Was Quantencomputer können - und was nicht: Quantum Brilliance-Europachef Dr. Mark Mattingley-Scott trennt Mythen von Fakten

Experte für Quantencomputer trennt Mythen von Fakten

STUTTGART, 12. November 2025 --- Der diesjährige Physiknobelpreis hat Quantencomputer noch stärker in die Öffentlichkeit gerückt. Rund um die Funktionsweise und das Potenzial der komplexen Technologie kursieren jedoch zahlreiche Mythen. Dr. Mark Mattingley-Scott, Europachef von Quantum Brilliance, einem deutsch-australischen Hersteller von Quantenhardware, klärt auf.

Mythos 1: Quantencomputer sind klassischen Computern überlegen
Das ist als pauschale Aussage nicht korrekt, entscheidend ist das Einsatzgebiet. Auf einem Quantencomputer lässt sich zum Beispiel gängige Office-Software nicht sinnvoll betreiben. Geht es hingegen um die Lösung von Problemen durch die Berechnung komplexer Wahrscheinlichkeitsverteilungen, haben Quantencomputer massive Vorteile gegenüber klassischen binären Systemen.

Mythos 2: Quantencomputer können alle Lösungen eines Problems parallel berechnen und gleichzeitig liefern
Das ist nicht zu 100 Prozent korrekt, denn ein Quantencomputer erschafft keine mysteriöse neue Dimension, in der alles parallel abläuft. Allerdings sind Quantenrechner sehr effizient darin, komplexe Wahrscheinlichkeiten zu berechnen. Denn sie nutzen Superposition und können so viele mögliche Zustände gleichzeitig darstellen. Das bedeutet aber nicht, dass sie alle Lösungen parallel "durchrechnen" und am Ende automatisch alle Ergebnisse ausgeben. Beim Messen kollabiert der Quantenzustand in genau eine Lösung. Der Vorteil entsteht erst durch Quantenalgorithmen, die Interferenz gezielt einsetzen, um die Wahrscheinlichkeit der richtigen oder nützlichen Lösung zu verstärken und andere zu unterdrücken.

Mythos 3: Qubits können unbegrenzt viele Informationen speichern
Qubits "speichern" keine Informationen im herkömmlichen Sinne. Was mit ihrer Anzahl jedoch exponentiell wächst, ist der Zustandsraum, also der Raum aller möglichen Überlagerungen (Superpositionen) und Verschränkungen. So spannen beispielsweise 32 Qubits einen Zustandsraum von 232 Dimensionen auf, was etwa 4,3 Milliarden Basiszuständen entspricht. Das bedeutet aber nicht, dass all diese Informationen gleichzeitig gespeichert oder ausgelesen werden können - beim Messen erhält man immer nur ein Ergebnis mit einer Länge von 32 Bits.

Mythos 4: Quantencomputer benötigen energiefressende Kryo-Kühlsysteme, die den Stromverbrauch exorbitant in die Höhe treiben
Der Energiebedarf von Quantencomputern hängt von den eingesetzten Qubits ab. Quantenprozessoren, die Stickstoff-Fehlstellen-Zentren in Diamantsubstraten (NV-Zentren) als Qubits nutzen, brauchen keine energieintensive Kühlung. Denn dank des stabilen Gitters aus Kohlenstoffatomen bleiben die nötigen Quanteneigenschaften auch bei Zimmertemperatur erhalten. Supraleitende Qubits hingegen müssen mit einem Kryo-Kühlsystem bis nahe dem absoluten Nullpunkt gekühlt werden, was große Mengen an Strom verbraucht.

Mythos 5: Je mehr Qubits ein Quantenrechner hat, desto leistungsfähiger ist er
Die Anzahl der Qubits ist eine der wichtigsten Kennzahlen im Quantencomputing. Mit jedem Qubit verdoppelt sich der Zustandsraum, wächst also exponentiell. Das heißt: Mit einem Qubit lassen sich zwei Zustände darstellen, mit zwei Qubits vier Zustände, mit 12 Qubits 212, also 4096 Zustände und mit "nur" 32 Qubits schon knapp 4,3 Milliarden Zustände. Ein wichtiges Detail in diesem Zusammenhang ist aber: Es geht hier immer um Qubits, die miteinander verknüpft sind und die Rechenleistung durch "Zusammenarbeit" kombinieren. Damit diese Zusammenarbeit funktioniert, spielen verschiedene Parameter wie Kohärenzzeit (wie lange "arbeiten" die verschiedenen Qubits zusammen?) und Fidelität (wie präzise sind die Operationen auf dem Quantencomputer?) eine zentrale Rolle.

Mythos 6: Quantencomputer werden klassische Systeme ablösen
Quantencomputer werden herkömmliche Systeme nie vollständig ablösen. Klassische Rechenoperationen wie die Multiplikation großer Zahlen funktionieren auf binären Rechnern sogar wesentlich besser. Geht es aber beispielsweise um eine Primfaktorzerlegung großer Zahlen, sind wiederum Quantenrechner viel effizienter - wenn sie beispielsweise den Shor-Algorithmus nutzen. Das wahrscheinlichste Szenario sind hybride Systeme, bei denen Quantencomputer als Beschleuniger eingesetzt werden, um klassische Rechner bei bestimmten Berechnungen zu unterstützen.

Mythos 7: Quantencomputer machen gängige Verschlüsselungsverfahren bald obsolet
Abhängig von der Definition von "bald" ist das möglich. Sollte es in den nächsten fünf Jahren keinen fundamentalen Durchbruch geben, dann wird das noch einige Jahrzehnte dauern. Umso wichtiger wird die Weiterentwicklung von Post-Quanten-Kryptographie (PQC). Deren kryptographischen Bausteine und Verfahren (Primitives) können, im Gegensatz zu den meisten aktuell verwendeten asymmetrischen Kryptosystemen, auch mit Quantencomputern nicht entschlüsselt werden. Entsprechende PQC-Key-Exchange-Verfahren gibt es bereits, ebenso wie einige gesetzliche Initiativen. So empfiehlt die EU ihren Mitgliedsstaaten in einem koordinierten Implementierungsfahrplan die Absicherung kritischer Infrastruktur bis spätestens Ende 2030.

Pressekontakt

Dr. Haffa & Partner GmbH

Herr Axel Schreiber
Karlstraße 42
80333 München

haffapartner.de
postbox@haffapartner.de

Firmenkontakt

Quantum Brilliance GmbH

Herr Dr. Mark Mattingley-Scott
Colorado Tower Industriestraße 4
70565 Stuttgart

https://quantumbrilliance.com

mark.mattingley-scott@quantum-brilliance.com

Quantum Brilliance wurde 2019 gegründet und ist ein wagniskapitalfinanzierter deutsch-australischer Hersteller von Quantencomputing-Hardware. Das Unternehmen bietet Quantenbeschleuniger aus synthetischen Diamanten sowie ein Set aus Softwaretools und Applikationen. Die Vision ist es, einen breiten Einsatz von Quantenbeschleunigern zu ermöglichen - um die Industrie in die Lage zu versetzen, Edge-Computing-Anwendungen und Supercomputer der nächsten Generation zu nutzen. Quantum Brilliance verfügt über Partnerschaften in Nordamerika, Europa sowie Asien-Pazifik und arbeitet mit Regierungen, Supercomputing-Centern, Forschungseinrichtungen und führenden Köpfen aus der Industrie zusammen.

Anlage: Bild