Martin Warnke

Quantum Computing

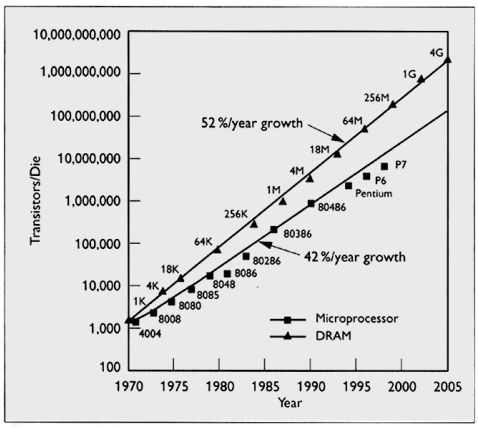
Nach gängiger Auffassung lautet eine der sympathischsten Eigenschaften heutiger Konsumentenelektronik, etwa Handheld oder Handy: ihre buchstäbliche Handlichkeit. Nicht so wie in der Frühzeit elektronischer Technik, in der das Wort ›Rechnerarchitektur‹ sich noch auf Objekte in Wohnzimmergröße bezog oder schon einmal zwei kräftige Männer vonnöten waren, um das experimentelle Mobiltelefon aus dem Kleinlaster zu hieven. Alles scheint nun tragbar, und an die Tragbarkeit knüpft sich die Vorstellung, man könne diese Dinger, wenn man nur wolle, einfach wegwerfen, weit von sich schleudern, um sich ihrer zu entledigen.[1]

Das ist, wir ahnen es, natürlich lediglich eine Wunschvorstellung. Denn so wie Linus ohne seine Schmusedecke überkommt uns Nervosität, wenn wir herumtasten und das Handy nicht mehr fühlen oder die vertraute Beule in der Hemdtasche fehlt, mit der wir uns unseres Organizers versichern. Wir würden also die Gadgets nicht mehr fortwerfen *wollen*, auch dann, wenn wir es noch könnten.

Aber selbst das Ungewollte wird so einfach in der Zukunft nicht mehr sein. Denn wenn man sich auf zweierlei verlassen kann in der Computerei, dann ist es der Ärger über den Wort-Prozessor des Marktführers und das Mooresche Gesetz. Über Ersteres lohnt sich nicht zu reden, gewisse Plagen scheinen nicht ausrottbar zu sein, aber Letzteres kann uns Anlaß zu Spekulationen geben.

Bekanntermaßen prognostiziert das Mooresche Gesetz, aufgestellt 1965 vom Mitbegründer von Intel, daß sich die Packungsdichte von

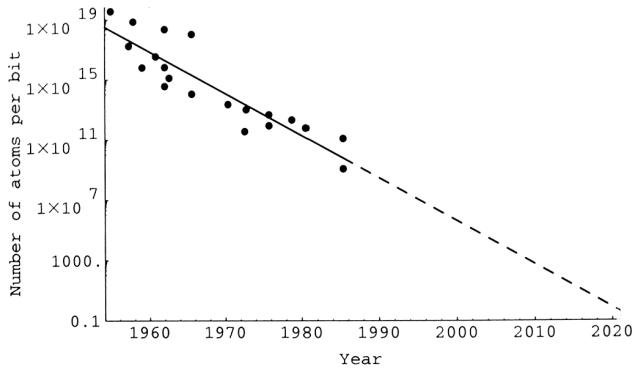
1 Die Feuilletons haben davon berichtet, daß sich zumindest in Finnland noch einige wenige Menschen erlauben, genau dies in Form der Disziplin ›Handy-Weitwurf‹ auch tatsächlich zu praktizieren. Wir konnten lesen: »Eine negative Grundeinstellung zu modernem Kommunikationsgerät ist nicht Pflicht, aber sicher hilfreich.« (http://www.heise.de/newsticker/meldung/38914, 3.1.2005)



Chips alle eineinhalb Jahre verdoppelt, was dasselbe ist wie eine Miniaturisierung in der Fläche um den Faktor Zwei in derselben Zeit.

Die Computerindustrie hat sich brav an die Vorhersage gehalten, und so kam es dann auch, daß Moore's Law[2] mit hoher Verläßlichkeit seit langem gültig ist:

Liest man Moores Gesetz anders herum,[3] trägt man also die Größe eines Schaltelements gegen die demnächst verstreichenden Jahre auf, dann wachsen die Bäume plötzlich nicht mehr in den Himmel, sondern die Zahl der Atome, die zur Repräsentation eines Bit noch erforderlich ist, verdunstet gegen Eins:

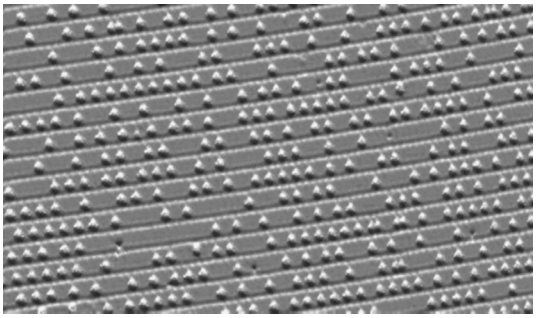


2 Vgl. Communications of the ACM, Vol. 41 No. 8 (1998), S. 50.
3 Vgl. Colin P. Williams/Scott H. Clearwater: Ultimate Zero and One. Computing at the Quantum Frontier, New York: Copernicus 2000, S. 6.

Es dauert nicht mehr lange, dann wird es schwer werden, einen Computer zu fassen zu bekommen, geschweige denn, sich seiner mittels Handgreiflichkeiten zu entledigen. Die Autoren des einschlägigen Buchs über das Quantencomputing »The ultimate zero and one«, Colin Williams und Scott Clearwater, drücken das so aus: »Computers are starting to disappear before our very eyes by becoming part of the fabric of our world.«[4]

Computer werden eher sein wie Staub, den man nur unvollkommen abklopfen kann, wie Feuchtigkeit, die in alle Ritzen kriecht, wie Rußpartikel in der Atemluft, gegen die nur noch katalytische Filter und auch die nur unvollkommen helfen.

