Ein Typ von 2-Qubit Operationen, wie z.B. das "Controlled NOT" = CNOT.

Jedes Gerät, das als Quantencomputer arbeiten soll, muss somit diese Arten von Rechenoperationen beherrschen. Kritisch sind vor allem die 2-Qubit Operationen, da dafür eine Wechselwirkung zwischen den Qubits benötigt wird. Ein typisches Beispiel ist das CNOT Gatter. Es kann durch seine Wahrheitstabelle definiert werden:

Kontroll-Qubit	Ziel-Qubit	Resultat
0	0	00
0	1	01
1	0	11
1	1	10

Dieses Gatter benötigt zwei Qubits für die Eingabe, wie auch für die Ausgabe. Wenn das Kontroll-Qubit 0 ist, wird das Ziel-Qubit nicht verändert. Ist das Kontroll-Qubit = 1, wird das Ziel-Qubit invertiert. Das Kontroll-Qubit bleibt in beiden Fällen unverändert. Es wird auch als "reversibles XOR" bezeichnet: Das Ziel-Qubit enthält das Resultat einer "exclusive OR = XOR" operation. Dadurch, dass man das Kontroll-Qubit auf den Ausgang überträgt, ist die Operation insgesamt reversibel und damit auch für Quantenrechner geeignet.

Diese Operation muss man auf jedes beliebige Paar von Qubits anwenden können. Dafür benötigt man im Prinzip physikalischen Wechselwirkungen zwischen allen Paaren von Qubits. Durch diese Wechselwirkungen "erfährt" ein Qubit, in welchem Zustand das andere Qubit sich befindet. So führt eine Wechselwirkung zwischen 2 Spins dazu, dass die Resonanzfrequenz eines Spins sich ändert, in Ahängigkeit davon, was der Zustand des anderen Qubits ist.

Figur 1.13 zeigt ein Beispiel, bei dem die Resonanzfrequenz eines Spins durch den Zustand der beiden benachbarten Qubits beeinflusst wird. Damit ist es möglich, eine Operation am Qubit A nur dann durchzuführen, wenn die Nachbarqubits im Zustand $|00\rangle$ sind.

Sind nicht alle diese Wechselwirkungen vorhanden, so ist es jedoch möglich, die entsprechende 2-Qubit Operation in eine Reihe von 2-Qubit Operationen zwischen nächsten Nachbarn zu zerlegen. Solche Systeme, welche nur Wechselwir-

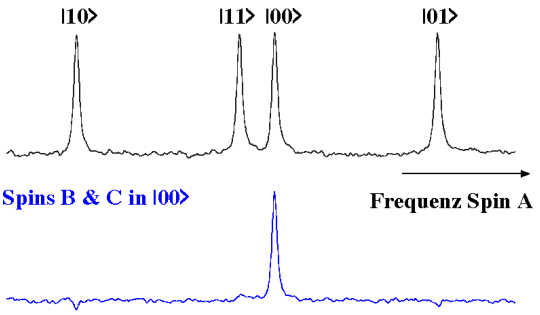

Abbildung 1.13: Änderung der Resonanzfrequenz durch Kopplung an benachbarte Qubits; gezeigt ist jeweils das Spektrum von Qubit A. Oben sind Qubits B und C in einem Überlagerungszustand; unten sind beide im Zustand 0.

kungen zwischen nächsten Nachbarn verwenden, sind häufig deutlich einfacher zu implementieren als Systeme, bei denen alle Qubits aneinander gekoppelt sein müssen. Die Zahl der 2-Qubit Operationen ist größer, sie nimmt aber höchstens linear mit der Anzahl der Qubits zu; der Gesamtprozess bleibt effizient.

1.2.8 Dekohärenz

Eine der schwierigsten Hürden, welche beim Bau eines Quantenrechners überwunden werden müssen, ist die Dekohärenz. Dieser Ausdruck fasst alle Prozesse zusammen, welche die Information vernichten, die in einem Quantenregister gespeichert ist. Wie oben betont, kann die Leistungsfähigkeit eines Quantenrechners auf die Möglichkeit zurückgeführt werden, logische Operationen an einer großen Zahl von Zuständen gleichzeitig durchzuführen, welche in einem Überlagerungszustand gespeichert sind. Wenn die relative Phase zwischen diesen Zuständen verändert wird, ist das Resultat effektiv mit der falschen Eingabe korreliert. Mit der Zunahme der Anzahl Qubits wird die Quanteninformation zunehmend fragiler.

