Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich (2010) 155(3/4): 69–74

Vom klassischen Computer zur Quanten-Information

Klaus Ensslin (Zürich)

Zusammenfassung

Unsere moderne Informationsgesellschaft basiert auf leistungsfähigen Computern, deren Funktionsweise überwiegend auf den Gesetzen der klassischen Physik beruht. Die Quantenmechanik beschreibt die Gesetze des Mikrokosmos, der Welt der Atome und Elektronen. Obwohl diese Gesetze häufig wenig intuitiv erscheinen, wurden sie mittlerweile durch zahlreiche Experimente bestätigt. Ein Elektron kann sich in zwei Zuständen gleichzeitig befinden, es könnte sich z. B. an zwei verschiedenen Orten aufhalten oder sich in zwei verschiedene Richtungen drehen. Diese Überlagerung von Zuständen kann genutzt werden, indem man ein klassisches bit, das entweder den Wert «0» oder den Wert «1» hat, durch ein qubit (quantum bit) ersetzt, dessen Zustand eine Überlagerung der Werte «0» und «1» ist. Diese Parallelität kann in einem zukünftigen Quanten-Computer für die effiziente Lösung gewisser Probleme eingesetzt werden, die für einen herkömmlichen Computer schwierig oder nur sehr langsam bearbeitbar sind. Dieser Artikel beschreibt die Grundlagen der klassischen und der Quanten-Informationsverarbeitung anhand von ausgewählten Beispielen.

From classical computers to quantum information processing

Our modern information society is based on powerful computers whose functionality is mainly governed by the laws of classical physics. Quantum mechanics describes the laws of the microcosm, i. e. the world of atoms and electrons. These laws often appear counterintuitive, but have been verified by numerous experiments. An electron may be in two states simultaneously, for example it may be at two different locations or it may rotate with two different angular momenta. Such superpositions of states can be exploited by replacing a classical bit, which takes on either the value «0» or the value «1», by the qubit (quantum bit), whose state is a superposition of the values «0» and «1». This parallelism can be used in a future quantum computer for the efficient solution of a special class of problems, which are hard to tackle for a conventional computer or whose solution may take an unacceptably long time. This article describes the basics of classical and quantum information processing using selected examples.

Schlagwörter: **Klassische Physik – Informationsverarbeitung – Quantenmechanik – Nicht-Lokalität – bits und qubits**

Keywords: **classical physics – information processing – quantum mechanics – non locality – bits and qubits**

1 EINLEITUNG

Die klassische Mechanik ordnet bewegten Objekten eine Geschwindigkeit und einen Ort zu einer bestimmten Zeit zu. Diese äusserst erfolgreiche Beschreibungsweise erlaubt beispielsweise die Berechnung der Bahn einer Billardkugel oder den Bremsweg eines Autos. Für sehr kleine Systeme wie Atome oder Elektronen ist diese klassische Beschreibungsweise jedoch unzureichend. Ein Elektron kann z. B. in zwei Zuständen gleichzeitig sein, d. h. es könnte gleichzeitig an zwei Orten sein oder sein Drehimpuls kann zu gegebener Zeit zwei verschiedene Werte gleichzeitig annehmen. Obwohl derartige Aussagen mit unserer täglichen Erfahrungswelt nur schwer in Einklang zu bringen sind, ist dieses «sowohl-als-auch» der Quantenmechanik durch zahlreiche Experimente bestätigt worden. Die meisten technischen Produkte unserer modernen Welt funktionieren hauptsächlich nach den Gesetzen der klassischen Physik. Die Theorien der Newton'schen Mechanik, der Thermodynamik sowie der Elektrodynamik sind inzwischen zum Teil mehrere Jahrhunderte alt. Trotzdem sind diese Konzepte immer noch die Grundlage für

