Shor und Grover: Was Quantenalgorithmen können

QUANTENTECHNOLOGIE · QUANTENCOMPUTER

Über Quantencomputer liest man oft, sie würden „alles“ schneller machen, vom Wetterbericht bis zur Online-Suche. Das stimmt nicht. Ein Quantencomputer ist kein schnellerer Computer, sondern ein anderer, und er ist nur dann überlegen, wenn jemand einen Rechenweg gefunden hat, der seine Quanteneigenschaften geschickt ausnutzt. Solche Rechenwege heißen Quantenalgorithmen, und es gibt erstaunlich wenige wirklich gute davon.

Zwei sind besonders berühmt, benannt nach ihren Erfindern Peter Shor und Lov Grover. Der eine könnte die Verschlüsselung des Internets brechen, der andere beschleunigt die Suche in ungeordneten Daten. Wir erklären, wie sie funktionieren, was sie können und was nicht, und wie weit man heute von ihrer praktischen Nutzung entfernt ist.

Warum man überhaupt besondere Algorithmen braucht

Ein Qubit kann sich in einer Überlagerung von 0 und 1 befinden, und mehrere Qubits zusammen werden durch sehr viele Zahlen gleichzeitig beschrieben. Das klingt, als könne ein Quantencomputer alle Möglichkeiten auf einmal durchprobieren. Das Problem: Am Ende misst man, und die Messung liefert nur ein einziges Ergebnis, zufällig ausgewählt nach den Wahrscheinlichkeiten des Zustands. Lässt man den Quantencomputer einfach „alles gleichzeitig“ rechnen, bekommt man eine zufällige Antwort, und die ist wertlos.

Ein guter Quantenalgorithmus muss deshalb die Wellennatur der Quantenzustände ausnutzen. Die Wege, die zu falschen Antworten führen, müssen sich gegenseitig auslöschen, die zur richtigen Antwort müssen sich verstärken, so wie Wellen im Wasser sich überlagern. Das gelingt nur bei Problemen mit einer besonderen inneren Struktur. Die Idee, dass Quantenrechner so etwas können, geht übrigens auf Richard Feynman zurück, der 1982 vorschlug, Quantensysteme mit Quantensystemen zu simulieren, weil klassische Computer daran scheitern [1].

Grover: die Nadel im Heuhaufen

Stellen Sie sich ein Telefonbuch mit einer Million Einträgen vor, aber verkehrt herum: Sie haben eine Telefonnummer und suchen den zugehörigen Namen. Weil das Buch nach Namen sortiert ist, hilft Ihnen die Ordnung nicht. Sie müssen Eintrag für Eintrag prüfen, im Durchschnitt eine halbe Million Mal.

Lov Grover zeigte Mitte der Neunzigerjahre, dass ein Quantencomputer das mit deutlich weniger Schritten schafft [2]. Er bringt alle Einträge in eine gleichmäßige Überlagerung, markiert den gesuchten durch ein umgedrehtes Vorzeichen und verstärkt ihn dann schrittweise, bis er bei der Messung fast sicher herauskommt. Die Zahl der nötigen Schritte wächst nur mit der Wurzel aus der Zahl der Einträge:

$$k_{\text{Grover}} \approx \frac{\pi}{4}\sqrt{N} \tag{1}$$

Einträge N	klassisch, im Mittel	Grover, etwa
10^3	500	25
10^6	500.000	785
10^9	500.000.000	24.836
10^{12}	500.000.000.000	785.398

Eigene Berechnung nach Gleichung (1), gerundet.