Wenn wir den Fortschritt der Rechnertechnik, die Zukünfte des Computers, ungebrochen weiterdenken, mithin an der *conditio sine qua non* der Computerindustrie festhalten, verlassen wir die Fertigungsbedingungen des klassischen Computers, betreten die Domäne des transklassischen Quantencomputers. Das gerade gezeigte Diagramm sagt aus, daß die Miniaturisierung die Computerbausteine etwa um das Jahr 2020 herum auf Atomgröße geschrumpft haben wird. Für Speicher gibt es erste Beispiele[5], bei denen eine Speicherstelle aus einem Silikonatom besteht, dessen An- oder Abwesenheit die binären Speicherwerte repräsentiert. Dieses Atom sitzt in einer Zelle aus neunzehn Goldatomen, so daß wir auf insgesamt zwanzig Atome pro Bit kommen, was schon dichter ist als die Methode, die Mutter Natur bei der DNA einsetzt und die zweiunddreißig Atome pro Bit verbraucht.



4 Ebd., S. 3.

5 Vgl. Roland Bennewitz/Jason N. Crain/Armen Kirakosian u. a.: »Atomic scale memory at a silicon surface«, in: Nanotechnology 13 (2002), S. 499–502.

Die absolute Grenze der Miniaturisierung liegt bei ungefähr einem Atom pro Bit.[6] Die wird spätestens, so Moore's Law, im Jahr 2020 erreicht werden, dem voraussichtlichen Jahr meiner Pensionierung als Rechenzentrumsleiter. Ich kann dann das im Folgenden geschilderte Problem getrost meiner Nachfolge überlassen und aus dem Ohrensessel heraus zusehen, was geschehen wird.

Die Geschehnisse werden uns dazu zwingen, die gewohnte Vorstellung von der Materialität unserer Computer über Bord zu werfen, denn auf atomarer Skala ist die Natur und sind die Artefakte nur noch mit Hilfe der Quantenphysik zu beschreiben. Von ihr hat der Physik-Nobelpreis-Träger Richard P. Feynman, der eigentlich immer ein blitzgescheiter Zeitgenosse mit extrem guter Auffassungsgabe war, der Entscheidendes zur Quantenphysik beigetragen hat, behauptet, er kenne niemanden, der sie wirklich verstehe. Und er schloß sich selbst mit ein.

Die Quantenphysik ist unglaublich genau in ihren Vorhersagen. So sagt sie voraus, wie stark der Magnet ist, den das Elektron durch ständige Rotation seiner Elementarladung erzeugt. Im Experiment kann man diese Größe, das ›Bohrsche Magneton‹, messen, und auf sieben Stellen genau[7] stimmt die Vorhersage mit der Messung überein, also auf ein Zehntel Millionstel genau. Das heißt schon etwas: spekulativ kann man eine Theorie nicht nennen, die zu solcher Präzision in der Lage ist.

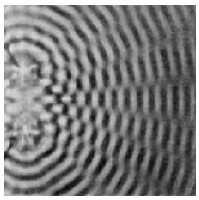
Sie ist aber nicht nur unglaublich genau, sondern auch genau genommen völlig unglaublich. Sie bricht mit unseren Vorstellungen einer Dingwelt (mit der Betonung auf *einer Welt* oder auf *dem Ding*, je nach Sichtweise, ich komme noch dazu), und sie bricht mit ihnen bis auf viele viele Stellen rechts vom Komma exakt.

Ihr Name rührt daher, daß die Annahme von Quanten, von unteilbaren elementaren Grundmaßen, aus denen die Mikrowelt aufgebaut ist, die seltsamen Phänomene erklären kann, mit denen sich die Physik um die Wende des neunzehnten zum zwanzigsten Jahrhundert plagte, etwa der Farbe, in der das Innere eines heißen Ofens leuchtet. So ist eben auch das Licht in Quanta abgemessen, mußte Max Planck widerstrebend postulieren, und nicht etwa beliebig verdünnbar: macht man das Licht sehr schwach, so zerfällt es in einzelne Lichtteilchen, die Photo-

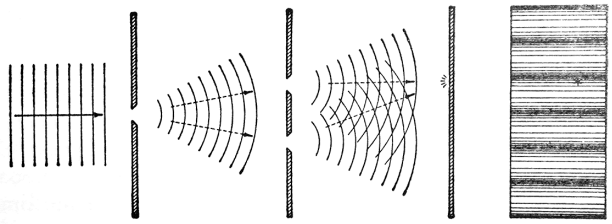
6 Da ein Atom in verschiedenen Zuständen sein kann, liegt die Grenze in Wirklichkeit noch darunter.

7 Vgl. Anton Zeilinger: Einsteins Schleier. Die neue Welt der Quantenphysik, München: C. H. Beck 2003, S. 147.

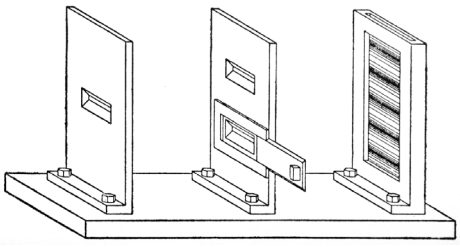
nen. Und dennoch gibt es die bekannten Interferenzbilder, wie man sie von Licht- und von Wasserwellen kennt, auch dann, wenn das Licht so schwach ist, daß es in einzelnen Photonen durch den Doppelspalt rieselt. Warum ist das so ungewöhnlich? Weil Interferenz[8], die Überlagerung von Wellen, halt ein Wellen- und kein Teilchenphänomen ist – zumindest in der uns gewohnten Makrowelt:



Und wie soll das gehen mit einzelnen Photonen? Es geht jedenfalls. Man kann es überprüfen mit Hilfe des Doppelspalt-Experiments, das Niels Bohr folgendermaßen aufgezeichnet hat:[9]



Und, von der Seite:

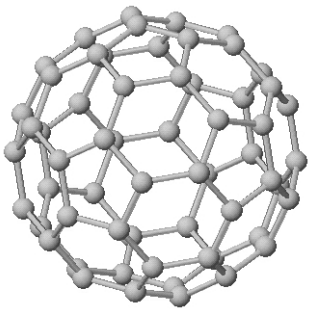


8 Eine hübsche Visualisierung findet man z. B. unter http://www.pk-applets.de/phy/interferenz/interferenz.html und unter http://www.didaktik.physik.uni-erlangen.de/grundl_d_tph/msm_qm/msm_qm_03d.html, letztere Seite lieferte auch das Bild.