das Funktionieren von Kühlschränken, Autos, Staubsaugern und Flugzeugen. Selbst moderne mikroelektronische Schaltkreise gehorchen nach wie vor in ihren wesentlichen Funktionen den Gesetzen der klassischen Physik. Diese Schaltkreise werden zwar heute immer kleiner und stossen mit ihrer Grösse in atomare Dimensionen vor. Dabei werden die Gesetze der Quantenmechanik relevant. Die heutige Ingenieurskunst besteht oft darin, einen neuen superkleinen Transistor zum Funktionieren zu bringen, obwohl die Elektronen aufgrund der Quantenmechanik eigentlich eher andere Wege gehen würden. Die Quantenmechanik wird oft eher als ein zu umgehendes Übel angesehen, denn als Chance, die völlig neue Möglichkeiten für moderne Technologien eröffnen könnte.

Die Quantenmechanik ist eine der intellektuell anspruchsvollsten und experimentell bestbestätigten Theorien der modernen Wissenschaften. Es gibt bis heute kein Experiment, dessen Ergebnis den Gesetzen der Quantenmechanik widerspricht. Gleichzeitig sind viele Vorhersagen der Quantenmechanik für mikroskopische Systeme so fern jeglicher Erfahrung unseres täglichen Lebens, dass ein intuitiver und leicht verständlicher Zugang für Nicht-Spezialisten nur schwer zu erreichen ist. So ist z. B. die Verschränkung (engl. entanglement) eine quantenmechanische Korrelation oder «spukhafte Fernwirkung» zweier Teilchen, wie Einstein dieses Phänomen bezeichnet hat, ohne Analogie in der täglichen Erfahrungswelt. Dies macht die Umsetzung und Nutzung der Gesetze der Quantenmechanik für technische Entwicklungen zu einer Herausforderung.

2 WIE FUNKTIONIERT EIN KLASSISCHER COMPUTER?

In unserem täglichen Leben benutzen wir das Dezimalsystem für die Darstellung von Zahlen. Ebenso können aber auch andere Zahlensysteme benutzt werden, wie z. B. das Binärsystem. Beim Dezimalsystem besteht jede Zahl aus einer Abfolge von Ziffern, die Vielfache von Zehnerpotenzen auflisten.

Beispiel Zehnersystem: $153 = 1 \bullet 10^2 + 5 \bullet 10^1 + 3 \bullet 10^0$

Ebenso kann man die Zahlen auch im Binärsystem darstellen, bei dem jede Ziffer nur die Werte «0» oder «1» annehmen kann und bei dem die Ziffern entsprechend Vielfache von Zweierpotenzen auflisten.

Beispiel Zweiersystem

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$

also

$$153 = 128 + 16 + 8 + 1 = 1 \bullet 2^7 + 0 \bullet 2^6 + 0 \bullet 2^5 + 1 \bullet 2^4 + 1 \bullet 2^3 + 0 \bullet 2^2 + 0 \bullet 2^1 + 1 \bullet 2^0$$

Damit schreibt sich die Zahl 153_{10} im Zehnersystem als 10011001_2 im Zweiersystem oder Binärsystem (die tiefgestellten Zahlen bezeichnen das benutzte Zahlensystem).

Jede Zahl und jede quantitative Information kann in Einheiten von bits gespeichert werden. Ein bit ist ein klassisches physikalisches System, das zwei durch Messung gut unterscheidbare Zustände haben kann, die wir mit «0» oder «1» bezeichnen. Ein Beispiel wäre ein Wasserhahn, der entweder offen oder zu ist, oder eine Lampe, die entweder an oder aus ist. Jede Rechenmaschine besteht aus einer Anordnung von Schaltern, die ein- oder ausgeschaltet werden können. Durch eine entsprechende Anordnung von Schaltern kann mit Hilfe des Binärsystems jede beliebige Zahl dargestellt werden. Ein Rechenvorgang bedeutet eine Kombination von solchen Schaltern mit entsprechenden Rechenvorschriften, die angeben, nach welchen Regeln die Schalter bei bestimmten Rechnungen umgelegt werden.

