

# QUANTEN COMPUTING

$\frac{1}{4}$  Grundlagen von Quantencomputing:  
Ein Interview mit Prof. Dr. DiVincenzo

## Impressum

### Herausgeberin:

Konrad-Adenauer-Stiftung e. V. 2021, Berlin

Umschlagfoto: © Adobe Stock/Bartek Wróblewski

Bildnachweis: S. 4 © Forschungszentrum Jülich/Ralf-Uwe Limbach

Gestaltung und Satz: yellow too, Pasiek Horntrich GbR



Der Text dieses Werkes ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international“, CC BY-SA 4.0 (abrufbar unter: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-95721-905-3

# Auf einen Blick

---

- › Nach nahezu zwei Jahrzehnten Forschung stehen Quantencomputer aktuell noch ganz am Anfang ihrer Entwicklung.
- › Es wird noch viel Grundlagenforschung und Entwicklungsarbeit zu einer ganzen Reihe von Aspekten von Quantencomputern benötigt, bevor verschiedene Anwendungsfelder des Quantencomputings tatsächlich erschlossen werden können.
- › Forschende erhoffen sich von Quantencomputern Durchbrüche in vielen rechenintensiven Anwendungsbereichen, etwa bei der Erforschung neuer Medikamente, bei der Entwicklung Künstlicher Intelligenz oder auch für die Optimierung von Lieferketten in der Logistik.
- › Aufgrund der enormen wirtschaftlichen und gesellschaftlichen Chancen, die sich mit Quantencomputern in der Zukunft verbinden, ist es für Deutschland und Europa entscheidend sich in diesem Bereich wettbewerbsfähig aufzustellen.

## Autor

---



**Prof. David DiVincenzo** gilt als Pionier im Bereich Quanteninformation. Mit seinem Namen ist unter anderem die Entwicklung von Kriterien verbunden, die ein Quantencomputer erfüllen muss, die sogenannten DiVincenzo criteria. Der Physiker ist Direktor des Jülicher Peter Grünberg Instituts, Bereich Theoretische Nanoelektronik (PGI-2), und lehrt an der RWTH Aachen am JARA-Institute for Quantum Information. Der US-Amerikaner wurde 2010 mit der Alexander von Humboldt-Professur ausgezeichnet, dem höchstdotierten internationalen Forschungspreis Deutschlands.

# Ein Interview mit Prof. Dr. DiVincenzo

---

**Sehr geehrter Herr Prof. Dr. David DiVincenzo, vielen Dank, dass Sie sich die Zeit für dieses Interview nehmen. Bevor wir eingehender in das Thema Quantencomputing einsteigen, möchte ich Sie fragen, was eigentlich das Besondere an der Quantenphysik ist, die dem Quantencomputing zu Grunde liegt?**

Man stelle sich einen beliebigen Gegenstand vor. Einerseits weist dieser Gegenstand als Ganzes diverse Eigenschaften auf, wie z. B. Größe, Form, Gewicht und Material. Andererseits besteht er aus kleinsten Teilchen, die sich im Einzelnen anders verhalten als das große Ganze. Hat man es mit einem silbernen Minutenzeiger zu tun, der gerade um eine Minute weiter im Uhrzeigersinn springt, so kann man nicht behaupten, dass alle Teilchen des Minutenzeigers die gleiche Ausrichtung haben und silbern sind. Physikalische Gesetze, die die Welt im Großen beschreiben, unterscheiden sich wesentlich von denen, die die Welt im Allerkleinsten – im subatomaren Bereich – beschreiben. Letzterem widmet sich die Quantenphysik.

Nun hat man sich Quantenphänomene bereits zunutze gemacht, um die Basis für moderne Technik zu entwickeln. Halbleiterbauelemente wie Dioden und Transistoren bilden bspw. die Grundlage der modernen Elektronik und sind in Computern, Smartphones und Fernsehern enthalten. Ohne Laser wären viele Fertigungsprozesse, Messverfahren und Kommunikation undenkbar. Auch viele materialwissenschaftliche Errungenschaften wie z. B. die Supraleitung basieren auf dem Verständnis der Quantenmechanik.

All diese Anwendungen wären ohne letztere nicht möglich. Jedoch sind die benutzten Phänomene stets makroskopischer Natur und beruhen auf dem kollektiven Verhalten einer großen Zahl mikroskopischer Teilchen.