9 Vgl. Niels Bohr: »Discussion with Einstein on Epistemological Problems in Atomic Physics«, in: Paul Arthur Schilpp (Hrsg.), Albert Einstein. Philosopher-Scientist, La Salle, Illinois: Open Court 1949, S. 199-241, hier S. 216 und 219.

Solange anständige Wellenfronten auf den Doppelspalt treffen und für Wellentäler und -berge sorgen, mag das ja einleuchtend sein; aber für nacheinander durch die beiden Spalte laufende einzelne Photonen, für die ein Fotopapier die charakteristischen Streifenmuster abliefert, auch?

Und nun wird es noch verrückter: Man kann dasselbe auch mit massiven Teilchen machen, etwa mit Elektronen, die zugegebenermaßen sehr leicht sind. Sie liefern auch die Streifen, als wären sie Wasserwellen. Und sogar auch mit ziemlich großen Gebilden, etwa den sechzig Kohlenstoff-Atomen eines Fullerens[10], das aussieht[11] wie ein Fußball, bekommt man das Phänomen der Interferenz:



Die Experimentralphysiker sind im Moment dabei, Interferenz zwischen immer größeren Materiestückchen nachzuweisen. Es sind auch schon Viren ins Auge gefaßt worden.

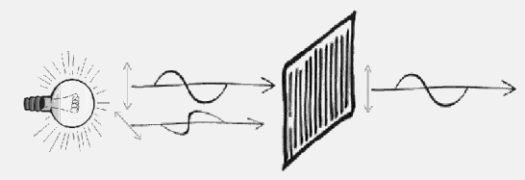
Übertragen ins Alltagsleben hieße das, daß hinter der berühmten Torschußwand aus der Sportschau die Bälle nicht nur direkt hinter den Löchern oben links und unten rechts in der Dekoration des Studios landen, sondern eben auch, wenn man nur oft genug schießt, in dem Bereich direkt zwischen den Löchern.

Vorstellen kann man sich das nicht. Aber man kann einen Formalismus entwickeln, der dann die oben erwähnte legendäre Präzision in der Vorhersage produziert – Augen zu und durch. Und dieser Formalismus geht ansatzweise so:

10 Vgl. Anton Zeilinger: Einsteins Schleier, S. 25 f.
11 http://www.ivw.uni-kl.de/Deutsch/Projekte_Partner/Proj_Abt2/Einzelprojekte/Fullerene.jpg

Jedes quantenphysikalische System, etwa ein Fulleren, ein einzelnes Elektron, ein Photon oder ein Molekül oder Atom, läßt sich durch den Zustand beschreiben, in dem es ist. Das ist nichts Neues und war schon in der klassischen Physik so. Nehmen wir als Beispiel die Polarisation eines Photons, die horizontal in x-Richtung oder vertikal in y-Richtung sein kann. Sie kennen das wahrscheinlich noch von den schicken Polaroid-Sonnenbrillen, die in meiner Jugend modern waren. Mit denen konnte man reflektionsfrei durch Wasseroberflächen schauen, und mit dreien davon konnte man lustige Sachen machen, wir kommen noch dazu.

Wenn die Polarisation in x-Richtung liegt, kann man sich das so vorstellen, daß das Licht, das ja eine elektromagnetische Welle ist, ihren elektrischen Feldstärkevektor eben in x-Richtung, horizontal, und nur dort, schwingen lässt. Entsprechendes gilt für die Richtung senkrecht dazu, vertikal:[12]



Wenn man die Polarisationsrichtung eines Photons mit einem Polarisationsfilter mißt, dann haben alle hindurchkommenden Photonen die Polarisationsrichtung des Filters.

Für das obere Photon, mit der Polarisationsrichtung in die senkrechte y-Achse, schreibt man

$$|y\rangle$$

und das andere, dessen Schwingung in x-Richtung verläuft,

$$|x\rangle$$

Jedes Photon, das völlig durch das senkrecht stehende Polarisationsfilter kommt, ist ein reines $|y\rangle$, jedes, das völlig durch ein waagerechtes Filter kommt, ein reines $|x\rangle$.

12 http://www.ihf.de/~schoene/unter_texte/texte/flachbildschirm/img005.gif

Allgemein kann man jedes Photon als eine Kombination eines |x>- und eines |y>-Photons schreiben:

$$|\text{photon}\rangle = c_1|x\rangle + c_2|y\rangle.$$

Das wird beispielsweise dann nötig sein, wenn seine Polarisationsrichtung zwischen x- und y-Achse liegt, etwa im Winkel von 45°:

$$|45°\rangle = 1/\sqrt{2}|x\rangle + 1/\sqrt{2}|y\rangle.$$

Und nun wird es seltsam: Was passiert, wenn man solche schrägen Photonen durch einen y-Filter schickt, einen senkrechten? Alle Photonen, die hindurchkommen, sind dann *reine* |y>, nicht etwa halb so *helle* |45°>-Photonen. Denn die Lichtenergie kann man nicht weiter unterteilen, sie ist ja quantisiert. Aber es kommen nur halb so *viele* hindurch. Natürlich passiert dasselbe für die x-Richtung. Richtig seltsam ist das dann, wenn man von *einzelnen* Photonen redet. So eines kann ja nun wirklich nur entweder durch das Filter gehen oder von ihm absorbiert werden. Halb durch oder halb absorbiert ist denkunmöglich.