Bei einem modernen Computer wird so ein Schalter durch einen Transistor realisiert. Dieser Transistor kann den elektrischen Strom entweder durchlassen oder eben nicht. Das sind die beiden Zustände, die die Zahlen «0» oder «1» repräsentieren. Bei der heute benutzten CMOS-Logik fliesst nur wenig Strom beim schnellen Umschalten von «0» nach «1». Der Transistor kann durch eine elektrische Spannung geschaltet werden und von einem anderen Transistor wie ein Wasserhahn auf oder zu gemacht werden. Die grosse Rechenleistung moderner Computer beruht auf der enormen Packungsdichte so genannter integrierter Schaltkreise, bei denen heutzutage Milliarden von Transistoren auf einem Chip zusammengeschaltet werden, um damit komplizierte Rechnungen mit ungeheurer Geschwindigkeit lösen zu können.

3 WAS IST QUANTEN-INFORMATION?

Ein Elektron kann quantenmechanisch durch eine Überlagerung zweier Zustände beschrieben werden. Salopp ausgedrückt bedeutet dies, dass ein Elektron quantenmechanisch in zwei Zuständen gleichzeitig sein kann. Zum Beispiel könnte das magnetische Moment des Elektrons (Eigendrehimpuls, auch Spin genannt) eine Überlagerung der Zustände sein, in denen sein Spin nach oben oder nach unten zeigt. Dies passiert so lange, bis das Elektron, oder besser gesagt sein Spin, entweder mit seiner Umgebung gekoppelt wird oder bis eine Messung durchgeführt wird. Sobald das Elektron einer Messapparatur mitteilen muss, in welche Richtung sein Spin zeigt, wird die Antwort «oben» oder «unten» sein. Eine mehrfache Wiederholung des

Experiments wird verschieden viele Ergebnisse für «oben» und «unten» liefern. Diese Häufigkeitsverteilung für die Messung von quantenmechanisch überlagerten Zuständen ist in vielen Experimenten bestätigt worden. Nennen wir den Zustand mit «Spin nach oben» im Folgenden «0» und den Zustand mit «Spin nach unten» «1». Dann bedeutet die Überlagerung zu einem allgemeinen quantenmechanischen Zustand «x», die Summe «x» = α • «0» + b • «1» zu bilden, wobei α und b Zahlen sind, die mathematisch beschreiben, mit welcher Wahrscheinlichkeit der Spin bei einer Messung nach oben («0») oder nach unten («1») zeigend gefunden wird.

Die Schrödinger-Gleichung, die die mathematische Grundlage für die Lösung quantenmechanischer Probleme liefert, ist eine lineare Gleichung. Diese Linearität bewirkt die Überlagerung bzw. die Superponierbarkeit von Lösungen. Dies hat die folgende wichtige Konsequenz: falls zwei verschiedene Funktionen (man nennt sie dann Wellenfunktionen) die Schrödingergleichung lösen, dann löst auch eine lineare Kombination (d. h. die Summe von Vielfachen der Funktionen) das Problem. Aus einem klassischen bit (entweder «0» oder «1») wird so ein quantum bit, auch qubit genannt (gleichzeitig «0» und «1»). Auf den ersten Blick scheint ein qubit viel unhandlicher zu sein als ein bit. Ein qubit ist nicht scharf definiert und die ganze Präzision der digitalen Datenverarbeitung scheint verloren zu gehen. Was gewinnt man dafür? Ein qubit, welches den Gesetzen der Quantenmechanik gehorcht, besteht aus einer Überlagerung von Zuständen. Man spricht auch von Parallelität einer Quantenrechnung, weil man dieselbe Rechnung mit der «0» und der «1» gleichzeitig durchführt. Das qubit kann in verschiedenen Basiszuständen («0» und «1») gemessen werden, mit klassischen bits kann man das nicht. So kann man mit qubits in einem Schritt Information über Korrelationen zwischen zwei Zuständen erhalten, für die man klassisch zwei Rechnungen durchführen muss. Doch wozu soll dies gut sein? Ein Quantencomputer kann schneller sein als ein klassischer Computer, wenn es ein Problem zu lösen gilt, welches von solch einer parallelen Datenverarbeitung profitiert. Die Addition von zwei Zahlen ist ein serieller Prozess, d. h. es werden verschiedene Rechenschritte nacheinander ausgeführt. Der dritte Schritt kann erst ausgeführt werden, wenn das Ergebnis des zweiten Schritts bekannt ist. Deswegen werden Zahlen vermutlich auch weiterhin von einem klassischen Computer addiert werden, der sehr gut serielle Probleme lösen kann. Im Folgenden sind zwei Beispiele aufgeführt, die aufzeigen, wie ein Quanten-Computer möglicherweise parallele Probleme schneller lösen könnte.