Der größte Beitrag zur Dekohärenz ist meist die Dephasierung. In einem einfachen Bild kommt es dazu, wenn der Unterschied in der Energie der beiden Zustände fluktuiert. Dadurch erhält die relative Phase einen zusätzlichen Beitrag, welcher proportional zur Energieänderung ist.

Das Resultat einer solchen Dephasierung, wie auch anderer Dekohärenz-Prozesse, ist ein Informationsverlust im System. Da es praktisch unmöglich ist, einen vollständige Quantenalgorithmus durchzuführen, bevor die Dekohärenz das System verändert, ist es notwendig, Strategien zu entwickeln, welche die Dekohärenz reduzieren oder ihren Effekt korrigieren. Eine mögliche Strategie ist die Quanten-Fehlerkorrektur. Dazu wird die Information über mehrere physikalische Qubits verteilt. Zu bestimmten Zeiten während der Rechnung werden dann Fehler gesucht und gegebenenfalls korrigiert.

1.3 Algorithmen und Implementationen

1.3.1 Quantenalgorithmen

Algorithmen, welche einen Quantencomputer benötigen, werden als Quantenalgorithmen bezeichnet. Der erste Quantenalgorithmus, welcher effizienter war als ein entsprechender klassischer Algorithmus, war der Detusch-Algorithmus und seine Verllgemeinerung von Deutsch und Jozsa. Der Algorithmus beantwortet die Frage, ob die Resultate einer gegebenen Funktion identisch oder gleichmäßig verteilt sind. Dieser Algorithmus ist konzeptionell interessant, hat aber wenig praktische Relevanz.

Ein nützlicher Algorithmus wurde 1994 von Coppersmith vorgeschlagen. Er zeigte, wie die Fouriertransformation auf einem Quantencomputer effizient implementiert werden kann. Die Fouriertransformation hat in Physik und Mathematik sehr viele Anwendungen. Insbeonsdere wird sie auch verwendet in der Zahlentheorie, bei der Suche nach den Prinfaktoren großer Zahlen. Die Quanten-Fouriertrasnformation wurde deshalb sogleich verwendet, um einen Algorithmus

für die Prinfaktorzerlegung zu entwickeln (Shor 1994). Die Primfaktorzerlegung ist nicht nur interessant für die Zahlentheorie, sie hat auch erhebliche Konsequenzen im Bereich der digitalen Datenübermittlung: die am weitesten verbreiteten kryptographischen Systeme beruhen auf der Schwierigkeit der Faktorisierung großer Zahlen.

Beim besten bekannten klassischen Faktorisierungsalgorithmus wächst die Rechenzeit mit der Anzahl l Ziffern wie $\exp(cl^{(1/3)}(\log l)^{(2/3)})$, d.h. exponentiell. Der Algorithmus von Shor benötigt hingegen einer Rechenzeit, welche wie $O(l^2 \log l \log\log l)$ zunimmt, d.h. (nur) polynomiell. Dies ist ein qualitativer Unterschied: Algorithmen, deren Laufzeit polynomiell wächst, werden als effizient bezeichnet, während Algorithmen mit einer exponentiellen Zunahme der Rechenzeit für große Eingaben nicht mehr verwendet werden können. Der Unterschied bedeutet, dass für genügend große Zahlen der Quantenalgorithmus immer schneller laufen wird als der klassische Algorithmus, auch wenn die Zykluszeit des klassischen Rechners sehr viel kürzer ist als die des Quantenrechners.

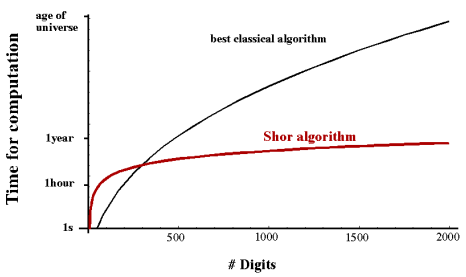

Abbildung 1.14: Vergleich der Rechenzeiten für die Primzahlzerlegung zwischen dem besten klassischen und dem Shor Algorithmus.