Es bleibt nichts anderes übrig, als den Ausgang des Experiments mit Hilfe von Wahrscheinlichkeiten zu beschreiben: mit der Wahrscheinlichkeit von 50% kommt es durch den y-Filter – also schafft es jedes zweite im Mittel –, mit der gleichen Wahrscheinlichkeit durch das x-Filter, ob es durchkommt, ist für den Einzelfall vollständig unvorhersehbar.

Der Formalismus der Quantenphysik beschreibt das so: Jedes Photon ist die *Überlagerung* eines |x> mit einem |y>. Es ist gleichzeitig ein |x> *und* ein |y>, mit bestimmten Anteilen von beidem, bemessen nach den beiden Koeffizienten c_1 und c_2:

$$|\text{photon}\rangle = c_1|x\rangle + c_2|y\rangle.$$

Es kommt mit der Wahrscheinlichkeit $|c_1|^2$ durch das x-Filter und mit der Wahrscheinlichkeit $|c_2|^2$ durch das y-Filter. Man kann übrigens tatsächlich ein einzelnes Photon nachweisen, es macht dann ›klick‹ im Photomultiplier, wenn es durchkommt.

Mit Polaroid-Sonnenbrillen ist solch ein Experiment leicht zu machen: erst schickt man alles Licht durch ein Brillenglas, das, sagen wir, in x-Richtung gedreht ist. Dann verkreuzt man die andere Sonnen-

brille quer dazu in y-Richtung, und nichts kommt mehr hindurch. Nun hat man Glück, wenn noch eine Dritte mitspielt. Die hält dann ihre Brille im Winkel von 45° zwischen die erste x-Brille und die zweite y-Brille. Und plötzlich wird es ein wenig hell! Warum?

Weil durch die erste Brille nur reine |x> kommen: die kann man schreiben als 1|x> + 0|y>. Das y-Filter läßt – in der ersten Variante des Experiments mit zwei Brillen – mit der Wahrscheinlichkeit |0|2 = 0 keine Photonen hinten mehr durch. Hält man aber eine 45°-x-y-Brille – die von der Dritten im Bunde – zwischen die erste und die zweite, entkommen dieser nur reine 45°-Photonen:

$$|45°\rangle = 1/\sqrt{2}|x\rangle + 1/\sqrt{2}|y\rangle,$$

denn die Messung durch die dazwischen gehaltene Brille wurde ja in 45°-Richtung gemacht. Die Wahrscheinlichkeit, mit der hinter dem schrägen Polarisationsfilter solche reinen |45°>-Photonen erscheinen, beträgt |1/√2|2 = 1/2, weil ja *vor* dem Filter nur *reine* |x>-Photonen da waren und der Anteil der |x> an den |45°> gerade einmal 1/√2 beträgt. So will es der Formalismus der Quantenphysik.

Nun werden die Photonen zum Schluß wieder in y-Richtung gefiltert, und es bleiben von den 45°-Photonen |1/√2|2 = 50%, ihr |y>-Anteil, übrig – und es bleibt nicht ganz dunkel. Insgesamt kommen dann durch den letzten Filter noch die Hälfte der Hälfte, also ein Viertel, derer, die es durch den ersten geschafft haben.

Die sogenannte Kopenhagener Interpretation, maßgeblich von Niels Bohr entwickelt, deutet ein solches Experiment so, daß jedes Photon als *Überlagerung* zweier verschiedener Sorten von Photonen beschrieben werden muß.

Die Geschichte der Überlagerung, also die Veränderung der Werte der Koeffizienten mit der Zeit, wird von der berühmten Schrödingergleichung beschrieben, von der hier nur gesagt sein soll, daß sie eine *Wellengleichung* ist. Deshalb kann man mit ihr Teilchenexperimente beschreiben, die Wellenphänomene aufweisen, wie die Beugungsmuster beim Doppelspalt-Experiment mit massiven Objekten wie Elektronen oder Fullerenen.

Unzumutbar und dennoch unvermeidlich bleibt wohl für immer die Doppelexistenz der Materie als Teilchen und als Welle. Sir William Henry Bragg wird das Wort zugeschrieben:

> Physisists use the wave theory on Mondays, Wednesdays, and Fridays, and the particle theory on Tuesdays, Thursdays, and Saturdays.[13]

Nur, daß es noch viel schlimmer ist, und der Montag auf einen Dienstag, der Mittwoch auf einen Donnerstag und der Freitag auf einen Samstag fällt, weil man nämlich in der Physik seit den hundert Jahren der Existenz der Quantenphysik immer beide Theorien zugleich benutzen muß.

Neben der wellenartigen Überlagerung von Systemzuständen muß für das weitere noch eine sehr wichtige Besonderheit der Quantenphysik erwähnt werden: durch die Messung des Zustands – bei den Photonen etwa durch das Aufstellen eines Polarisationsfilters – beeinflußt man das zu messende System. Wenn es vor der Messung noch als Überlagerung verschiedener Zustände existierte, ist es nach der Messung immer in einem reinen Zustand, einem sogenannten *Eigenzustand*. Es gibt den unbeteiligten externen Beobachter also nicht mehr. Jede Messung stört das System und zwingt es, von einer Zustands-Überlagerung in einen reinen Zustand überzugehen.

Also versuchen wir jetzt noch, das Doppelspalt-Experiment zu beschreiben.

Jedes Quanten-System, das durch den Spalt gekommen ist, um später auf den Schirm zu treffen, ist eine Überlagerung aus |oben>, was heißt, daß es durch den oberen Spalt gegangen ist, und |unten>, dem reinen Zustand für's Hindurchfliegen durch den unteren Spalt:

$$|\text{durch}\rangle = c_1|\text{oben}\rangle + c_2|\text{unten}\rangle$$

Wir haben, wohl gemerkt, keine Messung gemacht, darum haben wir eine Mischung aus beiden Zuständen.

Die Schrödinger-Gleichung macht dann wunderbare Wellen aus $c_1|\text{oben}\rangle$ und $c_2|\text{unten}\rangle$, und am Ende, auf dem Schirm, können sich die beiden Zustände überlagern, Interferenz veranstalten, als wären es Wasserwellen, in die man zwei Steine hat plumpsen lassen.