4 BEISPIEL: DAS INVERSE TELEFONBUCH-PROBLEM

Bei einem normalen Telefonbuch sind die Einträge alphabetisch geordnet. Wenn man die Telefonnummer einer bestimmten Person herausfinden will, so blättert man durch die Seiten, bis der entsprechende Eintrag des Namens gefunden wird. Dies ist ein serieller Prozess, den ein klassischer Computer (und ein Mensch) sehr gut bewältigen kann. Ist umgekehrt die Telefonnummer bekannt und die dazugehörige Person gesucht, so bleibt einem klassischen Computer (oder einem Menschen) nichts anderes übrig, als das ganze Telefonbuch zu durchsuchen, bis die Nummer gefunden wird. Dieser Weg kann bei einem dicken Telefonbuch (oder allgemein bei einer grossen Datenbank) lange dauern. Stünde hingegen ein Quanten-Computer zur Verfügung, der die ganze Information des Telefonbuchs in qubits, d. h. in einer parallelen Überlagerung von Datensätzen vorliegen hätte, so würde im Prinzip ein einziger Rechen-

Abb. 1. Das inverse Telefonbuch-Problem.
Fig. 1. The inverse telefone book problem.

schritt genügen, um die zur bekannten Telefonnummer zugehörige unbekannte Person zu finden. Nun sind klassische Computer heutzutage so leistungsfähig, dass sie auch ein normales Telefonbuch mit grosser Geschwindigkeit nach beliebigen auch nicht geordnet vorliegenden Informationen durchforsten können (Abb. 1). Für komplexere Datenbankabfragen könnte der Quanten-Computer jedoch einen Vorteil bringen.

5 BEISPIEL: PRIMFAKTOR-ZERLEGUNG

Die Primfaktor-Zerlegung von 15 ergibt $15 = 5 \cdot 3$. Für einigermassen handliche Zahlen lässt sich eine solche Aufgabe im Kopf lösen. Bei grossen Zahlen wird die Lösung jedoch schnell zeitaufwendig. Woran liegt das? Um die Primfaktoren einer grossen Zahl zu finden, bleibt einem nichts anderes übrig, als sequentiell alle Zahlen der Reihe nach auszuprobieren. Auch ein Computer löst dieses Problem auf sequentielle Art. Falls es also um die Primfaktor-Zerlegung sehr grosser Zahlen geht, so benötigt auch der beste heute verfügbare Computer mehrere Jahre für die Lösung. Dies ist der Grund, warum die am weitesten verbreitete Datenchiffrierung (die RSA-Verschlüsselung) heutzutage auf einem Code basiert, der zur Entschlüsselung eine Primfaktor-Zerlegung erfordert. Während die beiden Partner, die vertrauliche Daten austauschen wollen, den Code kennen (Primzahlen miteinander zu multiplizieren geht einfach und schnell), muss jemand, der die Daten abhören will, eine grosse Zahl (typischerweise bestehend aus bis zu 2048 bits, das ist eine Zahl mit über 600 Dezimalstellen) in Primfaktoren zerlegen und benötigt dafür nach heutigem Wissensstand und Technik zu lange für praktische Belange. Ein potenzieller Quanten-Computer löst Probleme mit einem parallelen Ansatz. Die Primfaktor-Zerlegung ist eine Aufgabe, die durch parallele Rechenmethoden viel schneller gelöst werden kann. Deswegen könnte ein Quanten-Computer alle heute eingesetzten Kryptographie-Verfahren obsolet machen. Gleichzeitig bietet die Quantenmechanik jedoch neue Wege für eine absolut sichere Datenübertragung.

