Ein Generationenwechsel **der Superlative**

Ingolf Wittmann über den Computer von morgen

Was ist ein Quantencomputer und wie unterscheidet er sich vom herkömmlichen Computer?

Der klassische Computer besteht aus Bits, die Nullen und Einsen darstellen können und in der Regel über sogenannte Transistoren mit einer Silikonstruktur funktionieren, die laut heutigem Stand im Nanometerbereich von sieben bis vierzehn arbeiten. Wenn ich so einen Rechner anschalte, dann zeigt sich der uns bekannte Vorteil, dass er bei einer Raumtemperatur von 0 bis 50 Grad Celsius solange Daten verarbeitet und lädt, bis man ihn wieder runterfährt. Er kann auch relativ große und komplexe Daten bewältigen.

Doch selbst diese enorme Rechnerleistung reicht nicht aus, um die dringendsten Fragen in der Physik und Mathematik zu klären. Und genau hier setzt das Quantencomputing an, denn diese Technologie verspricht hier Abhilfe. Ein Quantencomputer verwendet Technologien aus der Quantenmechanik, was uns eine ganz andere technische Ausgangslage verschafft, um viel komplexere Probleme zu adressieren. Doch der Nachteil schon vorneweg: Wenn wir über Quantenmechanik reden, dann sprechen wir über die kleinsten Teilchen, also über Elektronen, Neutronen oder Photonen, die manipuliert werden, um die Darstellung als Qubit – vergleichbar mit dem Bit des klassischen Computers – zu generieren. Mit Qubits kann ich aber nicht nur Nullen und Einsen darstellen, sondern theoretisch beliebig viele Zustände, was dem Quantencomputer enorme Vorteile verschafft. Das hängt jeweils vom Energielevel des entsprechenden Partikels ab. Manipuliert man die Energiemenge des Elektrons, dann verändert man sein Orbital, woraus der Energiegehalt des Qubits resultiert. Solche Prozesse können zum Beispiel im supraleitenden Bereich gemacht werden, das heißt, ich muss bei Temperaturen arbeiten, die kälter sind als das Weltall. Ein Quantumprogramm arbeitet bei etwa 15 bis 20 Millikelvin und in einem Zeitfenster von 70 bis 100 Mikrosekunden.

„Wenn wir über Quantenmechanik reden, dann sprechen wir über die kleinsten Teilchen, also über Elektronen, Neutronen oder Photonen, die manipuliert werden, um die Darstellung als Qubit – vergleichbar mit dem Bit des klassischen Computers – zu generieren."

Was hat ein Koffeinmolekül mit einem Quantencomputer zu tun?

Das ist ein beliebtes und viel zitiertes Beispiel, was gebraucht wird, um die Leistungsfähigkeit des Quantencomputers zu demonstrieren. Ein Koffeinmolekül besteht aus 95 Elektronen. Für die Berechnung der Energiebindung dieser Elektronen gibt es keinen klassischen Rechner, der über ausreichend Leistung verfügt. Wir reden von einer Kapazität von etwa 1050 klassischen Bits, die verwendet werden müssten. Einen so großen Rechner kann man gar nicht bauen, weil sich dahinter die Anzahl der Atome verbirgt, die sich auf der ganzen Erde befinden. Kurzum: Ein Quantenrechner kann ein solches Koffeinmolekül berechnen, wenn er 160 Qubits hätte. Aus diesem Beispiel leitet sich ab, dass alles, was mit der Welt und der Natur im physikalischen Sinn zu tun hat, mit einem Quantencomputer gut berechnet werden kann.

IBM Q Network

Bleibt der Quantencomputer dann doch lediglich ein wissenschaftliches Hilfsmittel oder gelingt es ihm wie dem herkömmlichen Computer, den Schritt an die breite Masse zu schaffen?

Also mehr als die Hälfte der Gespräche, die ich mit Industriekunden führe, ist kommerzieller Natur. Ich sehe den Quantencomputer für drei Bereiche brauchbar: 1. Materials Science, 2. Optimierung und 3. künstliche Intelligenz. Insgesamt sind wir damit in allen Bereichen aktiv, also sowohl im technisch-wissenschaftlichen als auch im kommerziell-wirtschaftlichen. Dass unser Smartphone der Zukunft mit einem Quantencomputer verbunden ist, das halte ich für durchaus möglich; dass ein Quantencomputer als ein mobiles Gerät zur Verfügung steht, erachte ich für eher unwahrscheinlich, wenngleich es auch nicht unbedingt unser Ziel ist.