Doch: was ist *eigentlich* passiert?

Wenn man das Experiment mit einzelnen Quantensystemen macht, einzelnen Fullerenen z. B.: wie können die interferieren? Sie gehen

13 Colin P. Williams/Scott H. Clearwater: Ultimate Zero and One, S. 11.

doch, so sagt der ›gesunde Menschenverstand‹, entweder oben oder unten durch den Spalt.

Ein anständiges ›Ding‹, ein Teilchen, würde sich so verhalten. Es hätte einen definierten Ort zu jeder Zeit, es könnte nur oben oder unten hindurch. Wie könnte es oben und unten gleichzeitig durch den Spalt treten?

Hier wurde 1957 eine atemberaubende Interpretation vorgeschlagen, und zwar von Hugh Everett.[14] Sie lautet: jedes Teilchen geht auch wirklich durch nur einen Spalt, und zwar jedes in einem separaten Universum. Immer, wenn es eine Alternative gibt, entsteht auch ein eigenes Universum, in dem das dann auch tatsächlich passiert. Am Ende werden alle Universen aufgesammelt, und es entsteht das Streifenmuster. Kein Naturgesetz spricht dagegen, aber dennoch ist die These ziemlich gewagt.[15]

Die andere Schule, die von Niels Bohr, hat die Kopenhagener Deutung vorgeschlagen, die besagt: Realität hat nur das wirklich ausgeführte Experiment, es macht keinen Sinn, danach zu fragen, ob das ›Ding‹ oben oder unten durchgegangen ist. Es gibt auch keine zwei verschiedenen ›Dinge‹, die gleichzeitig existieren, sondern nur den Interferenzstreifen. Augen zu, den Formalismus anwenden, und durch!

Jedenfalls, wenn man nachsieht, eine Messung macht, und herausbekommt, ob das Teilchen unten oder oben den Doppelspalt passiert hat, dann verschwindet der Interferenzstreifen. Das ist ja auch kein Wunder, denn Messungen liefern immer reine Eigenzustände, und nur |oben> oder nur |unten> geben keinen Anlaß zu irgendeiner Interferenz wie bei den Wasserwellen.

Mit einer Augen-zu-und-durch-Haltung läßt sich die mikroskopische Welt grandios in Formeln und Zahlen fassen, versucht man jedoch, wieder von ›Wie‹- auf ›Was‹-Fragen umzustellen – was man vielleicht gerade deshalb nicht tun sollte, und wovon abzuraten Niklas Luhmann nicht müde wurde –, stellt man also die Frage nach dem ›Was‹, dann gerät man in sehr unangenehme epistemologische Dilemmata. Vor meinem geistigen Auge sehe ich schon die Seins-Sucher mit diesen Widrigkeiten ringen, sich die ontologischen Haare raufen, ob nun das Ding im

14 Vgl. Hugh Everett III: »›Relative State‹ Formulation of Quantum Mechanics«, in: Reviews of Modern Physics Vol. 29 #3 (July 1957), S. 454-462. Vgl. dazu auch David Deutsch: Die Physik der Welterkenntnis, München: DTV 2000.

15 Eine Liste von frequently asked questions zur Theorie der Multiversen mit Literaturangabe findet man unter http://www.hedweb.com/manworld.htm#faq.

Multi- oder die Überlagerung separater Zustände im einen Kopenhagener Universum noch zu retten sei.

Genau diese Widrigkeiten machen aber den Pfiff des Quantencomputing aus, um das es als unvermeidlicher Utopie der *IT* nun gehen soll.

Irgendwelche Vorstellungen deterministischer robuster Maschinen werden gänzlich *ad acta* zu legen sein: die Ununterscheidbarkeit von Lesen und Schreiben auf der Skala des Planckschen Wirkungsquantums wird dazu führen, unsere Computermetaphern umzuformulieren. Etwa der Begriff eines ›Displays‹, das lediglich ›abzulesen‹ wäre, würde absurd, weil mit dieser Messung der beteiligten Quantenzahlen der Zustand des Computers selbst verändert werden müßte, man also auch gleichzeitig mit der Ausgabe eine Eingabe vornähme. Für die Kryptographie ergeben sich neue Möglichkeiten, etwa die absolute Fälschungssicherheit, für eine Medientheorie des Computers hieße das: neue Aufgaben, neue Metaphern, neue dicke Bücher.

Fangen wir beim Bit an. Das heißt dann nicht mehr Bit, sonden Qubit, es ist kein Schalter mehr, der nur in einer von zwei definierten Schaltzuständen sein kann, wenn man ihn nicht kaputt nennen will, sondern er kann sich in einer Überlagerung seiner beiden Eigenzustände befinden. Das ist quantenmechanisch, wie wir gesehen haben, völlig normal. Ein Photon etwa hat die beiden Eigenzustände |x> und |y>, es wird dann beschrieben als Superposition dieser beiden Eigenzustände:

$$|\text{photon}\rangle = c_1|x\rangle + c_2|y\rangle.$$

In Anlehnung an Matthäus 5, Kapitel 1, Vers 37 kann man nun sagen: Eure Rede aber sei nicht mehr: |x>|x>, |y>|y>. Und was darüber ist, das ist auch nicht mehr vom Übel, sondern einfach nur Quantenmechanik.

Wie sehen nun Qubits aus? Sie werden physikalisch realisiert durch irgendein geeignetes physikalisches System, das zwei reine Ausprägungen, zwei Eigenzustände hat. Etwa durch ein Photon mit seinen beiden Polarisationsrichtungen, ein Elektron mit seinen beiden Spin-Zuständen, ein Atom, das zwei Zustände haben kann oder irgend etwas anderes.

Nennen wir den einen Zustand |0>, den anderen |1>, die als reine Zustände die klassischen Bit-Werte 0 und 1 repräsentieren.

Typische Beispiele für den Zustand, in den man ein einzelnes Qubit bringen kann, wären dann etwa |0>, |1>, aber eben auch (|0> + |1>)/√2 oder (|0> - |1>)/√2.