6 WISSENSCHAFT UND TECHNOLOGIE

Die Quantenmechanik ist mittlerweile fast 100 Jahre alt. Warum sind diese Konzepte nicht schon früher in Technologien umgesetzt worden? Einstein, Bohr, Heisenberg, Schrödinger und viele andere haben grundlegende Beiträge zum Verständnis von atomaren Vorgängen geliefert. Schon früh hat sich Einstein aus prinzipiellen philosophischen Gründen dagegen gewehrt, dass es so etwas wie Nicht-Lokalität physikalisch geben darf, nämlich dass die Manipulation des einen Teils zweier (verschränkter) Quantenobjekte an einem Ort den Zustand des anderen Teils an einem anderen Ort verändert. Deswegen hat Einstein zahlreiche so genannte «Gedankenexperimente» entwickelt, bei denen es um die Frage ging, was wäre, wenn? Diese Gedankenexperimente waren in den 20er Jahren des letzten Jahrhunderts experimentell nicht zugänglich und wurden daher meist auf philosophisch/theoretischer Ebene diskutiert. Eines der berühmtesten Gedankenexperimente ist das Einstein-Podolsky-Rosen-Paradoxon (EINSTEIN, PODOLSKY, ROSEN, 1935). Es geht dabei um die Frage, ob zwei Teilchen an verschiedenen Orten, oder allgemeiner zwei quantenmechanische Objekte in einem überlagerten Zustand, sich sofort gegenseitig beeinflussen können, wenn der Zustand eines der Teilchen experimentell bestimmt wird. Erst in den 1970er und 1980er Jahren gab es Experimente mit Photonen, den Quanten des Lichts, die tatsächlich bewiesen, dass die Vorhersagen der Quantenmechanik auch in diesem Fall korrekt sind (ASPECT, GRANGIER, ROGER, 1982). Es ist also richtig, dass sich ein Teilchen in einer Überlagerung zweier Zustände befinden kann, auch wenn dies mit unserem täglichen Erfahrungsschatz inkompatibel zu sein scheint. Durch die stetige Weiterentwicklung der technologischen Methoden in den letzten 20 Jahren ist es gelungen, diese grundlegenden Konzepte der Quantenmechanik in vielen Laborexperimenten zu überprüfen und für Anwendungen nutzbar zu machen. Damit sind die intellektuellen Subtilitäten von Einstein und seinen Mitstreitern in vielen Labors zur Realität geworden. Ein Beispiel soll im Folgenden diskutiert werden.

7 ELEKTRONENZÄHLER AUF EINEM HALBLEITERCHIP

Abb. 2 zeigt die Oberfläche eines Halbleiter-Wafers, die mit den Methoden der Nanotechnologie strukturiert wurde. Die Hügellandschaft, die das Bild suggeriert, spiegelt in guter Näherung das Potenzial wieder, in dem sich die Elektronen bewegen. In den schwarzen Bereichen, d.h. in den Tälern bei tiefem Potenzial, können sich Elektronen frei bewegen. Die grauen Barrieren sind jedoch undurchdringlich für Elektronen. Falls sich ein Elektron von Gebiet A zu Gebiet B bewegen will, muss es die Ringstruktur dazwischen durchqueren. Dabei hat es die Möglichkeit, entweder den oberen Weg (markiert mit 0) oder den unteren

