

Der Kampf um den Quantencomputer – Teil 1

Das Rennen um das Superhirn läuft

Gegenwärtig kämpfen nicht nur die Großmächte USA und China um die Vorherrschaft bei den Quantencomputern. Auch die Europäische Union und einzelne Nationalstaaten unternehmen enorme Anstrengungen, der neuen Technologie zum Durchbruch zu verhelfen.

Ende Oktober 2019 hielt die Wissenschaftswelt den Atem an. Die US-Raumfahrtbehörde NASA hatte versehentlich einen Artikel des Wissenschaftsmagazins Nature auf ihre Webseite gestellt, in dem stand, dass der Quantenchip Sycamore von Google „in 200 Sekunden eine Berechnung durchführen könne, für die der schnellste Supercomputer der Welt 10.000 Jahre gebraucht hätte“. Spätestens seit dieser Meldung hat eine intensive Diskussion darüber eingesetzt, dass unsere Welt offensichtlich nicht aus Nullen und Einsen, sondern aus Quanten besteht und auch bei dem Stichwort Quantencomputer gehen die Meinungen weit auseinander. Einige sehen darin eine revolutionäre Veränderung der Rechnerwelt, die nahezu alle Lebensbereiche von der Wirtschaft über Naturwissenschaft bis hin zu Militärpolitik umfasst, andere zweifeln, ob diese Technik tatsächlich jemals zu einem breiten Einsatz kommen wird.

Fakt ist, dass funktionsfähige Quantencomputer jedes Produkt, jeden Prozess und jede Dienstleistung auf diesem Planeten grundlegend verändern werden. Der Wettbewerbsvorteil zwischen einem Unternehmen mit und ohne Quantencomputer ist fundamental. Eine Volkswirtschaft ohne Zugang zu Quantencomputern wird keine Rolle mehr in dieser Welt spielen. Dies gilt übrigens auch für gesellschaftspolitische und militärische Fragestellungen, da Quantencomputer das Feld der Künstlichen Intelligenz (KI) fundamental verändern werden. Diese zukünftige Entwicklung wirft bereits heute ihre Schatten voraus. So wurden von der US-Regierung schon Exportkontrollen für wichtige Schlüsselkomponenten für Europa in Kraft gesetzt.

Die Quantenwelt

Die Idee der Quantentechnologie besteht darin, dass wir die Welt besser verstehen, wenn wir uns der Quantensysteme bedienen. Das ist auch nicht weiter verwunderlich, denn auf der Ebene der Atome und ihrer Bestandteile, die sich in einer Größenordnung von 10¹⁵ abspielt, gelten die Regeln der Quantenmechanik. Der Inhaber des Lehrstuhls für Theoretische Physik an der Friedrich-Alexander-Universität, Erlangen-Nürnberg, Prof. Michael J. Hartmann, der an der Entwicklung des Google-Computers mitgewirkt hat und Co-Autor des erwähnten Nature-Artikels ist, hat die Unterscheidung zwischen Quantencomputern und herkömmlichen Rechnern so definiert, dass im Gegensatz zu den klassischen Computern, die die Informationen als Bitfolgen von Nullen und Einsen speichern, ein Quantencomputer diese in Quantenzuständen speichert. Die elementare Verarbeitungseinheit, das Qubit oder Qubit kann eben nicht nur Werte von Null oder Eins annehmen, sondern

sich für eine bestimmte Zeitspanne, die so genannte Kohärenzzeit, gleichzeitig in beiden Zuständen befinden. Der Quantencomputer ist dem normalen überlegen, da die Rechenleistung sich mit jedem Qubit verdoppelt und mit dieser exponentiellen Zunahme kann ein Quantencomputer mit 300 miteinander verschränkten Qubits mehr Zustände annehmen, als es Atome im Universum gibt.

