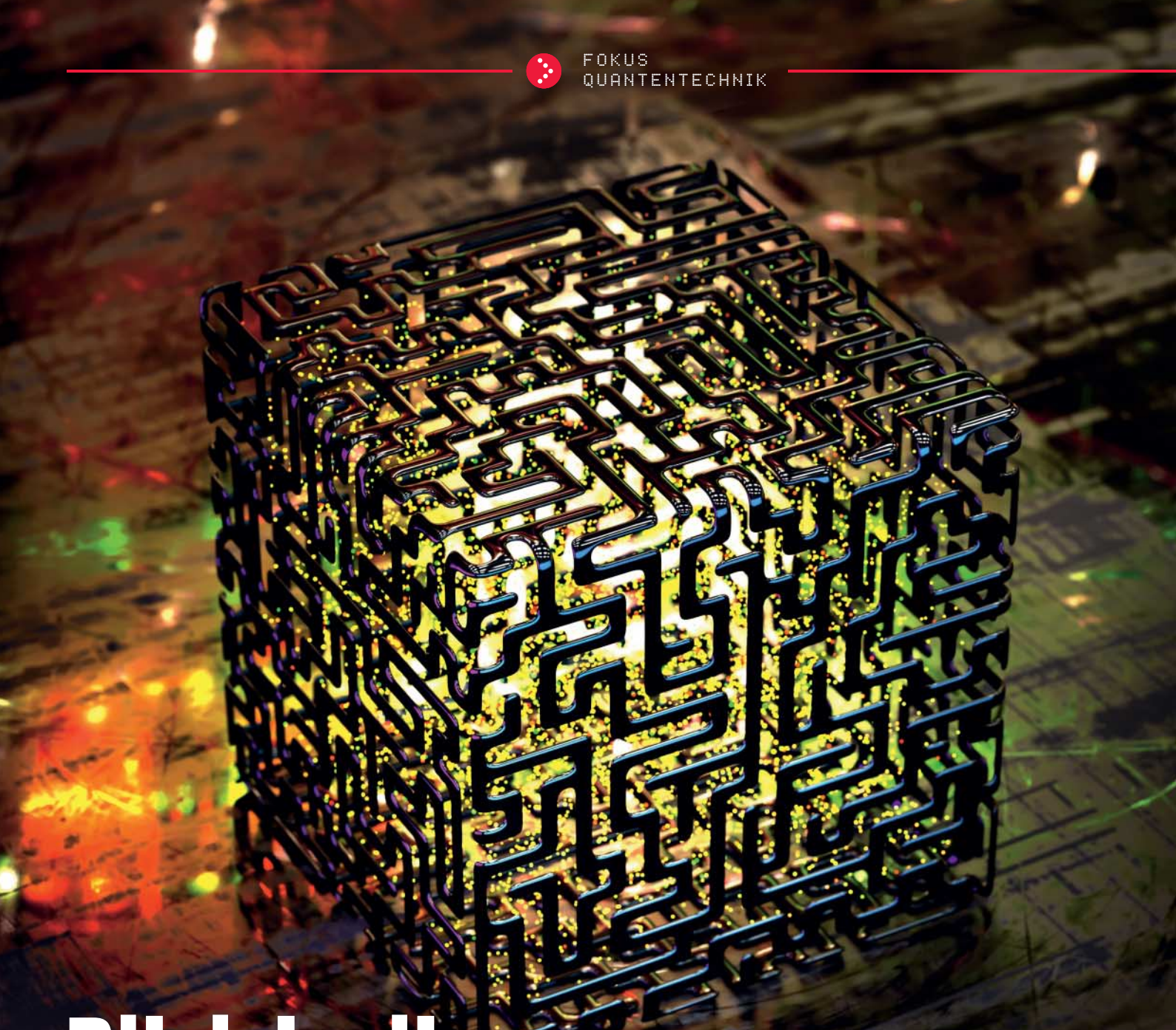


Blick in die Wunderkiste

Quantencomputer können viele Rechenoperationen parallel abarbeiten. Dazu nutzen sie die besonderen Spielregeln der Quantenwelt. Eine Einführung in die Funktionsweise der merkwürdigen Geräte.