Die Manipulation einzelner Quantenobjekte wie Atome, Elektronen oder auch Photonen erschließt weitere Quantenphänomene, welche anfänglich eher als praktisch belanglose Kuriosität erschienen, mittlerweile aber experimentell eindeutig untersucht und bestätigt sind. Deren Ausnutzung liegt im Fokus der Quantentechnologien der zweiten Generation. Für diese Quantenobjekte gelten physikalische Gesetze und Prinzipien, die das Potenzial für völlig neue technische Lösungen bieten.

**Aktuell wird immer mehr über Quantencomputing und der Forschung in diesem Feld berichtet. Hierbei wird immer wieder hervorgehoben, dass Quantencomputing eine der bedeutenden Zukunftstechnologien des digitalen Zeitalters darstellen wird. Können Sie uns kurz erläutern, warum Quantencomputing solch eine Bedeutung beigemessen wird?**

Computer und Netzwerke haben unser Leben grundlegend verändert. Doch nach Jahrzehnten rasanter Entwicklung sind Grenzen dieser Technologie erkennbar. Transistoren werden immer kleiner und nähern sich langsam subatomaren Größenordnungen. Sobald das Leistungsspektrum klassischer Rechner ausgeschöpft ist, wird ein fundamental neuer Ansatz nötig. Bereits heute sind wir in einigen Bereichen an dem Punkt, dass selbst Supercomputer gewisse Problemstellungen nicht mehr berechnen können, sei es etwa im Bereich der Optimierung von Logistikprozessen oder der Materialforschung.

Hier setzen neue Quantentechnologien schließlich an, wobei ein vielversprechender Entwicklungszweig dieser das Quantencomputing darstellt. Quantencomputer beruhen anders als heutige Rechner auf Phänomenen der Quantenmechanik und bergen das Potenzial, gewisse Aufgaben in einer relativ kurzen Zeit zu berechnen, für die

heutige Supercomputer unpraktikabel lange rechnen müssten. Durch diese Überlegenheit, auch Quantenüberlegenheit genannt, können Quantencomputer zur Lösung wichtiger Herausforderungen der Zukunft beitragen. Beispiele wären die Entwicklung neuer Werkstoffe und Pharmazeutika, oder die Gewährleistung sicherer Kommunikation im Internet. Aufgrund dieser Potenziale gelten Quantencomputer als eine Schlüsseltechnologie des 21. Jahrhunderts.

**Nachdem Sie eben schon erwähnt haben, dass Quantencomputer anders als heutige Rechner auf Phänomenen der Quantenphysik beruhen, können Sie dies eventuell noch genauer erklären und dabei auch aufzeigen, was ein Quantencomputer von heutigen Rechnern unterscheidet.**

In den 90er-Jahren wurde erkannt, dass sich quantenmechanische Teilchen als Informationsträger völlig anders verhalten als die klassischen Bits, auf denen heutige Informations- und Kommunikationssysteme aufbauen.

Die konzeptionelle Grundlage von Quantencomputern beruht im Wesentlichen auf zwei Phänomenen der Quantenmechanik – den Überlagerungszuständen (auch Superposition genannt) und der Verschränkung.

Quantenbits, auch Qubits genannt, können wie das klassische Bit den Zustand 1 oder 0 annehmen – aber auch gleichzeitig im Zustand 1 und 0 sein sowie in beliebigen Zuständen dazwischen. Verfügt man nun über mehrere Qubits, können wiederum solche Superpositionen abgebildet werden, die jeden möglichen klassischen Zustand des Gesamtsystems enthalten. So kann ein einzelner Quantenprozessor Rechenschritte auf vielen Zuständen simultan durchführen. Da die Anzahl der möglichen Zustände exponentiell mit der Anzahl der Qubits steigt, gilt dies auch für die Rechenleistung, welche weit jenseits derjenigen klassischer Computer liegen kann.

Quantencomputer nutzen zudem das quantenphysikalische Phänomen der Verschränkung. So können Qubits quantenverschränkt, also miteinander verknüpft sein. Wird ein bestimmter Zustand eines Qubits gemessen, so wird der Zustand der anderen mit ihm verlinkten Qubits in einen entsprechenden Zustand gebracht. Die Flexibilität, die die Manipulation im verschränkten Zustand bietet, trägt zu der hohen Effizienz bei, die Quantencomputeralgorithmen für bestimmte Aufgaben erzielen.