Nun sieht man schon: ein Qubit kann in Überlagerung *gleichzeitig* eine Null *und* eine Eins repräsentieren! So etwas geht in klassischen Computern nicht, da muß man die Bit-Stelle nacheinander mit dem einen und dann dem anderen Wert beschicken und jeweils durchrechnen lassen.

Verwendet man nun Qubits in Quantencomputern und rechnet mit ihnen, dann wird das Ergebnis wieder in dem Register aus Qubits stekken, das nun auszulesen wäre. Rechnen heißt dabei, daß man ein geeignetes Experiment anstellt, durch das ein Quantencomputer-Algorithmus realisiert wird. Am Ende liest man am Qubit-Register ab, was die Rechnung erbracht hat. Aber was heißt hier Lesen am Ende? Messen muß man dazu sagen, und Messen ist auch immer Schreiben, Präparieren und Zwingen in einen Eigenzustand. Man darf also nur möglichst wenig zusehen beim Quantencomputing, jeder Blick ins Innere, der über Zwischenergebnisse und Details einer Berechnung Auskunft gäbe, vielleicht die Begründung eines behaupteten Resultates einer Quantencomputer-Berechnung abgäbe, würde die Berechnung selbst unweigerlich zum Erliegen bringen. Also wieder: Augen zu und durch.

Man kann also ein Register aus Qubits beschicken mit Qubit-Mustern. Nicht nur pro Speicherstelle mit einer |0> oder einer |1>, sondern eben mit beidem zugleich. Ein acht Qubits breites Register speichert mithin nicht nur *eine* von 256 verschieden 0-1-Kombinationen

00000000
00000001
00000010

bis

01111110
01111111
11111111,

sondern *alle 256 zugleich*, denn alle Kombinationen von |0> und |1> sind ja an jeder Stelle zugleich in Überlagerung möglich. Man muß also nur ein Mal rechnen, um alle 256 Kombinationen von 0 und 1 dem Quanten-Algorithmus zu unterwerfen, nicht 256 Mal.

Und die Berechnung selbst? Jetzt wird es richtig *strange*: der Zustand des Quantensystems, die Anteile an |0> und |1> in ihrer Überlagerung, entwickeln sich gemäß der Schrödingergleichung, die eine

Wellengleichung ist. Und wenn dann z. B. im Verlauf der Berechnung die Elektronenspins miteinander interagieren oder Photonen gespiegelt und durch Polarisationsfilter und Doppelspaltblenden geschickt werden, aus denen die Schaltgatter des *quantum computing* bestehen werden, dann überlagern sich die Teilchen in einer Weise, wie es nur Wellen können: sie interferieren, sind überall gleichzeitig, schlagen alle Wege ein, gehen etwa durch *beide* Öffnungen des Doppelspalts, benehmen sich wie Spin-up *und* auch wie Spin-down und liefern am Ende als Resultat die Mélange aller dieser Parallel-Entwicklungen, genau so, als hätten sich alle Eigenzustände der Startkonfiguration separat entwickelt und als wären dann alle Resultate der reinen Zustände im Mischungsverhältnis der Startkonfiguration zum Resultat miteinander verschnitten worden. Ein Acht-Qubit-Register hätte dann also gestattet, alle 256 Kombinationsmöglichkeiten *parallel* durchzurechnen und zur Resultat-Superposition der acht Qubits aufzuentwickeln. Das ist die Quantenparallelität, die dadurch entsteht, daß Teilchen eben auch Wellen sind, die mit sich selbst und anderen Wellen, die wieder Teilchen sind, interferieren. Wächst die Zahl der Register-Qubits, dann steigt die Parallelität exponentiell, und zwar zur Basis 2.

Der Welle-Teilchen-Dualismus sorgt für die enorme Leistungsfähigkeit der Quantencomputer. Im Zyklus des *prepare-evolve-measure*, der die altvertraute Eingabe, Verarbeitung, Ausgabe ersetzen wird, werden alle möglichen Anfangskonfigurationen in alle zugehörigen Endkonfigurationen überführt. Schafft man also die Lösung eines quantenrechnerisch lösbaren Problems für ein schmales Register, dann braucht man nur noch größere Register zu bauen, um exponentiell leistungsfähigere Komputationen auszuführen.

Wo es um schiere Rechenleistung geht, etwa beim Brechen eines kryptographischen Codes, da sind Quantencomputer in ihrem Element: ein sechzehn-Qubit-Schlüssel, der 65 536 Kombinationen beherbergt, wird mit nur dem doppelten maschinellen Aufwand des acht-Qubit-Schlüssels bearbeitet, der nur 256 Kombinationen codieren kann, was ja nur ein Zweihundersechsundfünzigstel davon ist. Shors Quantenalgorithmus,[16] der Zahlen in ihre Primfaktoren zerlegt, ist so ein Beispiel, er

16 Vgl. Peter W. Shor: »Algorithms for quantum computation. Discrete logarithms and factoring«, in: 35th Annual Symposium on Foundations of Computer Science, Los Alamitos: IEEE Computer Society Press 1994, S. 124-134. Siehe auch: Colin P. Williams/Scott H. Clearwater: Ultimate Zero and One, S. 105 ff.

wurde 2001 mit einem Sieben-Qubit-Quantencomputer realisiert, der die Zahl ›15‹ faktorisieren konnte. Was jede und jeder von uns sofort im Kopf macht, nämlich auszurechnen, daß 15 = 3*5, ist von einer Fluor-Kohlenstoff-Eisen-Verbindung mit sieben Spins erledigt worden, was heißt, daß das nicht in irgendeinem Kopf passiert ist, weil da ja gar kein Kopf war, sondern in einer quittegelb leuchtende Suppe im Reagenzglas.[17]

Wo beim klassischen Computing Moores Gesetz der Rechenleistung berechenbare zeitliche Schranken setzt, stellt sich beim Quantencomputing die Frage der Registerbreite, die sich durchaus sprunghaft vergrößern kann. Kein Public-Key-Verschlüsselungsverfahren wäre mehr sicher, wenn die entscheidenden technischen Lösungen für breite Qubit-Register gefunden werden könnten.