VON NIELS BOEING

Im Zeitalter der Hochtechnologien ist ein Bonmot von Arthur C. Clarke zur Alltagsweisheit geworden, die in keiner Trendbroschüre fehlt. „Jede hinreichend fortgeschrittene Technologie ist von Magie nicht mehr zu unterscheiden“, schrieb Clarke 1973 in „Profiles of the Future“. Inzwischen scheinen sich auch IT -Konzerne damit abzufinden, wenn etwa IBM Quantencomputer in populärwissenschaftlichen Grafiken mit der „Magie der Quantenalgorithmen“ erklärt.

Der Grund dafür liegt in einer prinzipiellen Erkenntnis der Quantenmechanik aus den 1920er-Jahren: Ein physikalisches

Foto: Shutterstock

System des Quantenkosmos ist nicht in einem einzigen festgelegten Zustand, sondern in einer Überlagerung verschiedener möglicher Zustände. Ein Elektron etwa befindet sich mit unterschiedlichen Wahrscheinlichkeiten an verschiedenen Orten. Das brachte Physiker und Informatiker auf die Idee, mittels Überlagerung sogenannte Qubits zu schaffen, kurz für: Quantenbit. Den ersten Quantenalgorithmus präsentierte der Mathematiker Peter Shor 1996. In seinem epochalen Paper musste er aber noch zugeben: „Gegenwärtig weiß niemand, wie man einen Quantencomputer bauen könnte." Inzwischen weiß man es besser.

DIE GRUNDLAGEN

Während ein Bit dadurch dargestellt wird, dass am Ausgang eines Schaltkreises Strom fließt oder nicht (1 oder 0), lässt sich ein Qubit durch unterschiedliche Quantensysteme abbilden, bei denen eine bestimmte Zustandsgröße zwei Werte annehmen kann. Bei einem Elektron kann der Spin – oft lax als Eigendrehimpuls bezeichnet – nach oben oder nach unten zeigen. In supraleitenden Schleifen kann Strom bei ultrakalten Temperaturen widerstandslos mit oder gegen den Uhrzeigersinn kreisen. In einem Qubit können sich nun beide Zustände überlagern. Es gibt dort nicht 0 oder 1 wie bei klassischen Bits. Sondern 0 und 1.

Bei zwei Qubits sind die Möglichkeiten sogar noch vielfältiger: Dort überlagern sich auch die Kombinationen der Qubit-Zustände. Sie haben also parallel die Werte 00, 01, 10, 11 und repräsentieren damit 0, 1, 2, 3. Während ein zweistelliges Register aus zwei klassischen Bits eine einzige Zahl darstellen kann, kann ein zweistelliges Register aus zwei Qubits vier Zahlen darstellen. Ein zehnstelliges Register aus Qubits steht dann parallel für 1024 Zahlen, während ein zehnstelliges Register aus klassischen Bits immer noch nur eine Zahl repräsentiert.

Bei einigen Wissenschaftlern machte es da Klick. Lässt man einen klassischen Algorithmus auf die zehnstellige Binärzahl los, wird an dieser eine Rechenoperation durchgeführt. Ein Quantenalgorithmus hingegen lässt sich auf alle 1024 Binärzahlen parallel anwenden. Man könnte also im Prinzip Rechenaufgaben in Sekundenbruchteilen lösen, an denen sich herkömmliche Computer langwierig abarbeiten.