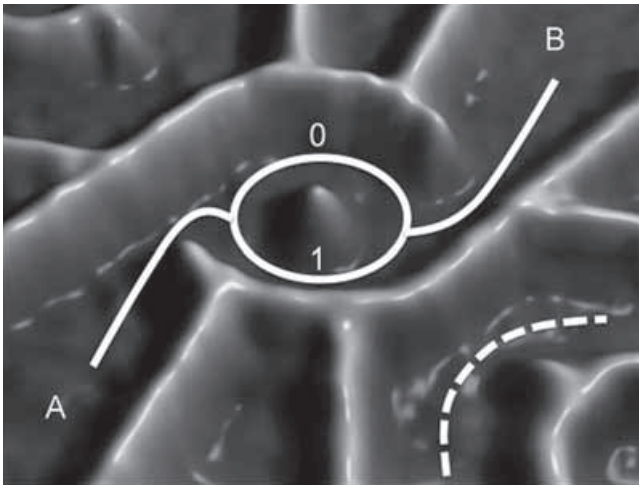

Abb. 2. Oberfläche eines Halbleiter-Wafers. Die Hügellandschaft repräsentiert das Potenzial, in dem sich die Elektronen bewegen (aus GUSTAVSSON et al. 2008).

Fig. 2. Surface of a semiconductor wafer. The hilly surface represents the potential, in which electrons move (from GUSTAVSSON et al. 2008).

Weg (markiert mit 1) zu nehmen. Aufgrund der Gesetze der Quantenmechanik führt die Möglichkeit, auf zwei verschiedenen Wegen zum Ziel zu kommen, zur Überlagerung von Zuständen und damit zu Interferenz.

Interferenz ist ein Phänomen, welches auftritt, wenn sich Wellen überlagern. Wirft man einen Stein ins Wasser, so bilden sich kreisförmige Wellen, die sich radial vom Zentrum entfernen. Werden zwei Steine gleichzeitig an verschiedenen Stellen ins Wasser geworfen, so breiten sich die Kreiswellen um jeden Auftreffpunkt aus und überlagern sich. Treffen zu einem Zeitpunkt an einem bestimmten Ort zwei Wellenberge aufeinander, entsteht ein noch höherer Wellenberg (konstruktive Interferenz). Wenn hingegen Minimum auf Maximum trifft, so kann dies zu Auslöschung führen (destruktive Interferenz). Ein Elektron, welches sich nach den Gesetzen der Quantenmechanik bewegt, hat Wellencharakter. Deswegen können Teilwellen, die verschiedenen Bahnen wie denjenigen in der obigen Figur folgen, miteinander interferieren. Dies kann dazu führen, dass das Elektron entweder gar nicht von A nach B gelangt, weil sich ein Minimum mit einem Maximum ausgelöscht hat (destruktive Interferenz), oder dass das Elektron von A nach B gelangt, weil sich zwei Maxima getroffen haben (konstruktive Interferenz).

Um die Verschiebung von Minima und Maxima (oder umgekehrt) zu beeinflussen (Phasenverschiebung), kann man sich einen grundsätzlichen physikalischen Effekt, den Aharonov-Bohm-Effekt, zu Nutze machen (AHARONOV, BOHM, 1959). Dieser Effekt führt dazu, dass sich die Phase, d.h. die relative Position eines Maximums (oder Minimums) der Welle, durch ein Magnetfeld verschieben lässt. Legt man nun ein Magnetfeld senkrecht zur oben gezeigten Ringstruktur an, können die Maxima der Teilwellen durch die beiden Ringarme «0» und «1» relativ zueinander verschoben werden. Man erwartet also, dass sich der elektrische Widerstand der Ringstruktur als Funktion eines Magnetfelds verändert, weil das Magnetfeld von «sich überlagernden Teilwellen» zu «sich auslöschenden Teilwellen» hin und herschaltet. Die gestrichelte Linie im unteren Teil der Abb. 2 zeigt einen weiteren Stromkreis, der dazu dient, die einzelnen Elektronen zu messen, welche die Ringstruktur durchqueren. Der elektrische Widerstand dieser «Messapparatur» ändert sich, wenn ein Elektron den Ring durchquert hat, oder eben nicht.