Aber kommen wir noch einmal zur Frage des Welle-Teilchen-Dualismus zurück, zur Ursache des Quanten-Parallelismus!

David Deutsch, einer der Pioniere des Quantencomputing, stellt die Frage, wie denn alle die Bitmuster im Quantenregister, etwa die 65536 im 16-Qubit-Register, und dann noch die astronomisch vielen Kombinationen der Zwischenergebnisse während der Berechnung überhaupt in Form physischer Entitäten repräsentiert werden können. Eine Über-

17 http://domino.research.ibm.com/comm/pr.nsf/pages/rsc.quantum.html

schlagsrechnung ergibt, daß schon bei mittelgroßen Problemen mehr Teilchen erforderlich wären, als es im Universum überhaupt gibt, denn wenn etwa ein Elektron oder ein Photon durch beide Schlitze eines Spalts fliegen muß, so muß es sich eben verdoppeln, um dann hinter dem Spalt Interferenzmuster bilden zu können, und alle diese intermediären Zustände des Quantencomputers müßten ja irgendwo und irgendwie von irgendetwas repräsentiert werden, wie es bei Digitalcomputern ja unvermeidlich ist.

Ein Universum wäre dann nicht genug. Es müssten so viele her, wie sich Entwicklungsalternativen ergeben, und die bildeten dann das bereits erwähnte Multiversum. Bei der Faktorisierung einer 250-stelligen Zahl schon einmal 10^{500}.

Und so stellt David Deutsch die Frage, die ihn als Pionier des Quantum Computing zum bekennenden Anhänger der Theorie der Multiversen werden ließ:

> Falls also das sichtbare Universum tatsächlich die ganze physikalische Wirklichkeit umfaßt, enthält sie nicht einmal näherungsweise die Ressourcen, die zur Faktorisierung einer solch großen Zahl nötig wären. Wer hat sie dann faktorisiert? *Wie und wo wurde die Rechnung durchgeführt?*[18]

Nicht nur die Zahl der Universen, in deren jedem einzelnen dann eine anständige Repräsentataion durch ein Bit möglich wäre, diese 1 mit 500 Nullen, sondern der Gedanke des Multiversums selbst läßt mich schwindeln, was zugegebenermaßen mein persönliches Problem und kein physikalisches Argument ist. Aber das *Ding* und der *Digital*computer wären im Multiversum gerettet. Kein Teilchen müßte mit sich selbst interferieren, sich wellenhaft selbst auslöschen oder aufschaukeln, wie es ihm in dem *einen Uni*versum zuzugestehen ist, in dem es dann allerdings kein anständiges Ding mehr gibt und auch keine digitale Repräsentation der Qubitmuster, also keine Digitalcomputer selbst mehr, denn ein Digitalcomputer ohne explizite Repräsentation aller an der Rechnung beteiligten Größen ist undenkbar.

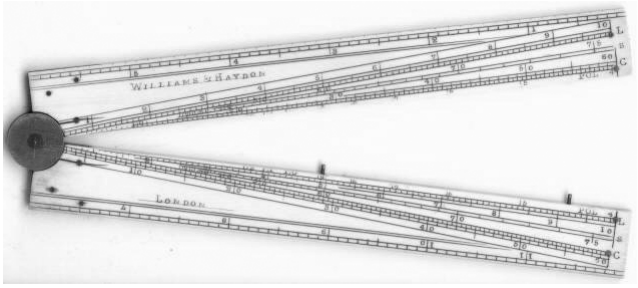
Wir haben also die Qual der Wahl, das Unentscheidbare selbst zu entscheiden: wir können es vorziehen, die Welt als Einheit von geheimnisvoll mit sich selbst interferierenden Wellenteilchen zu sehen, oder

18 David Deutsch: Die Physik der Welterkenntnis, S. 205. Hervorhebung im Original.

die heiße ontologische Kartoffel weiterreichen und uns dazu entschließen, in einem Multiversum zu leben, das sich in jedem Moment in eine astronomisch große Zahl von miteinander geheimnisvoll interagierenden Multiversen aufspaltet, die alle wie gewohnt Teilchen besitzen, die noch Teilchen sind und die Bits der Qubit-Vielfalt realisieren können.

Ich ziehe das Geheimnis der Teilchen vor, die Wellen sind, und muß daher den Schluß ziehen, daß Quantencomputer keine Digital- sondern Analogrechner sind, was jetzt noch zu belegen ist.

Es gibt zunächst ein Indiz für die Analogizität von Quantencomputern: es ist mit ihnen genau wie bei den wundervollen messingglänzenden Analogrechnern des Neunzehnten Jahrhunderts: sie konnten nur ihre Spezialaufgaben, dafür aber in Echtzeit, erledigen, etwa im zeichnerischen Fluge Integrale berechnen oder Kurven rektifizieren oder Winkelfunktionen berechnen, wie z. B. der Proportionalzirkel:[19]



Und genau so gibt es – bislang – auch nur Spezialprobleme, auf die man Quantencomputer ansetzen kann: Faktorisierung von Zahlen, das Durchsuchen von ungeordneten Listen – ebenfalls in Echtzeit.[20] Zu stark sind die physikalischen Einschränkungen der Quantenmechanik – etwa Reversibiliät –, als daß so grobschlächtig prozessiert werden könnte wie zu Turings Zeiten. Quantencomputer sind keine Simulationen von Quantensystemen, sondern nichts als sie selbst, Quantensysteme, deren Verhalten manchmal eine berechenbare Funktion in Echtzeit realisiert.