„Ich sehe den Quantencomputer für drei Bereiche brauchbar: 1. Materials Science, 2. Optimierung und 3. künstliche Intelligenz."

Programmierer kommunizieren über ein Dualsystem aus Einsen und Nullen mit ihrem Computer. Wie kommunizieren wir mit einem Quantencomputer? Bleibt unser Zugang zu einem Quantencomputer dann doch der herkömmliche Computer?

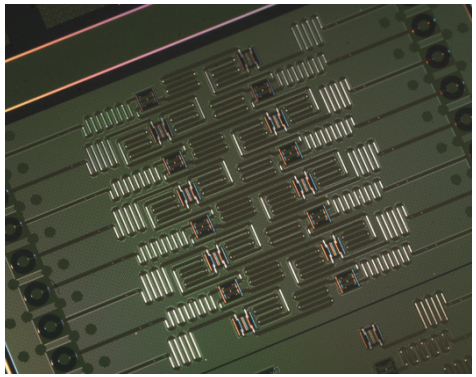
Alle momentan verfügbaren Lösungen in der Welt gebrauchen unseren herkömmlichen Computer als Kommunikationszugang zum Quantencomputer, denn der Quantencomputer ist ein Akzelerator zum klassischen Computer. Das heißt, ein Quantencomputer steht nicht alleine da, er ist eingebunden in eine klassische Rechnerumgebung. Nullen und Einsen gehen hinein – Nullen und Einsen kommen nach der Berechnung auch wieder heraus. Das, was dazwischen passiert, ist die sogenannte „Magic".

IBM hat mit dem Q-System seinen ersten kommerziell nutzbaren Quantencomputer Anfang des Jahres präsentiert. Die 20-Qubit-Maschine ist allerdings noch ausbaufähig und laut IBM nur ein erster Schritt. Wie will IBM die Kommerzialisierung des Quantencomputers bewerkstelligen?

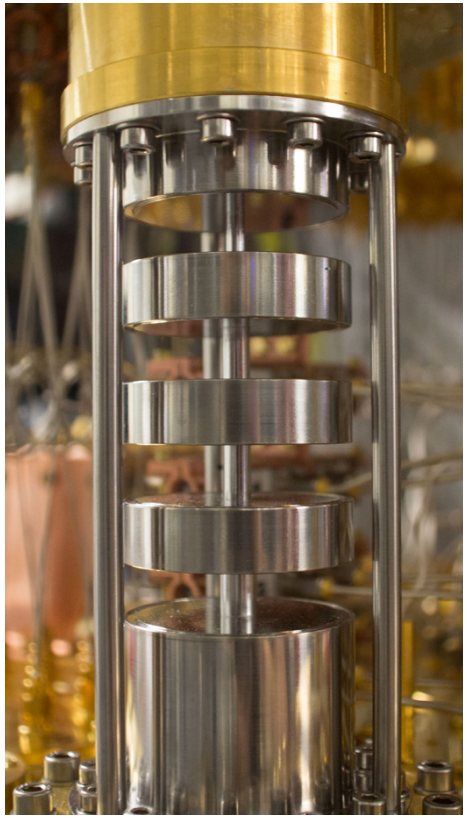
Was bedeuten zunächst einmal 20 Qubits? Es gibt die Möglichkeit, einen Quantencomputer auf einem klassischen Computer zu simulieren. Mit meinem Laptop könnte ich in etwa 20 Qubits an Leistungsfähigkeit erreichen – das heißt, solange dasselbe Problem sowohl auf einem Quantencomputer als auch auf meinem Laptop laufen würde. Der Vergleich zeigt uns, dass wir hier, was die Leistungsfähigkeit anlangt, noch relativ am Anfang sind mit der Entwicklung des kommerziell nutzbaren Quantencomputers. Unsere Top-Computer weltweit können ca. 50 Qubits simulieren. IBM hat einen Quantencomputer gebaut, der auch diese 50-Qubit-Leistungsfähigkeit erreicht. Dieses IBM Q System befindet sich derzeit in der Erprobung in den USA.

