

## 15=3×5

### Primfaktorzerlegung mit einem Quantencomputer

An die Primfaktorzerlegung aus dem Mathematikunterricht erinnert man sich für gewöhnlich dunkel und ungerne. Dass 15 das Produkt aus 3 und 5 ist, kann man noch leicht durch Ausprobieren erraten, doch bei grösseren Zahlen wird es selbst mit Computerhilfe immer schwieriger und zeitraubender, sie in ihre «mathematischen Elementarteilchen» zu zerlegen. Auf dieser Tatsache beruht die Sicherheit von einigen der heute verwendeten Verschlüsselungsmethoden. Ein Team von Wissenschaftlern des IBM Forschungszentrums in San Jose (USA) und der Universität Stanford hat nun erstmals einen einfachen Quantencomputer realisiert, der die Zahl 15 in ihre Primfaktoren zerlegen kann. Das Ergebnis an sich ist unspektakulär. Trotzdem lässt das Experiment erahnen, wozu zukünftige Quantencomputer in der Lage sein könnten.

Quantencomputer basieren auf dem Überlagerungsprinzip der Quantenmechanik. Während herkömmliche Computer mit Bits rechnen, die nur die Werte 0 und 1 annehmen können, sind in der Quantenwelt auch die «Grautöne» zwischen diesen beiden Werten erlaubt. So können die Spins von Atomen in einem Magnetfeld nicht nur nach oben oder unten zeigen (was die Werte 0 oder 1 darstellt); quantenmechanisch sind auch Überlagerungen von «oben» und «unten» möglich. Ein Quantencomputer nutzt die Grautöne solcher «Quanten-Bits», um bestimmte Aufgaben unvergleichlich schnell zu erledigen.

Bereits 1994 entwickelte der Mathematiker Peter Shor einen Algorithmus für Quantencomputer, der eine rasche Zerlegung von grossen Zahlen in ihre Primfaktoren versprach. Der nach seinem Erfinder benannte Algorithmus führt dazu, dass die Rechenzeit nicht mehr exponentiell mit der Anzahl der Stellen der zu faktorisierenden Zahl anwächst, wie das bei herkömmlichen Verfahren der Fall ist, sondern deutlich langsamer. So kommt es, dass klassische Computer für die Zerlegung einer Zahl mit Hunderten von Stellen

einige Milliarden Jahre brauchten, ein Quantencomputer dagegen nur wenige Minuten.

Die Ausführung dieses Algorithmus scheiterte bisher daran, dass die in den letzten Jahren realisierten Quantencomputer zu wenige Quanten-Bits besaßen. Auch der nun von der Forschungsgruppe um Isaac Chuang vorgestellte Quantencomputer hat bisher nur ein sehr einfaches Problem lösen können: die Zerlegung der Zahl 15 in ihre Primfaktoren. Dazu mussten die Forscher zunächst sieben miteinander gekoppelte Quanten-Bits erschaffen, wozu sie eigens ein komplexes Molekül mit Kohlenstoff- und Fluoratomen synthetisierten. Mit Hilfe der Kernspinresonanz konnten die einzelnen atomaren Spins angesteuert und so der Algorithmus Schritt für Schritt ausgeführt werden.

Das (korrekte) Endergebnis  $15=3\times 5$  war natürlich keine Überraschung, zeigte aber, dass die von Shor vorgeschlagene Rechenmethode in der Praxis tatsächlich umsetzbar ist. Vor allem das Problem der sogenannten Dekohärenz haben die Forscher nun zu ihrer Zufriedenheit im Griff. Die Dekohärenz führt dazu, dass die für das Funktionieren des Computers so wichtigen quantenmechanischen Überlagerungszustände nach und nach durch äussere Einflüsse zerstört werden.

Ein echter Zeitvorteil gegenüber herkömmlichen Computern ist erst bei der Zerlegung von grossen Zahlen zu erwarten. Hierzu müsste die Zahl der Quanten-Bits freilich auf einige Tausend erhöht werden, was mit den gegenwärtigen Methoden noch nicht möglich ist. Der positive Ausgang des Experiments stimmt die Forscher jedoch zuversichtlich, dass Quantencomputer eines Tages tatsächlich nützliche Rechnungen in Rekordzeit erledigen können.

*Oliver Morsch*

Quelle: Nature 414, 883–887 (2001).