Das ist eine echte, beweisbare Beschleunigung, aber eine bescheidene. Aus einer halben Million Schritten werden knapp 800. Für viele praktische Probleme reicht das nicht, um die Nachteile eines Quantencomputers aufzuwiegen, der jeden einzelnen Schritt viel langsamer und fehleranfälliger ausführt als ein Laptop. Und man weiß, dass es nicht besser geht. Schon 1997 bewiesen Charles Bennett und Kollegen, dass kein Quantencomputer eine ungeordnete Suche wesentlich schneller als mit der Wurzel aus N Schritten schaffen kann [3]. Die Hoffnung, ein Quantencomputer könne die schwersten Rechenprobleme einfach durch Ausprobieren aller Möglichkeiten knacken, ist damit vom Tisch.

Shor: Primzahlen und Geheimnisse

Ganz anders liegt es bei Peter Shors Algorithmus von 1994. Er zerlegt große Zahlen in ihre Primfaktoren, und zwar exponentiell schneller als jedes bekannte klassische Verfahren [4]. Das klingt nach einer mathematischen Spielerei, ist aber von enormer praktischer Bedeutung. Das weit verbreitete Verschlüsselungsverfahren RSA beruht darauf, dass es praktisch unmöglich ist, eine Zahl mit über 600 Dezimalstellen in ihre zwei Primfaktoren zu zerlegen. Ein ausreichend großer Quantencomputer könnte das.

Der Trick ist eine Umformulierung. Shor verwandelt die Frage nach den Faktoren in die Frage nach der Periode einer Zahlenfolge, also danach, nach wie vielen Schritten sich ein Muster wiederholt. Periodische Muster aufzuspüren ist genau das, worin Wellen gut sind. Der Quantencomputer erzeugt eine Überlagerung, in der die Periode als Rhythmus

versteckt ist, und eine sogenannte Quanten-Fourier-Transformation macht diesen Rhythmus sichtbar, so wie ein Prisma die Farben im Licht trennt. Aus der Periode lassen sich die Faktoren dann mit gewöhnlicher Mathematik ausrechnen. Shors Algorithmus bricht übrigens auch die verbreitete Verschlüsselung mit elliptischen Kurven, denn sie beruht auf einem verwandten Problem, dem diskreten Logarithmus, das er in derselben Arbeit gelöst hat.

Wie weit ist man?

Die erste Vorführung gelang 2001 in einem Labor von IBM: Ein Quantencomputer mit sieben Qubits zerlegte die Zahl 15 in 3 mal 5 [5]. Größere Zahlen, die echte Verschlüsselung bedrohen könnten, sind seither nicht ehrlich mit Shors Algorithmus zerlegt worden. Der Grund ist, dass man dafür sehr viele fehlerkorrigierte Qubits braucht, und die gibt es noch nicht.

Wie viele genau, haben Forscher von Google mehrfach abgeschätzt. 2021 kamen Craig Gidney und Martin Ekerå auf 20 Millionen fehleranfällige physikalische Qubits, die eine 2048-Bit-RSA-Zahl in acht Stunden knacken könnten [6]. Im Mai 2025 legte Gidney eine neue Schätzung vor: weniger als eine Million Qubits, dafür eine Rechenzeit von unter einer Woche, unter der Annahme einer Fehlerrate von 0,1 Prozent pro Rechenschritt [7]. Diese Arbeit ist ein Preprint, also noch nicht begutachtet, und die Annahmen sind anspruchsvoll. Die heutigen Maschinen haben einige Hundert bis einige Tausend Qubits. Der Abstand ist also noch groß, aber er schrumpft von zwei Seiten, durch bessere Hardware und durch bessere Algorithmen.

Deshalb stellen Behörden und Unternehmen schon jetzt auf neue Verschlüsselungsverfahren um, die auch einem Quantencomputer standhalten. Das hat einen handfesten Grund: Wer heute verschlüsselte Daten abfängt und speichert, könnte sie in einigen Jahren mit einem Quantencomputer entschlüsseln. Wie diese Umstellung funktioniert, erklärt unser Artikel über Post-Quanten-Kryptographie.