Was heißt es nun, dass IBM ein kommerziell nutzbares System zur Verfügung stellt? Das IBM Q Network, worin sich mittlerweile 78 Mitglieder befinden, besteht nicht nur aus Research-Komponenten, sondern aus industriell gefertigten Komponen-

IBM Q Experience ermöglicht es jedermann, sich mit dem Quantencomputer von IBM über die IBM Cloud zu verbinden



Der IBM 16 Qubit Processor wurde am 17. Mai 2017 als weltweit stärkster Quantencomputer-Prozessor angekündigt



Quantum Computer Mixing Chamber

ten, die zum Teil sogar in Deutschland entwickelt wurden, um Systeme industriell produzieren zu können. Mit unserem Quantencomputer kann theoretisch jeder arbeiten, auch Privatpersonen, die über IBM Q Experience auf bis zu 16 Qubits zugreifen können.

Welche physikalischen Leistungsgrenzen kann aber ein Quantencomputer selbst haben? Besteht das Risiko, dass auch er in 20, 30 oder 40 Jahren an seinen Endkapazitäten angelangt sein wird?

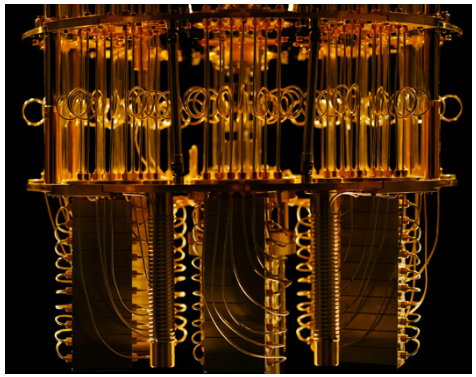
Der Quantencomputer adressiert einen ganz spezifischen Problembereich im mathematischen Umfeld. Über die möglichen Grenzen dieser Technologie wurde schon diskutiert, aber bisher hat noch keiner eine Ahnung, was genau ein mögliches Limit sein könnte. Es gibt gewiss eine Grenze, doch wo diese genau liegt, ist bisher unbekannt.

Was ist der Unterschied von Qubit und Qutrit?

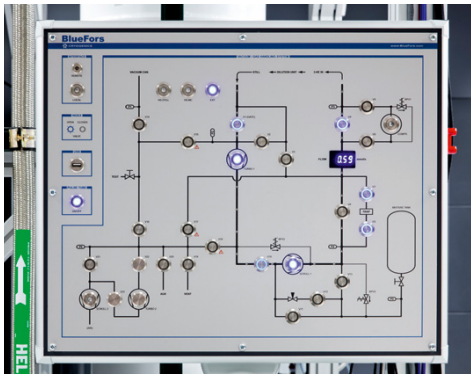
Der Begriff „Qutrit“ kommt aus der Quantenkommunikation, einem anderen Bereich der Quantentechnologie. Hier geht es um Übertragung von Informationen. Im Quantencomputing berechnen wir Dinge und versuchen, möglichst viele Qubits miteinander zu verbinden. Je mehr Qubits miteinander interagieren, umso leistungsfähiger und damit mächtiger ist mein Quantencomputer. Qutrit ist eine reine Quantumteleportation von Zuständen – in diesem Fall von drei Zuständen –, die parallel über drei verschiedene Glasfaserleitungen stattgefunden haben. Es gibt eigentlich kein direktes Pendant zwischen diesen beiden Begriffen, weshalb sich Qubit und Qutrit nicht miteinander vergleichen lassen.

Thema: Quantencomputing und Security. Sind die Quantencomputer der Zukunft aufgrund ihrer hohen Leistungskapazität eine Gefahr für unsere gängigen Verschlüsselungssysteme (zum Beispiel RSA-Schlüssel)? Gibt es Alternativen, die selbst vom Quantencomputer kommen und unserer Verschlüsselung dienen?

