ten eine Penning-Falle, die in zwei Segmente unterteilt ist (siehe Foto), in eine „Präzisionsfalle“ mit homogenem und eine „Analysatorfalle“ mit inhomogenem Magnetfeld [4]. Zwischen diesen beiden Segmenten können die Autoren das Ion mithilfe elektrischer Felder adiabatisch hin- und herschieben. So wird zunächst in der Analysatorfalle durch eine Art kontinuierlichen Stern-Gerlach-Effekt der Spinzustand des gespeicherten $^{12}C^{5+}$-Ions bestimmt. Anschließend wird das Ion in die Präzisionsfalle transferiert und mit Mikrowellen bestrahlt. Die Wahrscheinlichkeit für einen Spin-Flip wird nach Rücktransfer des Ions in die Analysatorfalle vermessen. Diesen Vorgang wiederholt man bei verschiedenen Frequenzen, bis der Spin-Flip am effizientesten ist. Auf diese Weise erhält man die Larmor-Resonanz und damit die Larmor-Frequenz.

Die relative Elektronenmasse beträgt nach den Messungen von Beier et al. 0,000 548 579 909 2(4) u. Das Ergebnis bestätigt innerhalb der 1,5-fachen Standardabweichung die bis dahin beste Messung. Die relative Präzision von ungefähr 7×10^{-10} entspricht einer Verbesserung um einen Faktor 3. Damit liegt die Messung sicherlich noch deutlich unter der gewünschten Präzision von 2×10^{-10}. Erst bei einer solchen Genauigkeit würde die neu bestimmte Elektronenmasse wesentlichen Einfluss auf die Werte anderer Naturkonstanten nehmen, wie z. B. die Rydberg-Konstante. Die neue Messung liefert jedoch die gewünschte und wichtige Redundanz, die Elektronenmasse in einem unabhängigen Verfahren bestimmt zu haben.

Ulli Eichmann

[1] *P. J. Mohr* und *B. N. Taylor*, Rev. Mod. Phys. **72,** 351 (2000).
[2] *T. Beier* et al., Phys. Rev. Lett. **88**, 011603 (2002).
[3] *D. L. Farnham* et al., Phys. Rev. Lett. **75**, 3598 (1995).
[4] *H. Häffner* et al., Phys. Rev. Lett. **85**, 5308 (2000).

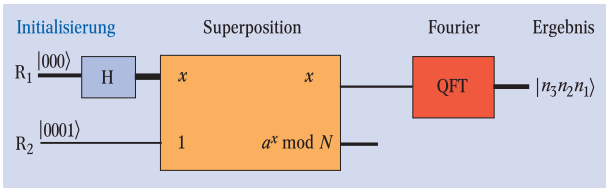
Kernspins knacken Code

Erstmals ist es Forschern gelungen, eine Zahl mit einem Quantencomputer zu faktorisieren.

Der Austausch geheimer Nachrichten funktioniert heute mit zwei binär codierten „Schlüsseln“, einem öffentlichen und einem geheimen. Der Sender verschlüsselt die Bits und Bytes der Nachricht mit dem öffentlichen Schlüssel des Empfängers, den dieser beispielsweise im Internet veröffentlicht hat, und schickt die entstehende Zahlenfolge auf nicht abhörsicheren Kanälen an den Empfänger. Der Empfänger dechiffriert die Geheimbotschaft mit seinem geheimen Schlüssel. So funktioniert zum Beispiel das Programm Pretty Good Privacy für die verschlüsselte Übermittlung von E-Mails. Die Sicherheit des Verfahrens beruht darauf, dass ein Spion zur *Entschlüsselung* der geheimen Botschaft eine große Zahl N in ihre Primfaktoren zerlegen müsste. Der Aufwand für die Zerlegung steigt jedoch exponentiell mit der Größe der Zahl N und wird bei großen Zahlen praktisch unmöglich. So würde die Zerlegung einer ganzen Zahl mit vierhundert Stellen mit den besten Höchstleistungsrechnern schätzungsweise zehn Milliarden Jahre dauern. Eine derartige Zahl gilt als *sicher*. Es ist deshalb nicht verwunderlich, dass Peter Shor 1994 gewaltiges Aufsehen erregte, als er einen Quantenalgorithmus vorschlug, der dies in etwa drei Jahren bewerkstelligen könnte, vorausgesetzt man hätte einen Quantencomputer.