Zur Illustration betrachten wir ein Zahlenbeispiel. Wir nehmen an, dass ein schneller klassischer Computer eine Zahl mit 50 Ziffern in einer Sekunde faktorisieren kann, während der Quantencomputer für die gleiche Aufgabe eine Stunde benötigt. Betrachtet man statt dessen eine Zahl mit 300 Ziffern benötigen beide Rechner etwa 2,5 Tage für die Zerlegung. Bei einer weiteren Erhöhung auf 1000 Ziffern benötigt der Quantencomputer 42 Tage, der klassische Rechner 19000 Jahre - offensichtlich zu lange für praktische Anwendungen. Bei 2000 Ziffern benötigt der Quantencomputer ein halbes Jahr, während die Rechenzeit des klassischen Computers etwa dem Alter des Universums entspricht.

1.3.2 Implementationen: Voraussetzungen

Ein Gerät, welches in der Lage ist, Quanteninformation zu verarbeiten, muss eine Reihe von Anforderungen erfüllen. So muss ein Quantenregister vorhanden sein, der geeignet ist, die Information zu speichern. Jede Implementation muss somit ein quantenmechanisches System mit N Qubits enthalten. Für einen leistungsfähigen Quantencomputer sollte N möglist groß sein.

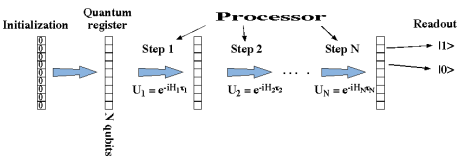

Abbildung 1.15: Prinzip des Betriebs eines Quantencomputers

Dies Qubits müssen in einen geeigneten Zustand initialisiert werden, typischerweie in den Grundzustand $|0\rangle$. Die Initialisierung ist immer ein dissipativer Prozess. Als nächster Schritt müssen die logischen Operationen angewendet werden. Jeder Schritt entspricht einer unitären Transformation

$$U_i = e^{-i\mathcal{H}_i\tau_i},$$

welche durch einen Hamiltonoperator $\mathcal{H}_i$ getrieben wird, welcher für eine Zeit τ_i angewandt wird. Dazu werden normalerweise elektromagnetische Felder angelegt, welche auf spezifische Qubits oder Paare von Qubits wirken. Der Quantenrechner muss deshalb die Möglichkeit haben, diese Felder zu erzeugen und präzise zu steuern. Zum Ende der Rechnung muss das Resultat, also der endgültige Quantenzustand, ausgelesen werden. Meist verwendet man dafür einen Prozess,

der in guter Näherung als ideale quantemechanische Messung (von Neumann), also als Projektion auf einen Eigenzustand der relevanten Observablen beschrieben werden kann.

Ein quantenmechanisches System, welches Information verarbeiten soll, muss eine Reihe von Bedingungen erfüllen. DiVicenzo hat die wichtigsten genannt:

- Es muss möglich sein, das System in einen wohl-definierten Anfangszustand zu initialisieren.
- Es muss möglich sein, unitäre Operationen auf jedes einzelne Qubit anzuwenden
- Es muss möglich sein, unitäre Operationen auf Paare von Qubits anzuwenden
- Die Information, welche im System gespeichert ist, insbesondere die relativen Phasen, muss lange genug erhalten bleiben, dass eine genügend große Zahl von logischen Operationen durchgeführt werden kann.
- Es muss möglich sein, die einzelnen Qubits zuverläßig auszulesen.

Natürlich kann jede dieser Bedingungen präziser formuliert werden. Kritisch ist dabei, dass alle Bedingungen gleichzeitig erfüllt sein müssen, da sie teilweise gegeneinander arbeiten. So ist das Ausführen logischer Operationen nur möglich, wenn die Qubits mit ihrer Umgebung in Wechselwirkung treten. Die Wechselwirkung mit der Umgebung führt jedoch auch zum Verlust der Quanteninformation (Dekohärenz).

Es ist deshalb nicht verwunderlich, dass es sich gezeigt hat, dass es schwierig ist, alle Bedingungen in einem einzelenen System zu erfüllen. Das erste physikalische System, in dem Quantenalgorithmen implementiert wurden, waren Systeme von Kernspins in Flüssigkeiten. Kernspins haben den Vorteil, dass sie sehr gut von ihrer Umgebung abgeschirmt sind und deshalb die Quanteninformation für relativ lange Zeiten (von der Größenordnung einer Sekunde) erhalten. Andererseits macht diese schwache Kopplung das Auslesen von einzelnen Kernspins sher schwierig. Diese Schwierigkeit wird in der Kernspinresonanz (NMR) umgangen, indem man nicht mit einzelnen Spins arbeitet, sondern mit vielen identischen Spins. Eine typische Probe enthält bis zu 10^{20} identische Spins.