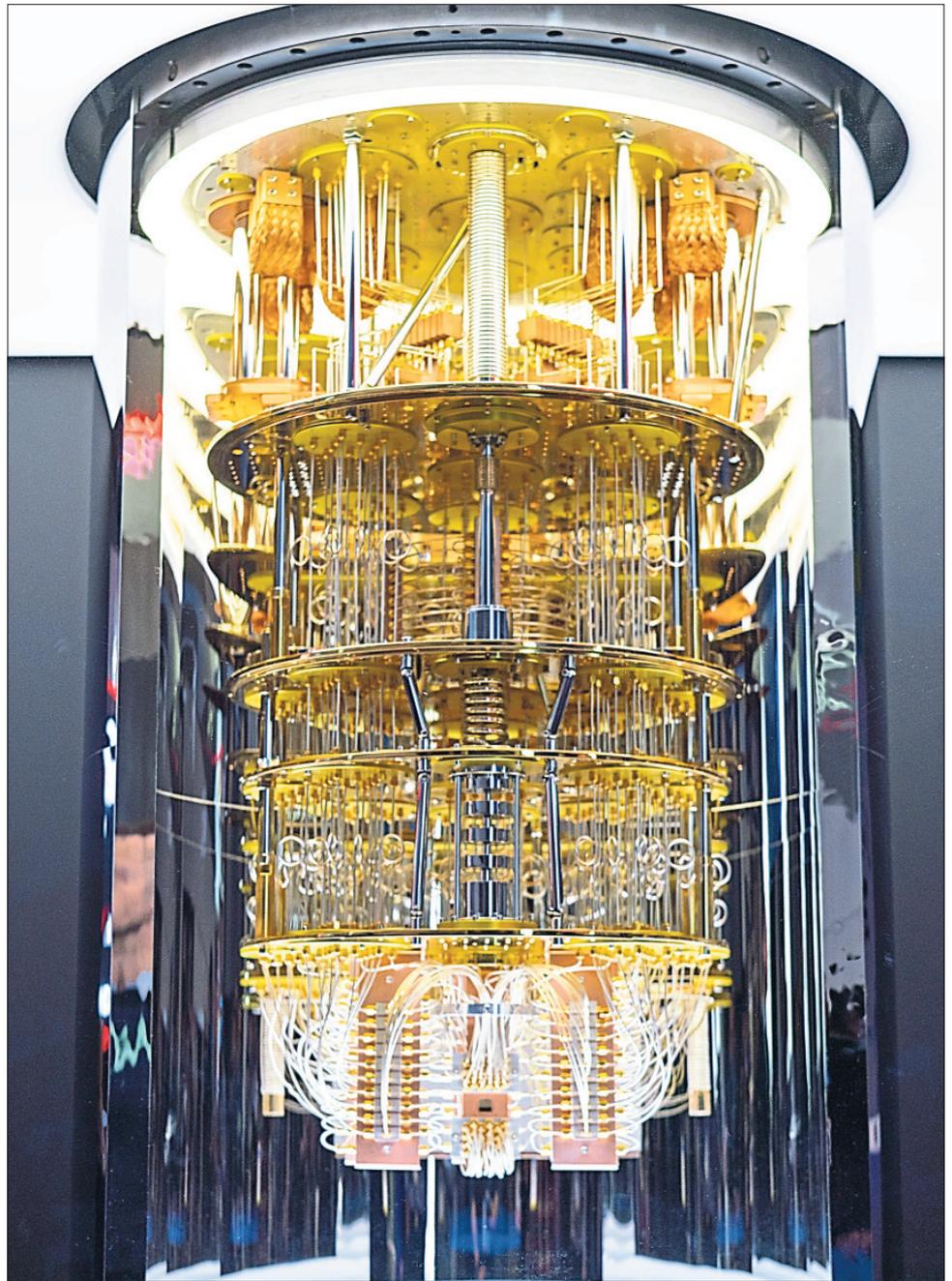
Eine mächtige Symbiose

Es existieren heute sehr viele wissenschaftliche, aber auch praktische Herausforderungen, die mit der Kapazität gegenwärtig existierender Supercomputer kaum oder überhaupt nicht zu lösen sind. Dazu gehört beispielsweise die Analyse und vor allem die Prognose von Finanzmärkten, aber auch die Optimierung von Fahrtrouten und Verkehrssystemen mit beliebig vielen Teilnehmern. Ähnliches gilt für Verschlüsselungstechnologien, für die enorme Datenmengen und ein gigantischer Einsatz von Energie erforderlich sind. Der CEO von Google, Sundar Pichai, hat in einem Interview mit der Technology Review im Dezember 2019 darauf hingewiesen, dass Künstliche Intelligenz und Quantencomputing eine mächtige Symbiose eingehen werden. Er vertritt die Auffassung, dass KI die Quanteninformatik beschleunigen kann und so die hartnäckigsten Probleme wie beispielsweise der Klimawandel lösbar werden.

Die Quantentechnologie ist jedoch keine brandneue Erfindung. Im täglichen Leben begegnen wir ihr bereits im Bereich der medizinischen Bildgebung oder auch bei der Anwendung von Laserlicht. Die Quantentechnologien der zweiten Generation ermöglichen mittlerweile aber viel genauere Messgeräte und eine stark verbesserte Sicherheit bei der Datenkommunikation. Diese Technologien werden enorme Auswirkungen auf Wirtschaft und Gesellschaft wie zum Beispiel in der Sicherheitspolitik haben.

Extrem schnelle Suche

Quantencomputer funktionieren prinzipiell anders als herkömmliche digitale Rechner. Im Unterschied zu deren Bits sind die kleinsten Recheneinheiten der Quantencomputer, die Quanten Bits (Qubits), in der Lage, sich untereinander zu verbinden und damit einen wesentlich komplexeren Gesamtzustand anzunehmen. Diese Verschränkung zu einem Gesamtzustand ist eine einzigartige Eigenschaft von Quantencomputern, die das komplexe wechselseitige Zusammenspiel herkömmlicher Rechner überflüssig macht. Dies ist bei einer extrem schnellen Suche in einer außerordentlich großen Datenmenge oder deren Optimierung, zum Beispiel bei logisti-



Mit dem Quantencomputer wie hier dem IBM Q auf der Consumer Electronics Show (CES) 2020 in Las Vegas könnte man einen Quantensprung in das Digitale Zeitalter machen.

