

# KEPLER TRIBUNE

Wissen in Gesellschaft

JKU / Kepler Tribune / Bitte ein Qubit

## Bitte ein Qubit

Quantencomputer werden die Welt revolutionieren. Physiker\*innen tüfteln an der Maschine, Anwender\*innen knobeln, was sie berechnen wollen – und der JKU Informatiker Robert Wille arbeitet daran, beide Welten zu vereinen.



Quantencomputer wurden bisher vor allem in Forschungslaboren verwendet. Mit dem IBM Quantum System One wurde erstmalig eine kommerzielle Nutzung möglich.

Am 14. Februar 1946 präsentierte die US-Armee der Welt einen elektronischen Supercomputer. Der ENIAC wog 30 Tonnen und seine Rechenleistung bestand darin, zehnstellige Zahlen in Millisekunden multiplizieren und dividieren zu können. Eine Berechnung, die heute kein Smartphone mehr heiß laufen lässt.

Ein Dreivierteljahrhundert später, am 23. Oktober 2019, präsentierte Google der Welt einen neuen Rechner. Der Sycamore-Chip löste eine rein akademische Aufgabe in 200 Sekunden, für die – so Google – aktuelle Supercomputer 10.000 Jahre benötigen würden. Der Begriff Quantenüberlegenheit machte die Runde. Das Staunen war groß, die PR natürlich auch, und der Widerspruch aus der wissenschaftlichen Community ließ nicht lange auf sich warten; konventionelle Rechner seien gar nicht so langsam, hieß es. Das Experiment hatte keinen praktischen Nutzen. Aber wie man es auch dreht und wendet, es hat aufgezeigt: das revolutionäre Potenzial eines künftigen echten Quantencomputers.

Einen voll funktionsfähigen Quantencomputer gibt es bis heute nicht. Forscher\*innen gehen davon aus, dass es noch mindestens zehn Jahre dauern wird, bis ein Quantencomputer gebaut wird, der das ganze Potenzial dieser neuen Technologie ausschöpfen kann. Aber dafür würde er dann die Welt revolutionieren – er wäre die technologische Innovation des 21. Jahrhunderts. Würde ein neues Computerzeitalter einleiten. Spezialberechnungen wären in Sekunden statt Jahren möglich. Gängige Internet-Verschlüsselungen schnellstens knackbar. E-Mails, Banküberweisungen, Militärkommunikation – all das wäre nicht mehr sicher.

Wer diesen ersten voll funktionstüchtigen Quantencomputer baut, besitzt den Generalschlüssel zum heutigen Internet und zu seinen Geheimnissen. Weltweit findet ein Wettrennen um die Technologie statt. Tech-Firmen und Staaten wollen vorne mit dabei sein. Die EU budgetierte für den Zeitraum 2018 bis 2028 rund eine Milliarde Euro für Quantentechnologie; Deutschland verkündete erst 2020 im Zuge des Corona-Konjunkturpakets, weitere zwei Milliarden investieren zu wollen; die USA zogen nach. Und China denkt überhaupt groß: Ein zweistelliger Milliardenbetrag fließt in ein neues Labor, und chinesische Forscher\*innen wollen die Leistung von Googles Chip schon längst in den Schatten gestellt haben. Doch Quantentechnologie verspricht mehr als nur Geschwindigkeit und den Einblick in die Daten anderer – China baut an einem Netzwerk, das quantenverschlüsselt und somit absolut abhörsicher ist.

Quanten – das ist der neue Wunderbegriff zukünftiger Technologien. Was hat es damit auf sich? Worauf baut die Hoffnung? Grundlagen liefert die Quantenphysik. Wer sich damit beschäftigt, stolpert über Begriffe wie Superposition und liest von „spukhafter Fernwirkung“, ein Zitat Albert Einsteins, weil selbst ihm die Quantentheorie Kopfzerbrechen bereitete, ja, er gar nicht daran glauben wollte. Es geht um sogenannte verschränkte Teilchen, die sich selbst nach einer Trennung weiterhin so verhalten, als wären sie verbunden. Und das selbst über große Distanzen hinweg. Linz– Peking etwa. Wer sich also mit Quantenphysik beschäftigt, dringt in eine Materie vor, die verrückt erscheint, weil sie nicht mit unserer Alltagserfahrung zusammengeht. Doch unsere Alltagserfahrung folgt schlicht den Regeln der „klassischen Physik“, die Quantenphysik hat eben ihre eigenen.