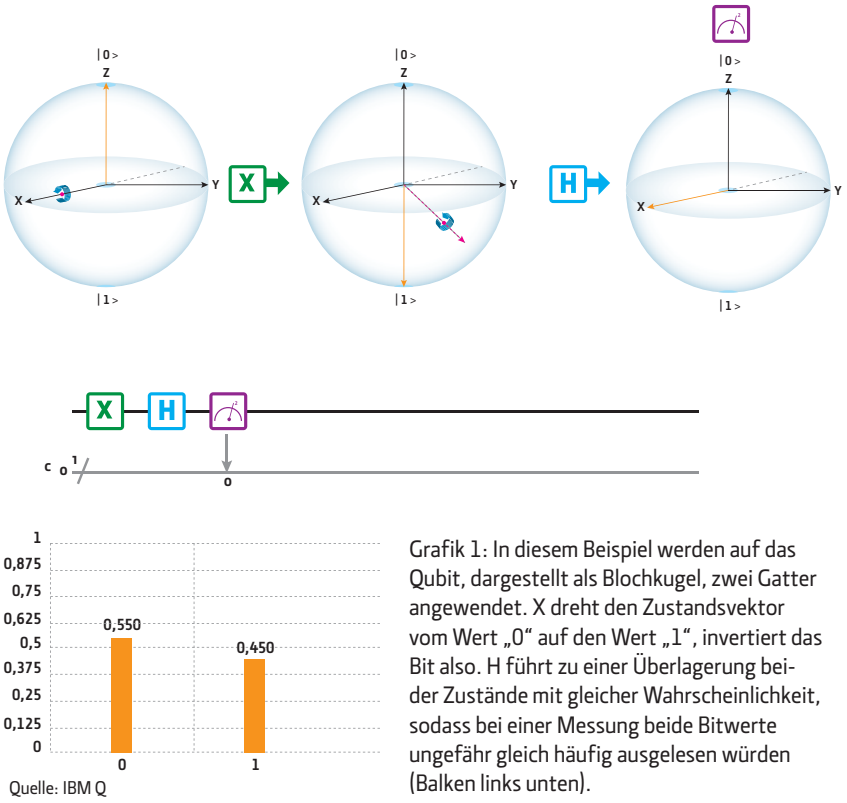
Eines von zwei Beispielen, die Shor in seinem Paper präsentierte, ist die Zerlegung von Zahlen in Primfaktoren. Nehmen wir die 15: Ihre Primfaktoren sind 3 und 5. Nun kann man die 15 noch im Kopf zerlegen. Bei sehr großen Dezimalzahlen wird es jedoch haarig, selbst für einen heutigen Computer. Um eine 232-stellige Zahl zu zerlegen – derzeitiger Rekord –, benötigt er etwa 10^{26} Rechenschritte (10^{26} ist eine Eins mit 26 Nullen, also 100 Quadrillionen). Ein ausreichend großer Quantencomputer könnte dies mit Shors Algorithmus theoretisch auf rund zwölf Millionen Rechenschritte verkürzen.

DIE SOFTWARE

Zwar gibt es noch keine Quantencomputer mit 768 Qubits, die nötig wären, um eine Dezimalzahl mit 232 Stellen darzustellen. Aber schon wenige Jahre nach Shors Paper wurden die ersten Prototypen für ganz einfache Quantenrechner gebaut. Shors Algorithmus setzte erstmals 2001 die Gruppe von Isaac Chuang vom MIT mit sieben Qubits für die Zahl 15 um. 2012 schafften es Igor Markov von der University of Michigan und Mehdi Saeedi von der Technischen Universität Amirkabir im Iran dann mit vier Qubits und einem kürzeren Algorithmus.

Was aber machen die Forscher genau, wenn sie einen Quantenalgorithmus auf Qubits anwenden? Als Beispiel sollen Qubits aus den bereits erwähnten supraleitenden Schleifen dienen. Die Umsetzung eines Algorithmus in mehreren Teilschritten lässt sich nun auf drei Ebenen betrachten: auf einer mathematischen, einer schaltungslogischen und einer physikalischen Ebene.

Mathematisch wird jedes Qubit mit einer sogenannten Blochkugel dargestellt (siehe Grafik 1). In dieser befindet sich sein Zustandsvektor: Zeigt er nach oben, zum „Nordpol", entspricht dies dem Bitwert „0". Der Südpol repräsentiert die „1". Zeigt er irgendwo auf die Kugeloberfläche zwischen den Polen, sind die Zustände „0" und „1" überlagert. Die verschiedenen Rechenschritte des Algorithmus drehen nun den Vektor von einem einzelnen oder auch mehreren Qubits hin und her. Jeder Rechenschritt entspricht dabei einer „unitären Transformation", wie Mathematiker sagen. Auf dieser Ebene ist der Algorithmus also eine Folge quantenmechanischer Berechnungen mit Matrizen aus komplexen Zahlen.