Wissenschaftler erhoffen sich daher von Quantencomputern Durchbrüche in vielen rechenintensiven Disziplinen, etwa bei der Erforschung neuer Medikamente, bei der Entwicklung Künstlicher Intelligenz oder auch für die Optimierung von Lieferketten in der Logistik.

Weiterhin ermöglicht die Eigenheit der Quantenmechanik, dass Zustände nicht ohne Veränderung beobachtet sowie gelesen, also gemessen werden können. Das Ergebnis sind Kommunikationsprotokolle, welche physikalisch gegen unbemerktes Abhören geschützt sind – ein Forschungsgebiet der Quantenkryptografie.

**Nachdem Sie jetzt einige der Grundlagen für Quantencomputer erläutert haben, würde ich Sie gern fragen, was eigentlich das Problem bei der Entwicklung von Quantencomputern darstellt?**

Quanten besitzen eine Eigenschaft, die dafür verantwortlich ist, dass unsere makroskopische Welt eher klassisch als quantenhaft aussieht – sie sind äußerst störanfällig und zerfallen leicht in den klassischen Zustand. Man nennt das Phänomen Dekohärenz. Das Problem ist, dass aufgrund der Dekohärenz die elementaren Logikoperationen oft fehlerhaft sind – derzeit misslingt auch bei den am weitesten entwickelten Quantenrechnern typischerweise jede hundertste Operation mit zwei Qubits. Im Gegensatz dazu wird eine elementare Rechenoperation auf unseren Desktopcomputern nur vernachlässigbar selten falsch ausgeführt. (Bei der Nutzung mag ein anderer Eindruck entstehen, dies liegt jedoch primär an Programmierfehlern.)

Um diese hohe Störanfälligkeit und Fehlerrate zu minimieren, verfolgen Wissenschaftler zwei Lösungsansätze. Im ersten versucht man bessere Qubits zu bauen. Hierzu zählen u. a. Ionenfallen-Qubits und Majorana-Qubits mit dem theoretisch vorhergesagten Potenzial, durch topologische Effekte eine bahnbrechende Immunität gegen Dekohärenz zu erzielen. Im zweiten versucht man, durch Fehlerkorrektur mit fehlerhaften Qubits zuverlässige Ergebnisse zu erzielen. Hier arbeitet man mit supraleitenden Qubits und siliziumbasierten Quantenpunkten als einem mit der heutigen Halbleitertechnologie gut kompatiblen Ansatz.

**Während also Superposition und Verschränkung Quantencomputer ermöglichen, ist die Dekohärenz die große Hürde. Angesichts der von Ihnen skizzierten Potenziale einerseits und der großen Herausforderung andererseits drängt sich zwangsläufig die Frage auf, wo die heutige Forschung im Bereich Quantencomputing steht und wann wir eigentlich mit Quantencomputern rechnen können?**

Nach nahezu zwei Jahrzehnten Forschung an den Eigenschaften einzelner Qubits stehen Quantencomputer aktuell noch ganz am Anfang ihrer Entwicklung.

Bisher ist es gelungen, Rechensysteme mit bis zu gut 50 verschränkten Qubits zu realisieren. Dies ist für praktische Anwendungen jedoch noch deutlich zu wenig, und die Qubits arbeiten noch zu ungenau. Je nach Ansatz werden Verbesserungen von mehreren Größenordnungen in der Fehler-rate oder Zahl der Qubits benötigt.

Ein Ansatz, von dem relativ frühe Erfolge zu erhoffen sind, ist die Verwendung von bis zu einigen hundert Qubits für kurze Algorithmen, sodass Fehler selten genug auftreten. Dadurch kann das Potenzial jedoch nicht voll ausgeschöpft werden. Für längere Algorithmen wird die sogenannte Quantenfehlerkorrektur notwendig, welche die unvermeidbaren Fehler korrigiert. Der Preis dafür ist eine Vergrößerung der notwendigen Qubit-Zahl um einen Faktor 1.000 bis 10.000. Noch keine der

verfolgten Implementierungsansätze für Qubits hat die Voraussetzungen für eine solche Hochskalierung geschaffen.