Genau diesen Algorithmus haben Chuang und Mitarbeiter vom IBM Forschungslabor in Almaden, Kalifornien, nun in einer Minimalkonfiguration mit sieben Kernspins realisiert. Mit diesem System gelang es ihnen, die Zahl 15 durch quantenmechanische Operationen in die Faktoren 3 und 5 zu zerlegen – keine große Leistung für Kopfrechner, doch eine eindrucksvolle Demonstration der potenziellen Rechenleistung eines Quantencomputers.

Bislang werden unterschiedliche Ansätze verfolgt, einen Quantencomputer zu realisieren. So experimentieren einige Gruppen mit Ionen in einer Ionenfalle oder mit Quantenpunkten in einem Halbleiter. Die Quantenzustände der einzelnen Ionen und Quantenpunkte dienen dabei als so genannte Qubits. Im Unterschied zu klassischen Bits können sie nicht nur die Werte 0 und 1 speichern, sondern auch quantenmechanische Superpositionen, etwa $(|0\rangle+|1\rangle)/\sqrt{2}$. Bei Rechenoperationen mit solchen Zuständen können alle möglichen Rechenwege parallel berücksichtigt werden. Auf dieser „massiven Quantenparallelität“ beruht die Schnelligkeit von Quantencomputern. Chuangs Gruppe experimentiert schon seit einigen Jahren mit „NMR-Quantencomputing“ (NMR steht für *nuclear magnetic resonance*). Dabei dienen Moleküle in einer Flüssigkeit und ein NMR-Spektrometer als Hardware. Als Qubits fungieren die Kernspins der einzelnen Atome in den Molekülen. Die Kernspins lassen sich aufgrund unterschiedlicher Resonanzfrequenzen mit Hochfrequenz gezielt adressieren und auslesen. Außerdem beruhen Rechenoperationen auf der Wechselwirkung der Kernspins untereinander. In diesem System führten Chuang et al. nun den Shor-Algorithmus aus.



Ein Quantencomputer nutzt das Superpositionsprinzip, um viele Rechenschritte gleichzeitig auszuführen und damit die Primfaktoren zu bestimmen. Nach der Initialisierung (H) werden die Quantenregister R_1 sowie R_2 superponiert. Eine Fourier-Transformation liefert das gewünschte Ergebnis.

Um einen effizienten Algorithmus zu finden, mit dem sich große Zahlen in ihre Primfaktoren zerlegen lassen, musste Shor tief in die Trickkiste der Zahlentheorie greifen. Die Idee besteht darin, die Primfaktorenzerlegung auf ein anderes Problem zurückzuführen: das Auffinden der Periode r der Funktion $f(x)=a^x \bmod N$, wobei N die zu faktorisierende Zahl ist und $a^x \bmod N$ bedeutet: bilde die Differenz von a^x und einem Vielfachen von N, so dass diese Differenz kleiner als N ist (mod steht für „modulo“). Betrachten wir das Beispiel $N=15$. Die Zahl $a<15$ muss im Shor-Algorithmus so gewählt werden, dass der größte gemeinsame Teiler (ggt) von a und $N=15$ gleich eins ist, d. h. $\mathrm{ggt}(a, 15)=1$. Dies trifft für die Zahlen $a=2$, 4, 7, 8, 11, 13, 14 zu und erfordert nicht die Kenntnis der Primfaktoren. Auch bei großen Zahlen N lassen sich geeignete Zahlen für a relativ leicht finden. Das nachfolgende Verfahren funktioniert dann mit jeder dieser Zahlen. Wie groß ist nun die Periode von $f(x)$? Für $a=2$, 7, 8 und 13 ist $f(x)=f(x+4n)$ mit ganzzahligem n, wie man leicht nachrechnen kann. Die Periode ist 4 für jeden dieser Werte von a. Für 4, 11 und 14 ergibt sich eine andere Periode.