Das erste Experimente, welches Quantenalgorithmen an einem Einzelsystemen durchführte, verwendete atomare Ionen, welche in einer elektromagnetische Falle gespeichert waren. Ein Vorteil dieses Systems ist, dass atomare Ionen einer Sorte identisch sind. Die Speicherung in einer elektromagnetischen Falle eliminiert die meisten Kopplungen mit der Umgebung (außer mit der Falle). Es werden deshalb ebenfalls sehr lange Dekohärenzzeiten erreicht. Die größte Schwierigkeit besteht darin, die logischen Operationen mit genügend hoher Präzision zu implementieren.

Einige Quantenalgorithmen sind auch an Photonen implementiert worden. Die direkte Implementation ist jedoch nicht skalierbar, sondern benötigt Resourcen (z.B. Spiegel, Strahleiler), die exponentiell mit der Größe des Systems zunehmen. Erst kürzlich wurde gezeigt, dass es möglich ist, eine besondere Art von optischen Experimenten zu verwenden, welche zu einer skalierbaren Implementation führen.

Der Bau von Quantencomputern mit einer großen Zahl von Qubits wird möglicherweise nur in Festkörpern möglich sein. Es gibt eine Reihe von Vorschlägen für solche Implementationen, welche z.B. Halbleiter-Nanostrukturen oder Supraleiter verwenden. Die Arbeiten an diesen Systemen sind allerdings noch nicht sehr weit fortgeschritten.

1.3.3 Beispiele für Implementation

Eine Reihe unterschiedlicher Systeme wurden als Quantencomputer vorgeschlagen. Aufgrund der direkten Beziehung zwischen Qubits und Spins 1/2 liegt es nahe, Spinsysteme für die Quanteninformationsverarbeitung zu verwenden. Dies erlaubt nicht nur eine einfache Abbildung der Information auf den quantenmechanischen Zustand, sondern diese Systeme haben auch eine

relativ geringe Dekohärenzrate, weil die Spin-Freiheitsgrade gut von ihrer Umgebung isoliert sind.

Leider führt diese schwache Wechselwirkung auch dazu, dass es schwierig ist, das Resultat der Rechnung auszulesen. Spins wurden deshalb meist als Ensemble verwendet, so dass man beim Auslesen das Signal einer sehr großen Zahl von Spins zur Verfügung hat. Kernspinresonanz (NMR) in Flüssigkeiten ist diejenige Technik, die bisher am weitesten fortgeschritten ist. Sie verwendet typischerweise Proben mit rund 10^{20} identischen Molekülen. Leider ist es schwierig, dieses System zu einer großen Zahl von Qubits zu skalieren.

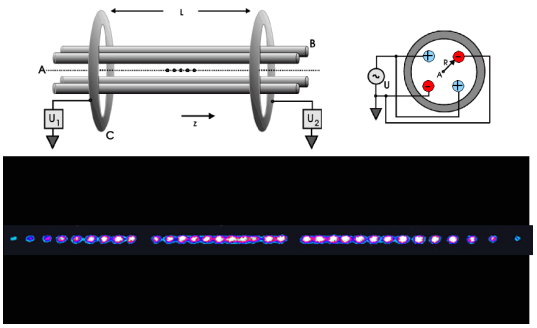

Abbildung 1.16: Atomare Ionen in einer Falle.

Ein anderes physikalischen System, welches relativ gut von seiner Umgebung isoliert ist, besteht aus atomaren Ionen in einer elektromagnetischen Ionenfalle. Die Speicherung der Information in diesem System ist etwas schwieriger, weil zum einen das System grundsätzlich eine unendliche Zahl von Zuständen besitzt (während nur 2 benöigt werden), und es außerdem relativ schwierig ist, die Freiheitsgrade dieses Systems mit genügender Präzision zu steuern. Der wesentliche Vorteil von gespeicherten Ionen liegt in der relativ leichten Möglichkeit, den Zustand einzelner Ionen auszulesen.

Die dritte existierende Implementation eines Quantencomputers sind einzelne Photonen. Photonen sind eigentlich ideale Quantenobjekte: sie können in beliebigen Mengen hergestellt, über große Distanzen transportiert und einzeln detektiert werden. Die Schwierigkeit liegt bei der Wechselwirkung: normlaerweise gibt es zwischen Photonen keine Wechselwirkungen. Diese zu erzeugen ist deshalb die größte Schwierigkeit,

Zusätzlich gibt es eine große Zahl von Vorschlägen für Systeme, welche zur Quanteninformationsverarbeitung verwendet werden könnten. In den meisten Fällen handelt es sich um Festkörper, z.B. um Halbleiter oder Supraleiter. Dabei kann man auf die Technologien zurückgreifen, welche für die Mikroelektronik entwickelt wurden. Die größten Schwierigkeiten bei diesen Systemen sind zum einen die Herstellung der sehr kleinen Strukturen mit hoher Präzision und Reproduzierbarkeit, zum andern die Dekohärenz, welche meist sehr kurz ist.