Quelle: IBM Q

Grafik 1: In diesem Beispiel werden auf das Qubit, dargestellt als Blochkugel, zwei Gatter angewendet. X dreht den Zustandsvektor vom Wert „0" auf den Wert „1", invertiert das Bit also. H führt zu einer Überlagerung beider Zustände mit gleicher Wahrscheinlichkeit, sodass bei einer Messung beide Bitwerte ungefähr gleich häufig ausgelesen würden (Balken links unten).

DIE HARDWARE

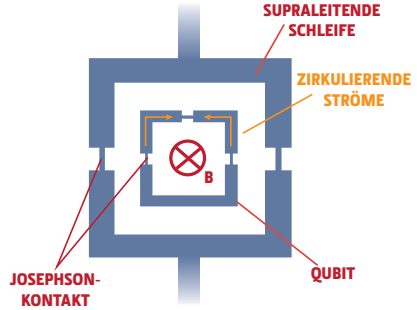
Auf der schaltungslogischen Ebene im Computer ordnet man diesen Rechenschritten sogenannte Quantengatter zu. In der klassischen Computertechnik sind Gatter Schaltkreise, die den Input – hineinfließende Ströme – durch eine Reihe von Transistoren leiten. Ein Beispiel ist das Nicht-Gatter: Es kehrt den Bitwert um. Fließt Strom hinein, also eine „1“, fließt keiner heraus, „0“, und umgekehrt. Für Quantencomputer sind analog verschiedene Standardgatter entwickelt worden, die nur auf ein einzelnes oder auch auf zwei oder drei Qubits wirken. Das Hadamard-Gatter etwa erzeugt die Überlagerung der Bitzustände in einem Qubit. Das X-Gatter dreht den Zustandsvektor in der Blochkugel um 180 Grad von „0“ auf „1“ (siehe Grafik 1). Jedes Gatter entspricht dabei einem Teilschritt auf der mathematischen Ebene. Die Quanteninformatiker können mithilfe der Gatter einen schematischen Schaltplan anlegen (siehe Grafik 4).

Auf der physikalischen Ebene entspricht jede Gatter-Operation wiederum der Wechselwirkung eines Mikrowellensignals mit der supraleitenden Schleife. Die Mikrowellen werden durch einen Wellenleiter in die Schleife geleitet (siehe Grafiken 2 und 3). Als elektromagnetische Wellen haben sie auch ein schwingendes Magnetfeld in sich. Dieses induziert in der Schleife einen Strom. Je nachdem, wie das Feld moduliert ist, fließt der Strom mit dem oder gegen den Uhrzeigersinn, oder es ändert sich die Phase des Stromflusses. Jedem Quantengatter und jeder zugehörigen mathematischen Transformation kann so ein anderes Mikrowellensignal zugeordnet werden. Physikalisch ist der Algorithmus also nichts anderes als eine Abfolge von Mikrowellensignalen, die den Strom in der supraleitenden Schleife manipulieren – so lange, bis alle Rechenschritte durchgeführt sind und der Zustand der Schleife, also des Qubits, abschließend gemessen wird.

Auf die Qubits eines Quantenrechners wird so eine Folge von Rechenschritten angewendet – manche nur auf ein Qubit, manche auf zwei oder drei gleichzeitig. Eine wichtige Voraussetzung ist, dass die Qubits miteinander „verschränkt“ sind, wie es in der Quantenmechanik heißt, also nicht unabhängig voneinander vorliegen (siehe Seite 68). Nur dann lassen sie sich auf die gewünschte Weise manipulieren.