Bei großen Zahlen lässt sich die Periode r nicht einfach durch Ausprobieren finden. Die Kunst besteht darin, einen Algorithmus zu finden, mit dem dies möglich ist. Ein Satz

aus der Zahlentheorie lehrt uns, dass $(a^{r/2}-1)\times(a^{r/2}+1)$ ein Vielfaches von N ist und dass eine gute Chance besteht, dass die Größen $\mathrm{ggt}(a^{r/2}-1, N)$ und $\mathrm{ggt}(a^{r/2}+1, N)$ Primfaktoren von N sind. In unserem Beispiel bedeutet dies $\mathrm{ggt}(7^{4/2}-1, 15)=3$ und $\mathrm{ggt}\,(7^{4/2}+1, 15)=5$. (Dies gelingt allerdings nicht in jedem Fall. Der Versuch muss dann mit anderen Werten von a wiederholt werden). Bei großen Zahlen steigt der Aufwand für die Berechnung des ggt nur mit einer Potenz von N und nicht exponentiell. Für diese Aufgabe genügt ein klassischer Computer.

Auf diese Weise hat Shor die Primfaktorenzerlegung zurückgeführt auf die Bestimmung der Periode von $f(x)$. Damit ist indes noch nichts gewonnen, denn auch diese Aufgabe wird exponentiell schwieriger mit wachsendem N. Der Trick besteht nun darin, für die Berechnung der Periode ebenfalls einen Quantenalgorithmus anzuwenden, und zwar die Quanten-Fourier-Transformation (QFT). Diese QFT nutzt wiederum die massive Quantenparallelität (Superposition und Verschränkung) aus, um schneller zum Ergebnis zu kommen als die klassische FFT. Hierfür muss zunächst eine Superposition aller möglichen Rechenwege konstruiert werden.

Dafür benötigen wir zwei Quantenregister R_1 und R_2. Register R_1 enthält die Zahl x und Register R_2 die Zahl $f(x)$. Beide Register werden kombiniert zu einem Gesamtzustand $|x,f(x)\rangle$. Für das Register $R_1=|n_3,n_2,n_1\rangle$ sehen wir drei Bits vor und für das Register $R_2=|m_4,m_3,m_2,m_1\rangle$ vier Bits, um die Zahlen 0, 1, ... , 15 zu repräsentieren. Insgesamt also sieben Bits. Da es sich um Qubits handelt, wird der gesamte erforderliche Quantenzustand durch $|R_1\rangle\,|R_2\rangle=|x,f(x)\rangle=|n_3,n_2,n_1,m_4,m_3,m_2,m_1\rangle$ beschrieben, wobei m_j, n_k die Werte $\pm1/2$ bzw. 0 oder 1 für die beiden Eigenzustände der Kernspins annehmen. Im Folgenden werden wir die Register auch in Dezimaldarstellung angeben, z. B. $R_1=|110\rangle=|6\rangle$.

In der Praxis verwenden die Autoren speziell synthetisierte Moleküle mit jeweils fünf ^{19}F- und zwei ^{13}C-Spins als Qubits. Jedes der Moleküle in flüssiger Phase stellt ein Quantenregister mit sieben Qubits dar. Im Prinzip ließen sich die Rechenoperationen mit einem einzigen Molekül als Quantencomputer durchführen, durch das Rechnen mit ca. 10^{20} Molekülen gleichzeitig wird jedoch das Signal verstärkt. Zum Auslesen der Quantenregister werden die Spektrallinien der Spins 1, 2 und 3 beobachtet. Sie geben Aufschluss über die Orientierung der einzelnen Kernspins. Zur Durchführung des Shor-Algorithmus strahlten Chuang et al. etwa 300 Hochfrequenzpulse selektiv auf die einzelnen sieben Kernspins ein. Zunächst brachten sie die Moleküle in den Anfangszustand $|R_1,R_2\rangle=|0,1\rangle=|0000001\rangle$ und die drei Qubits von R_1 zur Überlagerung von 0 und 1. Danach enthält R_1 alle acht Werte von x in Superposition. Eine anschließende Multiplikation mit R_2, welches so präpariert wurde, dass es $f(x)$ enthält, führt zum Quantenzustand

$$|\psi\rangle=\frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x,f(x)\rangle \quad .$$

Dieser Zustand enthält also eine Superposition aller möglichen Ergebnisse. Zur Festlegung der Periodizität von $f(x)$ wird nun noch eine QFT auf R_1 durchgeführt und das Ergebnis ausgelesen. Die Spektren von R_1 enthalten dabei die Information über die Periodizität.