1.4 Physikalische Grenzen

Wie Rolf Landauer bemerkte ("Information is physical") ist es nicht immer sinnvoll, Information rein abstrakt zu behandeln. Aus der Tatsache, dass Information auch in einem physikalischen System dargestellt werden muss, ergeben sich Grenzen für die Leistungsfähigkeit aller denkbaren Rechner. Diese stellen allerdings für die heute existierenden Rechner noch keine wesentliche Einschränkung dar.

1.4.1 Energieverbrauch

Ein Rechner, der boole'sche Logik verwendet, verliert pro Rechenschritt ungefähr ein Bit an Information. Informationsverlust bedeutet Erzeugung von Entropie. Pro bit beträgt die Entropiezunahme $\Delta S = k_B \ln 2$. Diese Entropiezunahme entspricht einer Wärmeproduktion von $\Delta Q = k_B T \ln 2$. Dies stellt eine universelle Grenze für klassische Computer dar.

Ein Quantencomputer arbeitet reversibel und hat deshalb keinen minimalen Energieverbrauch. Er benötigt jedoch einen minimalen Energieinhalt (der nicht verbraucht wird), um mit endlicher Geschwindigkeit rechnen zu können. Die

Zeit für eine elementare Rechenoperation beträgt mindestens

$$\tau = \frac{h}{4E}.$$

Hier bezeichnet τ die Rechenzeit, $h = 6.626 \cdot 10^{-34}$Js die Planck'sche Konstante und E die Energie des Systems.

Eine weitere Einschränkung für reversible Rechner (wie z.B. Quantenrechner) ergibt sich aus der Tatsache, dass sie Fehler machen. Diese Fehler müssen korrigiert werden, und dabei entsteht wiederum Entropie. Bei einer Fehlerrate ϵ ergibt sich eine Wärmeproduktion $\delta Q = \epsilon\, k_B T \ln 2$.

1.4.2 Der ultimative Rechner

Aus diesen (un ähnlichen) Überlegungen berechnete z.B. Seth LloydLloyd [1] den "ultimativen Laptop". Unter der Annahme, dass der Rechner eine Masse von 1 kg und ein Volumen von 1 l besitze, berechnete er z.B. die maximale Rechengeschwindigkeit. Der Energieinhalt ist prinzipiell gegeben durch die Masse des Systems,

$$E = mc^2 = 9 \cdot 10^{16}\mathrm{J}.$$

Daraus folgt eine maximal mögliche Rechengeschwindigkeit von

$$n = \frac{4E}{h} = \frac{4mc^2}{h} = 5 \cdot 10^{50}$$

Operationen pro Sekunde - offensichtlich noch weit oberhalb aller heute absehbaren Möglichkeiten. Allerdings würde bei dieser Rechengeschwindigkeit und einer endlichen Fehlerrate von (z.B.) $\epsilon = 10^{-8}$ (ein sehr hoch gestecktes Ziel) dabei eine Leistung von

$$P = n\,\epsilon\, k_B T \ln 2$$

in Wärme umgesetzt werden. Bei Raumtemperatur entspricht dies rund $2 \cdot 10^{21}$W. Die effizienteste Möglichkeit, dies Wärme aus dem System abzuführen, ist über die Schwarzkörperstrahlung. Dies würde aber immer noch dazu führen, dass der Rechner bei einer Temperatur von 600 Mio K arbeiten müsste. Bei dieser Temperatur steigt der Energieumsatz auf $4 \cdot 10^{26}$W. Diese Energie könnten am effizientesten durch Umwandlung von Materie in Energie zur Verfügung gestellt werden. Für diese Leistung wäre eine Umwandlung von

$$\frac{dm}{dt} = \frac{P}{c^2} = 10^9 \frac{\mathrm{kg}}{\mathrm{s}}$$

notwendig, d.h. rund eine Million Tonnen pro Sekunde!

Literaturverzeichnis

[1] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000.

[2] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38:114–117, 1965.