Diese Regeln macht sich die Idee des Quantencomputers zunutze. Klassische Computer rechnen mit 0 und 1. Quantencomputer hingegen rechnen mit Quantenbits, kurz Qubits. Diese Qubits können 0 und 1 gleichzeitig sein, genauer: Sie können unendlich viele Werte gleichzeitig annehmen. Die sogenannte Superposition. Sie erlaubt paralleles Rechnen. Theoretisch.

Praktisch scheitert es noch daran, Qubits zu verwirklichen. Die Dinger sind einfach noch zu flüchtig – sie überleben nicht sehr lange. Und sie sind unzuverlässig. Je mehr Qubits man einem Rechner hinzufügt, desto fehleranfälliger wird er. Eine vergleichbare Herausforderung gab es bereits in den 1940er Jahren: Der ENIAC rechnete unzuverlässig, wenn nur eine seiner Tausenden Elektronenröhren ausfiel. Den heutigen Physiker\*innen geht es darum, Qubits besser zu beherrschen und den Quantencomputer zu konstruieren; experimentelle Maschinen wie die von Google benötigen bislang ein Vakuum, das auf knapp über den absoluten Temperatur-Nullpunkt von minus 273 Grad Celsius gekühlt ist. Doch was passiert, wenn diese Fragen gelöst sind und die Maschine kommt? Damit auch Fachfremde den Rechner benutzen können, benötigt es Werkzeuge. „Sie müssen schließlich nicht Physik studiert haben, um heute einen klassischen Computer zu bedienen“, sagt Robert Wille, der daran arbeitet, dass es auch bei Quantencomputern so wird.

Robert Wille ist Informatiker, er leitet das „Institute for Integrated Circuits“ an der Johannes Kepler Universität Linz, ist Mitbegründer des „LIT Secure and Correct Systems Lab“ der JKU und wissenschaftlicher Geschäftsführer des Software Competence Center Hagenberg. Für seine Forschung wurde er kürzlich mit dem Consolidator Grant des Europäischen Forschungsrats (European Research Council), einer der renommiertesten Wissenschaftsauszeichnungen Europas, ausgezeichnet. Wille und sein Team simulieren speziell entwickelte Quantenalgorithmien auf konventionellen Rechnern, was so viel heißt wie: Tut der Algorithmus, was Forscherin und Forscher im Sinn hatten? Und inwieweit ist die Simulation überhaupt möglich? Kann ich denn ein Programm auf echten Quantenrechnern ausführen? Das sind die Fragen, mit denen er sich beschäftigt. Wille sagt: „Wir laufen Gefahr, dass wir am Ende hochleistungsfähige Quantencomputer entwickeln, deren volles Potenzial wir aber nicht perfekt ausnutzen können.“

Als Informatiker steht Wille zwischen Physiker\*innen, die den neuen Rechner bauen, und jenen Forschenden, die ihn mit speziellen Aufgaben füttern wollen, um eine bestimmte Frage zu lösen: Was macht der Klimawandel mit einer Region in 30 Jahren? Welche Wirkstoffe sind für ein bestimmtes Arzneimittel sinnvoll? In welche Primzahlen kann ich eine tausendstellige Zahl zerlegen, um eine Verschlüsselung zu knacken?

Doch oft testen Forscher\*innen falsche Modelle, begeben sich in Sackgassen. „Das hält enorm auf“, sagt Wille. Ein Grant des Europäischen Forschungsrats erlaubt es ihm und seinem Team künftig, interdisziplinär zu arbeiten. „Wir können uns dann ein halbes Jahr neben die Anwender\*innen setzen, um zu verstehen, was sie genau vorhaben“, sagt Wille. „Und ein halbes Jahr neben die Physiker\*innen, um deren Probleme zu verstehen.“

Die Funktionsweise eines Quantenrechners ist perfekt dafür geeignet, die sprichwörtliche Nadel im Heuhaufen zu finden. Klassische Computer müssten jeden Grashalm einzeln umdrehen, „bei 50 Trillionen möglichen validen Lösungen“ eine fast unmögliche Aufgabe, so Wille. Quantenrechner hingegen könnten sich durchs Heu wühlen. Sie sind exzellent für Optimierungen und Simulationen, jene Aufgaben, bei denen es darum geht, zig Optionen zu prüfen. Dass sie klassische Computer in Zukunft ablösen, ist daher unwahrscheinlich. Der Quantencomputer wird kein Generalist sein. Sondern ein kälteliebender Experte für Spezialaufgaben – ein faszinierend begabter und einer, um den das globale Wettrennen längst begonnen hat.

[← ZURÜCK ZUR ÜBERSICHT](#)

NEWS 12.03.2021

Wissen

ARTIKEL TEILEN

Erschienen in [Ausgabe 1/2021](#)