Einen Geheimcode wird man mit diesem Experiment noch nicht knacken können. Jedoch zeigt dieses Beispiel, dass auch kompliziertere Quantenalgorithmen im Prinzip durchführbar sind. Ein Quantencomputer der Zukunft wird dann aber wohl aus festen und hochskalierbaren Bausteinen bestehen.

Michael Mehring

[1] *L. M. K. Vandersypen* et al., Nature **414**, 883 (2001)
[2] *P. Shor*, SIAM J. in Computing **26** 1484 (1997)
[3] *M. Mehring*, Appl. Mag. Res. **17**, 141 (1999)

Prof. Dr. Michael Mehring, 2. Physikalisches Institut, Universität Stuttgart, 70550 Stuttgart

Lupe im All

Einem internationalen Astronomen-Team ist es erstmals gelungen, einen als Gravitationslinse wirkenden Stern in unserer Milchstraße direkt zu fotografieren.

Die Schwerkraft wirkt nicht nur auf Materie, sondern sie zieht auch Lichtstrahlen an und lenkt sie von ihrer geradlinigen Bahn ab. Dies hat Albert Einstein 1916 in der Allgemeinen Relativitätstheorie hergeleitet. In Physik-Lehrbüchern ist nachzulesen, dass Arthur Eddington 1919 in der berühmten Sonnenfinsternis-Expedition diese Lichtablenkung gemessen und die Einsteinsche Vorhersage quantitativ bestätigt hat. Trotz dieses Erfolgs wurden „Gravitationslinsen“ lange Zeit als astronomische Kuriosität betrachtet. Selbst als Sjur Refsdal in den 60er Jahren zeigte [1], dass man mit der gravitativen Lichtablenkung sowohl die Massen von Sternen bestimmen als auch die Hubble-Konstante messen kann, die das Alter und die Größe des Universums bestimmt, gab es nur wenig Interesse an dieser Forschungsrichtung. Erst als 1979 mit dem Doppelquasar Q0957+561 das erste Gravitationslinsensystem identifiziert wurde [2], begann der Erfolgsweg dieser neuen Methode.

Seit fast drei Jahrzehnten gibt es Hinweise darauf, dass ein Großteil der Materie im Weltall nicht direkt sichtbar ist, sondern sich nur durch die Schwerkraftwirkung verrät. Mögliche Kandidaten für diese „Dunkle Materie“ sind einerseits „MACHOs“ (MAssive Compact Halo Objects), kompakte Objekte mit sternähnlichen Massen in den äußeren Bereichen der Milchstraße. Zum anderen gelten die so genannten „WIMPs“ (Weakly Interacting Massive Particles) als vielversprechend. Herkömmliche (licht-sammelnde) astronomische Beobachtungstechniken haben prinzipielle Schwierigkeiten beim Nachweis dieser Dunklen Materie. Der Gravitationslinseneffekt dagegen ist gut dafür geeignet. Dies ist sicher einer der Gründe, warum er in den letzten Jahren mehr und mehr Anwendungen erfuhr.

Heute untersucht man die Lichtablenkung von ganz verschiedenen Objekten, die nahezu 20 Größenordnungen in der Masse umfassen (für eine Übersicht, siehe etwa [3]): „Giant Luminous Arcs“ in Galaxienhaufen – hochverstärkte und stark verzerrte Bilder von Hintergrundgalaxien – helfen uns, Gesamtmasse und Massenverteilung in diesen Galaxienhaufen zu bestimmen. Aus der Zeitverzögerung der Lichtsignale von Mehrfachquasaren, die durch die Lichtaufspaltung einzelner Galaxien produziert werden, wird die Hubble-Konstante gemessen. Auch Objekte geringerer Masse wie einzelne Sterne und sogar Planeten können als Linsen wirken, auch „Microlensing“ genannt.

Und genau mit diesen Mikrolinsen kann man – wie im Jahre 1986