Zu der Schwierigkeit der Realisierung hinreichend vieler robuster Qubits kommt die Realisierung geeigneter Kontrollsysteme. Jedes Qubit benötigt sorgfältig abgestimmte, hochpräzise Kontrollsignale. Für kleine Systeme lassen sich bewährte Verfahren, diese zu erzeugen, nicht ohne Weiteres hochskalieren. Manche Qubits werden bei Raumtemperatur im Ultrahochvakuum betrieben und erfordern genaue Laserimpulse, welche sich nur mit sehr aufwändigen, makroskopischen Lasersystemen erzeugen lassen. Andere sind zwar mit einfacher zu erzeugenden elektrischen Signalen kontrollierbar, müssen dafür aber nahe dem absoluten Nullpunkt bei minus 273 Grad Celsius betrieben werden.

Somit wird noch viel Grundlagenforschung und Entwicklungsarbeit zu einer ganzen Reihe von Aspekten benötigt, bevor verschiedene Anwendungsfelder des Quantencomputings erschlossen werden können.

**Erlauben Sie mir hieran anschließend noch eine weitere Frage: Welche Rolle kann Quantencomputing aus Ihrer Sicht im Kontext einer sich beschleunigenden Digitalisierung in Zukunft spielen und wo ist mit Quantencomputern als erstes zu rechnen?**

Das Quantencomputing ist Teil eines größeren Bestrebens, eine Vielzahl innovativer physikalischer Technologien zum Einsatz zu bringen, um neue Formen der rechenintensiven Datenverarbeitung zu ermöglichen. Wir sehen, dass Digitalisierung gigantische Rechenzentren mit hoher Kapazität bedeutet, und dort wird zuerst das Quantencomputing entstehen. Dadurch wird das Rechenzentrum zu einem noch dominanteren Faktor bei der Digitalisierung.

**Wenn man der Berichterstattung der letzten Monate folgt, scheint es so, dass mit IBM und Google einerseits sowie Baidu und Alibaba andererseits insbesondere US-amerikanische und chinesische Firmen im Wettstreit um Quantencomputer tonangebend sind. Wo stehen eigentlich Deutschland/Europa bei der Forschung an Quantencomputern und gibt es Kooperationen mit den oben genannten Firmen?**

Mit diversen nationalen Förderprogrammen investieren aktuell viele Regierungen, v. a. China und die USA, in Quantentechnologien. In 2018 startete das dritte Forschungsflaggschiff der Europäischen Kommission, um die Entwicklung der Quantentechnologien auch in Europa mit einer Milliarde Euro Fördergeldern voranzutreiben. Zusätzlich fördert die Bundesregierung die Entwicklung der Quantentechnologien in Deutschland mit 650 Millionen Euro bis 2021. Im Rahmen der durch die Covid-19-Pandemie hervorgerufenen Wirtschaftskrise 2020 beschloss die Bundesregierung am 3. Juni 2020 ein Konjunkturprogramm, in welchem Quantentechnologien, insbesondere Quantencomputing, Quantenkommunikation, Quantensensorik und Quantenkryptografie, mit einem Finanzvolumen in Höhe von zwei Milliarden Euro gefördert werden sollen. Ziel dabei ist es, dass deutsche Institute und Unternehmen die zweite Quantenrevolution mitgestalten und international eine führende Rolle übernehmen.

Große Konzerne wie Google, IBM und Microsoft haben bereits experimentelle Quantencomputer vorgestellt. Partnerschaften zwischen diesen Konzernen und den deutschen außeruniversitären Forschungseinrichtungen sind bereits entstanden: Während IBM seinen Quantencomputer „Q System One“ in einer Partnerschaft mit der Fraunhofer-Gesellschaft nach Deutschland bringt, wurde ein gemeinsames Forschungsprogramm zwischen dem Forschungszentrum Jülich und Google initiiert. Die Jülich Unified Infrastructure for Quantum Computing, kurz JUNIQ, wird für die Ausbildung von Spezialisten in der Industrie verfügbar und über die Cloud europäischen Nutzern zugänglich sein. Forscherinnen und Forscher beider Partner bekommen zusätzlich die Möglichkeit, Simulationen auf den Superrechnern am Jülich Supercomputing Centre (JSC) durchzuführen und mit Googles Quantenprozessoren zu experimentieren.