Abb. 3 zeigt die Zählrate (counts per second) des oben beschriebenen Elektronenzählers als Funktion des Magnetfelds. In der Tat variiert die Zählrate periodisch mit dem Magnetfeld. Dies bedeutet, dass Interferenz für einzelne Elektronen auf einem solchen Halbleiterchip nachgewiesen wurde. Jedes Elektron interferiert mit sich selbst. Das kann nur der Fall sein, wenn die beiden Teilwellen des Elektrons, die die beiden Zustände beschreiben, gleichzeitig die Pfade «0» und «1» durchlaufen. Die periodische Zählrate ist also direkt ein experimenteller Beweis für das «sowohl als auch» der Quantenmechanik. Während derartige Experimente vor 20 Jahren mit hochkomplexen Apparaturen durchgeführt wurden, ist es heute möglich, die Gedankenexperimente der Gründer der Quantenmechanik auf einem Halbleiterchip durchzuführen, der nicht grundsätzlich verschieden ist von den Strukturen, die in unseren heutigen Computern ihren Dienst verrichten. Lediglich die Abmessungen dieses ringartigen Einelektronen-Transistors sind kleiner als bei

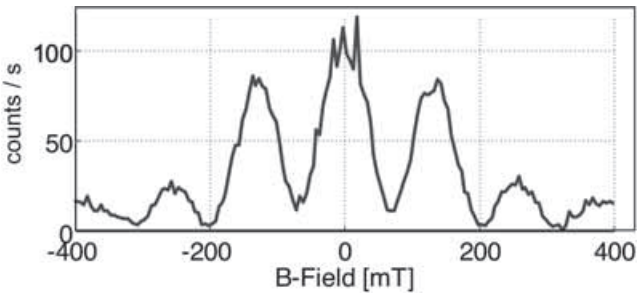

Abb. 3. Elektronenrate als Funktion der magnetischen Feldstärke in einem Elektronenzähler (aus GUSTAVSSON et al. 2008).

Fig. 3. Electron rate as a function of magnetic field strength in an electron counter (from GUSTAVSSON et al. 2008).

kommerziellen Transistoren und seine Temperatur liegt weit unter der Raumtemperatur.

8 WO GEHT DIE REISE HIN?

Das obige Beispiel soll illustrieren, dass grundsätzliche Konzepte der Quantenmechanik, wie die Nicht-Lokalität oder die Überlagerung von verschiedenen Zuständen, nicht nur abstrakte Gedankengebäude sind, sondern zu messbaren Konsequenzen in handfesten Laborexperimenten führen können. Dies nimmt diesen Phänomenen nichts von ihrer Eigenartigkeit. Sie bleiben ausserhalb unseres unmittelbaren Erfahrungsbereichs und lassen sich deswegen nur sehr begrenzt mit Analogien aus unserem täglichen Leben (siehe Beispiel Wasserwellen) verstehen. Nichtsdestotrotz hat die enorme technische Entwicklung der letzten Jahrzehnte zu Experimenten geführt, die es erlauben, grundsätzliche quantenmechanische Effekte nicht nur nachzuweisen, sondern Quantensysteme auch sehr präzise zu manipulieren und für gewisse Zwecke masszuschneidern. Dies ist normalerweise der Übergang von den Grundlagen-Wissenschaften zu den Ingenieurs-Wissenschaften. Es geht jetzt darum, den Weg von «quantum science» zu «quantum engineering» vorzubereiten.