Was sonst noch geht

Neben Shor und Grover gibt es weitere Quantenalgorithmen, und die vielleicht wichtigste Anwendung ist die, an die Feynman zuerst gedacht hatte: die Simulation von Molekülen und Materialien. Das Verhalten vieler Elektronen in einem Molekül ist selbst ein Quantenproblem, und klassische Computer müssen dafür mit groben Näherungen arbeiten. Ein Quantencomputer könnte es direkt nachbilden, etwa um bessere Katalysatoren, Batteriematerialien oder Medikamente zu entwerfen. Für Optimierungsaufgaben aus Logistik und Finanzwelt gibt es ebenfalls Ansätze, ob sie dort einen echten Vorteil bringen, ist allerdings umstritten.

Ehrlich betrachtet ist die Liste der Probleme, bei denen ein Quantencomputer nachweislich viel schneller ist, kurz. Das ist kein Makel, sondern zeigt, wie besonders diese Maschinen

sind. Sie werden den klassischen Computer nicht ersetzen, sondern ihn ergänzen, für genau die Aufgaben, bei denen die Quantenwelt selbst den Schlüssel liefert. Wie die Maschinen gebaut werden, erklären die Artikel über den Quantencomputer und über Quantencomputer in Deutschland.

Zum Weiterlesen

Quantum Computing verstehen

Matthias Homeister · Springer Vieweg, 2022 · ISBN 978-3-658-36433-5

Erklärt Grovers und Shors Algorithmus Schritt für Schritt mit Schulmathematik. Ideal, um die Ideen wirklich nachzuvollziehen.

Bei Amazon ansehen*

Quantum Computation and Quantum Information

Michael A. Nielsen, Isaac L. Chuang · Cambridge University Press, 2010 (englisch) · ISBN 978-1-107-00217-3

Das Standardwerk mit allen Beweisen, für Studierende und alle, die tief einsteigen wollen.

Bei Amazon ansehen*

* Werbelink: Kaufen Sie über diesen Link, erhalten wir von Amazon eine kleine Provision, am Preis ändert sich für Sie nichts. Mehr Empfehlungen auf unserer Seite Bücher zur Quantenphysik.

Quellen

1. R. P. Feynman: *Simulating physics with computers.* In: International Journal of Theoretical Physics 21 (1982), S. 467–488, doi:10.1007/BF02650179.
2. L. K. Grover: *Quantum Mechanics Helps in Searching for a Needle in a Haystack.* In: Physical Review Letters 79 (1997), S. 325–328, doi:10.1103/PhysRevLett.79.325.
3. C. H. Bennett, E. Bernstein, G. Brassard, U. Vazirani: *Strengths and Weaknesses of Quantum Computing.* In: SIAM Journal on Computing 26 (1997), S. 1510–1523, doi:10.1137/S0097539796300933.
4. P. W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* In: SIAM Journal on Computing 26 (1997), S. 1484–1509, doi:10.1137/S0097539795293172.

5. L. M. K. Vandersypen u. a.: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.* In: Nature 414 (2001), S. 883–887, doi:10.1038/414883a.
6. C. Gidney, M. Ekerå: *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.* In: Quantum 5 (2021), 433, doi:10.22331/q-2021-04-15-433.
7. C. Gidney: *How to factor 2048 bit RSA integers with less than a million noisy qubits.* Preprint, Mai 2025. arXiv:2505.15917.

Zitiervorschlag

```
quanten.de: Shor und Grover: Was Quantenalgorithmen können.
Stand: Oktober 2026. URL:
https://quanten.de/quantenalgorithmen.html (PDF:
https://quanten.de/pdf/quantenalgorithmen.pdf)
```

Texte und Abbildungen © 2026 quanten.de. Nutzung mit Quellenangabe und Link gern, kommerzielle Nutzung nach Absprache: info@quanten.de

Weiterlesen: Was ist ein Qubit? · Quantencomputer · Post-Quanten-Kryptographie · Quantenkryptographie

---