Überlegen durch echte Parallelität

IBM-Forscher beweisen einen speziellen Vorteil der Quantencomputer gegenüber klassischen Rechnern

Werden Quantencomputer Schlüssel knacken und Probleme lösen, die bisherige Rechnerarchitekturen niemals bewältigen können? Ja, sagt eine IBM-Forschergruppe, und sie kann den Quantum Advantage erstmals für einen bestimmten Fall beweisen.

Von Alexander Braun

Überraschenderweise erst jetzt haben Wissenschaftler bewiesen, dass der Quantencomputer einen Vorteil gegenüber allen heutigen Computern hat, wenn auch nur für einen sehr speziellen Fall. Erreicht hat diesen Meilenstein ein Projektteam aus Sergey Bravyi von IBM Research, David Gosset von der University of Waterloo und Robert König von der TU München [1].

Quantencomputer sind viel schneller als alle heutigen Computer, die sich auf das Rechnermodell der Turingmaschine zurückführen lassen; so ist es regelmäßig in Beiträgen zum Thema Quantencomputer zu lesen. Eines Tages werden Quantencomputer viele aktuelle Verschlüsselungen knacken. Der Mathematiker Peter Shor wies bereits 1994 nach, dass sein Quantencomputer-Algorithmus die Primfaktorzerlegung einer großen Zahl in polynomieller Zeit bezogen auf die Anzahl der Eingangs-Bits erledigen kann (Komplexitätsklasse P), während alle bekannten klassischen Algorithmen wenigstens subexponentielle Zeit dafür benötigen [2] – der Mathematiker würde das als NP-schwer bezeichnen. Dieses Faktorisierungsproblem bildet aber zum Beispiel die Grundlage für RSA, ein weit verbreitetes Verfahren für Public-Key-Verschlüsselungen und digitale Signaturen.

Konstante Rechenzeit

Aufgrund derartiger Durchbrüche bezweifelt kaum jemand, dass Shors Algorithmus (und selbst der erste bekannte Quantenalgorithmus überhaupt, der Deutsch-Josza-Algorithmus [3]) seinem klassischen Pendant prinzipiell überlegen ist. Die Frage ist nur: Erfindet vielleicht in Zukunft jemand einen neuen klassischen Algorithmus, welcher das Problem ebenfalls in polynomieller Zeit bewältigen kann? Denn einen Beweis dafür, dass die Primfaktorzerlegung ein NP-schweres Problem ist, hat bisher niemand geliefert.

Hier nun setzt der Beitrag der Forschergruppe an. Sie hat sich eine mathematische Problemklasse gesucht und gefunden, die zwei wichtige Eigenschaften hat: Zum einen lässt sich die Komplexitätsklasse der Algorithmen mathematisch beweisen, zum anderen existiert eine Quantenversion der Lösung, welche den gewünschten Geschwindigkeitsvorteil zeigt. Das Spannende daran: Die Komplexitätsklasse des Quantenalgorithmus ist konstant. Egal wie viele Input-Bits man hinzufügt, die Zeit zur Berechnung des Algorithmus bleibt immer dieselbe. Für den klassischen Algorithmus beweisen die Autoren, dass er nicht in konstanter Zeit abgearbeitet werden kann.

Die Autoren bevorzugen hierbei den Begriff des Quantum Advantage gegenüber der 2013 von John Preskill eingeführten Quantum Supremacy [4]. Laut Preskill umschreibt Quantum Supremacy, dass Quantencomputer einmal Aufgaben erfüllen können, die über das hinausgehen, was bisher in klassischer Computertechnik erreicht werden kann. Der Unterschied zum Quantum Advantage ist graduell und selbst Gegenstand der Diskussion.

Das mathematische Problem selbst ist bei Weitem nicht so spektakulär wie einst bei Shor, und es wird auch kurzfristig keine konkreten Ergebnisse hervorbringen. Doch darum geht es nicht: Wenn auch nur für eine sehr spezielle Problemklasse aus der linearen Algebra, so wurde hier der Vorteil des Quantencomputers gezeigt. Und diesmal muss die Fachwelt nicht darauf warten, ob in Zukunft vielleicht noch jemand eine bessere Idee hat. Der Vorteil ist schon heute vorbehaltlos bewiesen. *(agr@ct.de)* c't

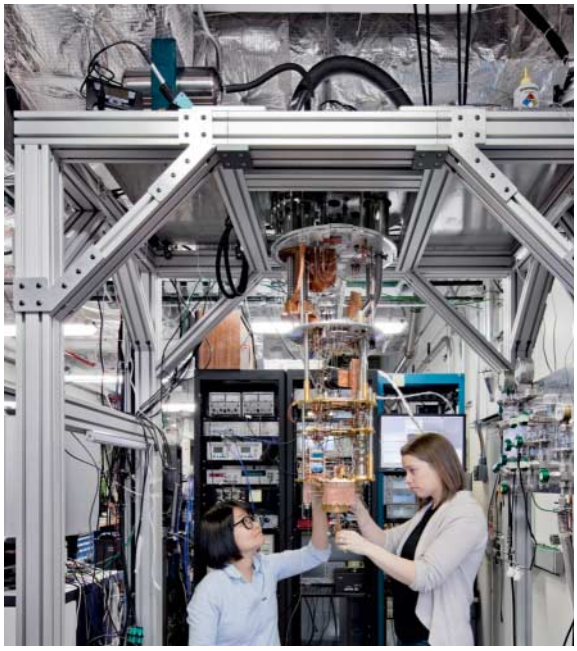

Foto: IBM

Hoher Aufwand, der aber Vorteile bringt: Arbeiten am geöffneten Kühlsystem, das im Betrieb Qubits auf Temperaturen nahe dem absoluten Nullpunkt hält. Ein 20-Qubit-System ist im Projekt IBM Q für Tests über die Cloud nutzbar.

Literatur

[1] Bravyi, S., Gosset, D., König, R., Quantum advantage with shallow circuits, Science 362 (2018)

[2] Shor, Peter W. (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., 26 (5), arXiv: quant-ph/9508027v2

[3] Deutsch, D., Josza, R., Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A. 439, (1992)

[4] Preskill, J., Quantum computing and the entanglement frontier, Rapporteur talk at the 25th Solvay Conference on Physics, https://arxiv.org/abs/1203.5813