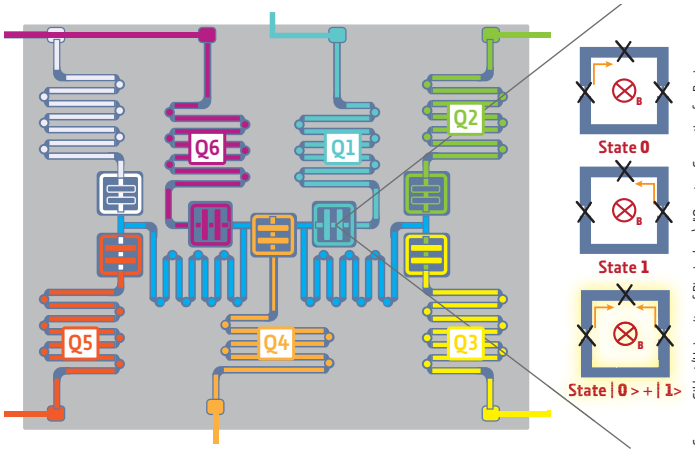
Markov und Saeedi fanden 2012 eine Abfolge von zwei Quantengattern, X und CNOT, mit deren Hilfe sie in vier Qubits eine sogenannte Modulo-Berechnung durchführen konnten (siehe Grafik 4). Dabei wird für die Zahl, deren Primfaktoren man finden möchte – hier: 15 –, mittels Division mit Rest eine Zahl gesucht, aus der sich dann die Primfaktoren direkt berechnen lassen – die sogenannte Periode. Der Shor-Algorithmus liefert diese Periode, nicht die Primfaktoren selbst. Die aus der Periode zu berechnen, kann dann ein herkömmlicher Computer übernehmen.

Bislang ist eine solche Implementierung von Quantenalgorithmen noch ein aufwendiger Vorgang, der weitaus kniffliger ist als hier schematisch beschrieben. „Insofern ist die Einschätzung, dass da etwas ‚Magie‘ dabei ist, nicht so falsch“, sagt der Physiker Frank Wilhelm-Mauch von der Universität Saarbrücken.



Quelle (grafik 2 und 3): Abhinav Kandala et al.: "Hardware-efficient Quantum Optimizer for Small Molecules and Quantum Magnets", arXiv:1704.05018v1 [quant-ph] 17 Apr 2017

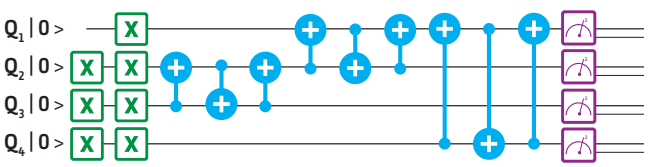
Grafik 2: Als Qubit dient eine supraleitende Schleife mit einem sogenannten Josephson-Kontakt, über den sich der supraleitende Strom manipulieren lässt. Ihr Strom kreist mit dem oder gegen den Uhrzeigersinn. Beide Stromrichtungen überlagern sich während der Berechnung, erst am Ende wird gemessen, welche tatsächlich vorliegt. Da beide Richtungen eine gewisse Wahrscheinlichkeit haben, muss die Messung viele Male wiederholt werden, um die „wahrscheinlichere“ zu finden – also den Ergebnis-Bitwert für dieses Qubit.



Suzanne Gildert (University of Birmingham): "Quantum Computing for Beginners: Building Qubits", Präsentation 28.3.2007

Grafik 3: Eine Anordnung aus sieben supraleitenden Schleifen, die sieben Qubits repräsentieren. Die Wellenleiter, die zu Qubits hinführen, dienen dazu, mittels Mikrowellen eine Gatteroperation durchzuführen, also die Zustände der Qubits gezielt zu ändern. Die beiden blauen Wellenleiter in der Mitte verschränken die Qubits miteinander. Die Ausschnittsvergrößerung (rechts) zeigt Beispiele dafür, welche Zustände die Wellenleiter in die Qubits induzieren können.

Shors Algorithmus mit vier Qubits für die Zahl 15



Quelle: IBM Q

Grafik 4: Die Gatterfolge für den Shor-Algorithmus, wie von Markov und Saeedi implementiert, wird von links nach rechts gelesen. Zunächst werden X-Gatter auf einzelne Qubits, dann CNOT-Gatter (+) jeweils auf zwei Qubits angewendet. Am Ende werden die Zustände und damit die Bitwerte der Qubits gemessen.