FOTO: IBM

schen Systemen wie Verkehrsnetzen, von großem Vorteil.

Eine große Herausforderung ist ganz aktuell in der derzeitigen Corona-Krise, unter extrem hohem Zeitdruck Diagnoseverfahren und einen Impfstoff zu entwickeln. Dazu hat sich das Forschungszentrum jülich gemeinsam mit anderen internationalen Forschungseinrichtungen und Unternehmen einer Initiative des kanadischen Quantencomputer Herstellers D-Wave Systems Inc. angeschlossen und den Nutzern freien Zugang zu Quantencomputer-Systemen gewährt. Potenzielle Anwendungen sind dabei die Analyse neuer Diagnosemethoden in der Medizin, die hochaufgelöste Modellierung der Ausbreitung des Virus sowie eine Optimierung der Logistik, beispielsweise von Versorgungsketten und Abläufen in Krankenhäusern.

Die neue Technologie kommt auch in der Quantenkommunikation zur Anwendung. Daran arbeitet beispielsweise das Max-Planck-Institut für die Physik des Lichts in Erlangen unter Feder-

führung des Institutsgründers Professor Leuchs. Dabei werden die verschränkten Quantenzustände zum Austausch von Schlüsseln genutzt, indem man Photonen an zwei weit voneinander entfernte Orte sendet. Da sich unbekannte Quantenzustände nicht kopieren oder störungsfrei vermessen lassen, werden Fehler in der Übertragung festgestellt und können so eigen Lauschangriff aufdecken.

Kryptographie

Diese Quantenkryptographie oder Quantenschlüsselverteilung (QKD Quantum Key Distribution) ist schon länger kommerziell verfügbar und wird insbesondere von Banken und Regierungen genutzt. Allerdings lässt sich diese Technik nur bei Punkt-zu-Punkt-Verbindungen und Distanzen von weniger als 100 km realisieren. Interessant ist dabei die Frage, ob diese Technologie auch auf bereits zurückliegende Kommunikation anwendbar sein wird.

Quantencomputer können auch in der Messtechnik eingesetzt werden. Es lassen sich damit physikalische Größen wie Druck, Temperatur, Position, Zeit, Geschwindigkeit, Beschleunigung, elektrische und magnetische Felder oder die Gravitation extrem präzise messen. Dadurch erzielt man eine wesentlich höhere optische Auflösung. Zahlreiche Anwendungsfälle ergeben sich sowohl im Bereich der industriellen Präzisionsmesstechnik, der medizinischen Diagnostik und der Beobachtung als auch in der Satellitennavigation für den Luft-, See-, Schienen- und Straßenverkehr.

Wo können Quantencomputer eingesetzt werden? Dies hat Prof. Frank Wilhelm-Mauch bei einer Anhörung im Deutschen Bundestag im Ausschuss Digitale Agenda aufgezeigt:

- **Energieforschung:** Entwicklung von energiereicheren Prozessen (Quantenvorteil mathematisch bewiesen);
- **Verkehr:** Planung von Verkehrsfluss (Quantenvorteil nicht quantifiziert), Schaltungsfehlersuche in

- Luft- und Raumfahrtssystemen;
- **Medizin/Pharmazie:** Entwicklung von Wirkstoffen (Quantenvorteil mathematisch bewiesen);
- **Industrie 4.0:** schnelles Lösen von Gleichungssystemen im Hintergrund (Quantenvorteil nicht quantifiziert);
- **Verteidigung:** Crypt-Analyse (Quantenvorteil mathematisch bewiesen);
- **Maschinenlernen:** schnelles Trainieren (Quantenvorteil bewiesen, aber extreme Hardwareanforderungen);
- **Blockchain:** sichere komplexitätsbasierte Verschlüsselung.

Wilhelm-Mauch weist aber auch auf die aktuell noch massiv bestehende Fehleranfälligkeit von Quantencomputern hin. Fehlerraten von 1 zu 1000 seien durchaus gängig und 1 zu 1 000 000 das beste bisher Erreichbare. Bei 1 MHz Taktfrequenz tritt derzeit noch jede Sekunde ein Fehler auf und es bedarf weiterer enormer Anstrengungen, um die Rate zu verringern.

Fortsetzung auf Seite 19.

Beilagenhinweis:

Dieser Ausgabe liegt eine Beilage der MTS Maschinenteknik Schrode AG, Hayingen bei.

Wir bitten unsere Leser um Beachtung!