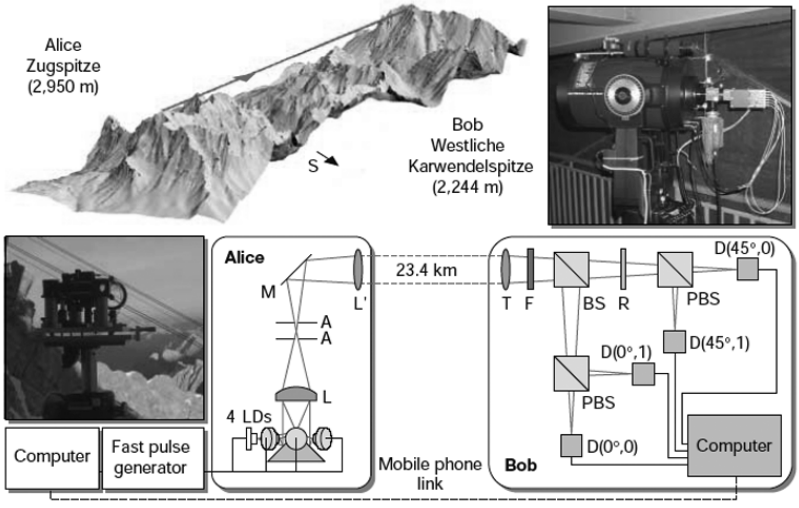
Zudem sind Quantencomputer Maschinen, die abliefern, was nach Turing eben nicht berechenbar ist, Zufallszahlen zum Beispiel. Genau wie eine Wasserwelle nicht die Differentialgleichungen lösen muß, um

19 www.rechenwerkzeug.de/propzirk.htm

20 Eine Übersicht bietet Colin P. Williams und Scott H. Clearwater: Ultimate Zero and One, a. a. O., Kap. 2 und 4.

nach allen Regeln der Hydrodynamik am Strand zu brechen, und folglich ihre Wassermoleküle auch nicht zur Repräsentation der Bitmuster einer Simulation ihrer selbst hergeben muß, so wenig muß ein Quantencomputer mit Hilfe seiner diskreten Elemente die kombinatorische Explosion seiner Qubit-Superpositionen in unserem guten alten und einzigen Universum explizit codieren – wenn man ihn als Analogrechner akzeptiert. Er evolviert eben, nachdem man ihn präpariert hat, um am Ende seinen finalen Zustand einer Messung zur Verfügung zu stellen.

Noch ein Wort zur Kryptographie, deren Sicherheit massiv durch die massive Quantenparallelität und Shors Verfahren zur Faktorisierung bedroht ist: Übertragungstechnik mit Musterabgleich, wie es das Quantencomputing zur Verfügung stellt, bei der jedes Lesen auch ein Schreiben, also ein Verändern des Datenbestandes ist, eine solche Übertragungstechnik auf Glasfaserbasis erlaubt den Austausch von Kryptographie-Schlüsseln, deren Abhorchen mit ins Beliebige steigerbarer Wahrscheinlichkeit offenbar werden würde.[21] Alice und Bob könnten mit Sicherheit ausschließen, daß Eve sie abhört, und das wurde schon praktisch realisiert auf eine Distanz von zehn Kilometern.[22]



21 Vgl. Colin P. Williams/Scott H. Clearwater: Ultimate Zero and One, Kap. 4.
22 Vgl. Christian Kurtsiefer/Harald Weinfurter u. a.: »A step towards global key distribution«, in: Nature, Vol. 419 (2002), S. 450.

Lassen Sie mich bitte kurz zusammenfassen, worin die unvermeidliche Zukunft des Computers in Gestalt der Quantencomputer liegen wird:

Quantencomputer werden sehr klein, auf atomarer Skala, operieren.

Quantencomputer werden Analogrechner sein, oder wir akzeptieren die Multiversumtheorie.

Quantencomputer sind der Tod der Kryptographie mit öffentlichen Schlüsseln, und

Quantencomputer sind der Garant für absolut abhörsichere Kommunikationskanäle.

Und zu guter Letzt: eine Ontologie des Quantencomputing wird sich mit völlig neuen Phänomenen herumschlagen müssen. Nicht mehr das Binäre und Digitale allein sind deutend zu bewältigen, folgende Kategorien stehen zur Klärung an:

die der Repräsentation,
der Dinghaftigkeit und des Universums,
der Realität des Mikrokosmos.

Oder aber, als durchaus realistische Alternative, wir verzichten auf Deutung, finden uns mit dem Unvermeidlichen und Unverständlichen ab, rechnen quantenphysikalisch, machen die Augen zu und: durch!

Literatur

Bennewitz, Roland/Crain, Jason N./Kirakosian, Armen u. a.: »Atomic scale memory at a silicon surface«, in: Nanotechnology 13 (2002), S. 499–502.

Bohr, Niels: »Discussion with Einstein on Epistemological Problems in Atomic Physics«, in: Paul Arthur Schilpp (Hrsg.), Albert Einstein. Philosopher-Scientist, La Salle, Illinois: Open Court 1949, S. 199-241.

Communications of the ACM, Vol. 41 No. 8 (1998), S. 50.

Deutsch, David: Die Physik der Welterkenntnis, München: DTV 2000.

Everett III, Hugh: »›Relative State‹ Formulation of Quantum Mechanics«, in: Reviews of Modern Physics Vol. 29 #3 (July 1957), S. 454-462.

Kurtsiefer, Christian/Weinfurter, Harald u. a.: »A step towards global key distribution«, in: Nature, Vol. 419 (2002), S. 450.

Shor, Peter W.: »Algorithms for quantum computation. Discrete logarithms and factoring«, in: 35th Annual Symposium on Foundations of Computer Science, Los Alamitos: IEEE Computer Society Press 1994, S. 124-134.

Williams, Colin P./Clearwater, Scott H.: Ultimate Zero and One. Computing at the Quantum Frontier, New York: Copernicus 2000.
Zeilinger, Anton: Einsteins Schleier. Die neue Welt der Quantenphysik, München: C. H. Beck 2003.

erschienen in: Martin Warnke, Georg Christoph Tholen, Wolfgang Coy (Hrsg.): HyperKult II – Zur Ortsbestimmung analoger und digitaler Medien. transcript, Bielefeld 2005. S. 151-172. ISBN 3-89942-274-0.