Mithilfe des von Shor entwickelten Verfahrens könnte man einen RSA-Schlüssel knacken. Dafür bräuchte man einen universellen, fehlerfreien Quantencomputer mit sehr vielen Qubits, den es heutzutage und auf absehbare Zeit noch nicht geben



IBM Q Dilution Refrigerator



Das IBM Q System Control Panel wird u. a. gebraucht, um das IBM Q System auf 15 Millikelvin abzukühlen

wird. Wir haben immer noch fehlerbehaftete Quantenrechner, außerdem ist die Anzahl der Qubits, die wir zur Verfügung stellen, limitiert. Wir reden hier von mehreren tausend physikalischen Qubits, die notwendig wären, um den RSA-Schlüssel zu knacken. Um mit den ganzen Problemen der fehlerbehafteten Qubits umgehen zu können, müsste man die physikalischen in logische Qubits zusammenpacken. Wir gehen davon aus, dass man in 10 bis 30 Jahren einen Quantencomputer bauen könnte, der einen 1024- oder 2048-RSA-Schlüssel knacken könnte. Dennoch müssen sich bereits heute Unternehmen Gedanken machen, wie ihre verschlüsselte Datenlandschaft und deren Security-Mechanismen ausschauen.

Ein gutes Beispiel ist die neue Generation des Personalausweises, die eingeführt werden soll. Die alte Version besaß auch einen RSA-Schlüssel, der in absehbarer Zeit durchaus entschlüsselbar wäre. Ein Personalausweis hat eine Lebenszeit von rund 30 Jahren, weshalb man bereits jetzt nach neuen quantum safe-Verschlüsselungssystemen Ausschau hält.

Daimler ist ein prominenter Partner der IBM in puncto Quantencomputing. Welchen Nutzen erhoffen sich beide von dieser Kooperation? Ist gerade die Autoindustrie ein besonders interessanter Bereich für Quantencomputer, wenn ja, warum?

Das Hauptinteresse der kommerziellen Kunden, die in das IBM Netzwerk eintreten, ist es, erstmal zu lernen, was das große Thema Quantencomputing betrifft. Wie funktioniert es? Welche Probleme kann ich unter Umständen auf einem Quantenrechner lösen? Bringt mir der Quantencomputer tatsächlich Vorteile? Alle Kooperationen, dir wir eingehen, geschehen deshalb unter Research-Aspekten.

Daimler interessieren zum Beispiel vor allem die Bereiche Produktion und Logistik, aber auch der Materials Science Bereich, etwa in der Batterientechnologie. Wie kann ich die Materialeigenschaften von Batterien optimieren, um eine längere Leistungsfähigkeit zu erzielen? Gerade solche Probleme mit einem Quantencomputer durchrechnen und simulieren zu können, kann einen Wettbewerbsvorteil bringen.

Interview: Hannes Mittermaier

Ingolf Wittmann

Ingolf Wittmann hat an der Universität Stuttgart Informatik und Betriebswirtschaftslehre studiert und als Diplom-Informatiker abgeschlossen. Der berufliche Start begann 1987 bei der Firma Nixdorf als Unix System Engineer auf der ÖD Geschäftsstelle in Stuttgart. 1990, mit der Ankündigung der RS/6000, übernahm Ingolf Wittmann die AIX Marketingverantwortung in der IBM Deutschland. Danach folgten die Positionen als RS/6000 Vertriebsbeauftragter und als Vertriebsleiter für ERP Lösungen.

2001 wurde Ingolf Wittman zum Technical Director ernannt und hat unterschiedliche nationale und internationale Positionen in unterschiedlichen IBM Organisationen bekleidet.

Seit 2014 verantwortet Ingolf Wittmann in Europa das High Performance Computing Geschäft für den akademischen und Geschäftskundenbereich. Seit 2017 hat er den technischen Bereich für Quantum Computing in IBM EMEA aufgebaut und leitet die EMEA IBM Q Ambassadors.

Ingolf Wittmann ist Mitglied des IBM DACH Technical Leadership Teams und ist für das Profession Development der technischen Professions in der IBM verantwortlich.

Er hat Bücher über AIX 4 und AIX 5L geschrieben und ist regelmäßiger Sprecher für Presse und Analysten bezüglich IT-Trends, Technologien und Open Source.

Ingolf Wittmann ist seit 2005 aktives Mitglied im Bitkom und Vorsitzender des BITKOM Arbeitskreises High Performance Computing und Quantum Computing und ist weiterhin stellv. Vorsitzender des BITKOM Lenkungsausschusses IT Infrastruktur.

Fotos: IBM Research, Connie Zhou, Graham Carlow