Eine mögliche Anwendung von Quantensystemen für die Informations-Verarbeitung wurde in den vorherigen Kapiteln skizziert. Der Weg zu einem tatsächlichen Quanten-Computer wird jedoch noch steinig und lang sein. Der «beste» bis heute realisierte Quanten-Computer war in der Lage, die Zahl 15 in ihre Primfaktoren zu zerlegen. Das entspricht ungefähr dem Zustand der Mikroelektronik kurz nach der Entwicklung des ersten Transistors 1948. Niemand hat damals die Entwicklung hin zu moderner Datenverarbeitung und unserer heutigen Informations-Gesellschaft vorhergesagt. Das Internet hat sich erst viel später entwickelt. Genauso wenig ist im Moment klar, welche überraschenden Anwendungen sich aus «quantum science» und «quantum engineering» ergeben werden. Möglicherweise werden sich die ersten neuen Technologien im Bereich von Quanten-Computern oder auch Quanten-Kryptographie etablieren. Es könnte jedoch genauso sein, dass sich völlig neue Gebiete für Anwendungen ergeben werden, die wir im Moment nicht einmal erträumen können.

9 SCHLUSSBEMERKUNG UND VERDANKUNGEN

In den letzten zehn Jahren haben sich Physiker aus den Bereichen der Quantenoptik und der Festkörperphysik zusammengefunden, um mit komplett verschiedenen Experimenten intellektuell sehr verwandte Fragestellungen zu untersuchen. Mittlerweile sind Wissenschafter aus der Chemie, der Informatik, der Elektrotechnik sowie der Mathematik dazugestossen und es entwickelt sich ein zunehmend intensiverer Diskurs über die Zukunft der Quanten-Wissenschaften. An der ETH Zürich finden diese Diskussionen innerhalb des Netzwerks QSIT (quantum systems for information technology, www.qsit.ethz.ch) statt. Zahlreichen Kollegen aus diesem Kreis bin ich dankbar für den Austausch von Ideen, die auch in diesem Artikel beschrieben wurden. Speziell möchte ich mich bei Simon Gustavsson, Renaud Leturcq und Thomas Ihn für die Zusammenarbeit bedanken, die zu den Experimenten mit einzelnen Elektronen in Ringstrukturen geführt hat. Für Kommentare zu diesem Artikel bedanke ich mich bei Ilona Blatter, Christina Egli, Jonathan Ensslin, Thomas Ihn und Claudia Vinzens.

10 LITERATUR

AHARONOV, Y. and BOHM, D. 1959. Significance of electromagnetic potentials in quantum theory, Physical Review 115, 485.

ASPECT, A., GRANGIER, P. and ROGER, G. 1982. Experimental Realization of Einstein-Podolsky-Rosen-Bohm-Gedankenexperiment: A new violation of Bell's inequalities, Physical Review Letters 49, 91.

EINSTEIN, A., PODOLSKY, B. and ROSEN, N. 1935. Can quantum-mechanical description of physical reality be considered complete?, Physical Review 47, 777.

GUSTAVSSON, S., LETURCQ, R., STUDER, M., IHN, T., ENSSLIN, K., DRISCOLL, D. C. and GOSSARD, A. C. 2008. Time-resolved detection of single-electron interference, Nanoletters 8, 2547.

Prof. Klaus Ensslin, Laboratorium für Festkörperphysik der ETH Zürich, Schafmattstrasse 16, CH-8093 Zürich,
E-Mail: ensslin@phys.ethz.ch

Image: Quantum error correction protocols detect and correct processing errors in trapped-ion quantum computers. (Credit: IQOQI Innsbruck/Harald Ritsch). In order to reach their full potential, todayâ€™s quantum computer prototypes have to meet specific criteria: First, they have to be made bigger, which means they need to consist of a considerably higher number of quantum bits. Second, they have to be capable of processing errors. â€œWe still fail in running complex computations because environmental noise and errors cause the system to get out of control,â€ says quantum physicist Rainer Blatt fro http://quanten-computer.eu. Physik. Domain info. Latest check. 5 months ago.