Quantum Computing

# 1 Grundlagen

Konventionelle Rechner basieren auf einer Hardware aus Halbleiterelementen wie Transistoren und Mikrochips. In diesen werden Informationen in Form von Bits gespeichert und verarbeitet, die jeweils die Werte 1 oder 0 annehmen können. Operationen werden durch das Abrufen gespeicherter Werte und Verarbeitung in logischen Operationen realisiert.  
In Quantenrechnern hingegen werden Informationen in Quanten-Bits oder Qubits gespeichert. Als Speichermedium wird dabei ein System mit messbaren und manipulierbaren quantenmechanischen Eigenschaften verwendet. Der entscheidende Unterschied zur konventionellen Informatik ist, dass die verwendeten Qubits neben 0 und 1 auch einen Superpositionszustand annehmen können, in dem der Qubit zu einem bestimmten Prozentsatz 1 und ansonsten 0 ist. Wird der Zustand des Qubits in Superposition gemessen, kollabiert die Superposition und der Qubit nimmt einen der diskreten zustände an. Der Prozentsatz ist dabei die Wahrscheinlichkeit, dass der jeweilige diskrete Zustand angenommen und gemessen wird. Der Zustand des Qubits kann also mit einem Vektor in der Form |ψ⟩ = α|0⟩ + β|1⟩ beschrieben werden, als Linearkombination der Zustände 0 und 1 mit den jeweiligen Wahrscheinlichkeiten α und β.

Die Datenverarbeitung in Quantenrechnern erfolgt, indem das System aus Qubits in Superposition durch quantenmechanische Operationen gezielt so beeinflusst wird, dass sich die Wahrscheinlichkeiten der Zustände der Qubits entsprechend der logischen Operation verändern. Bei der Negation eines Ein-Qubit-System in dem Zustand |ψ⟩ = α|0⟩ + β|1⟩ würde das System in einer Weise beeinflusst werden, dass das resultierende System mit dem Vektor |ψ⟩ = β|0⟩ + α |1⟩ beschrieben werden kann, die Wahrscheinlichkeiten also invertiert sind. Die tatsächlich genutzte physikalische Methode zur Realisierung dieser Operation ist dabei abhängig von der Art und Anzahl der genutzten Qubits in diesem speziellen Quantenrechner.

Es werden neben der Superposition noch viele weitere quantenmechanische Prozesse ausgenutzt, allen voran die Quantenvorschränkung. Dabei handelt es sich um einen Zustand, in dem die Zustände von zwei oder mehr Qubits voneinander abhängig sind. Das einfachste Bespiel dafür ist der Spin zweier verschränkter Elektronen. Besitzt eines der Elektronen einen bestimmbaren Spin, ist der Spin des anderen Elektrons automatisch entgegengesetzt. Diese Verschränkung kann für viele Quanten künstlich herbeigeführt werden und ist Grundlage für viele Algorithmen.

# 2 Aktueller Stand

Das Gebiet der Quantenrechner und der Quanteninformatik befindet sich derzeit noch stark in der Entwicklung. Dabei wurden zuerst verschiedene Ansätze für geeignete quantenmechanische Systeme untersucht, wobei aktuell synthetische Moleküle, Photonen und supraleitende Mikrochips die vorherrschenden Systeme darstellen. Die meisten Systeme sind dabei rein theoretisch und deshalb schwer vergleichbar, allerdings wurden einige Systeme bereits erfolgreich umgesetzt. Bereits 2001 konnte ein Quantenrechner mit 7 Qubits aus eigens synthetisierten Molekülen dazu eingesetzt werden, die Zahl 15 in ihre Primfaktoren zu zerlegen. An dieser Methode Methode wird weiterhin geforscht, bisher konnten allerdings keine größeren Zahlen verarbeitet werden.  
2016 wurde mittels verschränkter Photonen erfolgreich eine sogenannte Quantenteleportation über ein städtisches Glasfasernetz durchgeführt. Dabei handelt es sich um die Übertragung von Informationen, genauer eines Quantenzustandes, zwischen Sender und Empfänger. Der Vorteil dieser Methode besteht darin, dass kein physikalischer Überträger zwischen beiden Seiten ausgetauscht wird, sondern die Information direkt über die Quantenverschränkung übertragen wird. Dabei wird in der Mitte zwischen beiden Parteien aus einem Photon mit hoher Energie ein Paar verschränkter Photonen erzeugt, die anschließend jeweils zu Sender und Empfänger übertragen werden. Wird eines der Photonen von dem Sender manipuliert, kann diese Änderung an dem anderen Photon nachvollzogen werden. Der Vorteil dieser Methode ist, dass die Kommunikation nicht unbemerkt von einer dritten Partei abgefangen werden kann.

Aktuell sind auf dem Markt sogenannte adiabatische Quantencomputer oder „Quantum Annealing Computer“ erhältlich. Diese Varianten der Quantencomputer besitzen einen beschränkten Funktionsumfang und sind auf die Ausführung bestimmter Verfahren spezialisiert. Allgemein werden damit globale Extremwerte von komplexen Funktionen bestimmt. So können beispielsweise Optimierungen durchgeführt werden, indem verschiedene Möglichkeiten durch bestimmte Quantenzustände repräsentiert werden und das System anschließend dazu angeregt wird, sich in den Zustand der geringsten Energie zu begeben. Anhand des resultierenden Zustands kann die Lösung der Fragestellung abgeleitet werden. So wurden beispielsweise mit Systemen der Firma D-Wave bereits in Kooperationen vereinfachte Probleme der Missionsplanung für Satelliten und des Luftverkehrsmanagements gelöst [4]. 2016 brachte D-Wave ein aktuelles System mit 2000 Qubits auf den Markt, das mit supraleitenden Mikrochips arbeitet. Diese hohe Zahl an Qubits konnte erreicht werden, da in adiabatischen Quantencomputern keine Quantenverschränkung hergestellt oder genutzt wird und das System damit weniger fehleranfällig wird. Obwohl die Quantenrechner theoretisch erheblich schneller als konventionelle Rechner sein sollten, konnte es bisher in der Praxis nicht abschließend nachgewiesen werden [5]. Der Aufbau des aktuellen D-Wave 2000Q ist in Abbildung xy gezeigt. Der supraleitende Mikrochip muss permanent auch wenige mK gekühlt werden, um ungewollte Quanteneffekte zu minimieren und jegliche gemessene Signale müssen mehrfach verstärkt werden, um ausgewertet werden zu können.

Abbildung D-Wave 2000Q

Ein universeller, Turing-kompletter Quantencomputer konnte bisher nicht realisiert werden und existiert nur als theoretisches Konzept. Große Hürden bei der Umsetzung sind vor allem die benötigten Mechanismen zur Fehlerkorrektur, spontane quantenmechanische Effekte wie der Verlust der Quantenverschränkung oder der Dekohärenz, sowie die Tendenz der Systeme, sich selbstständig dem Zustand der geringsten Energie anzugleichen. Diese Effekte limitieren im Moment die maximale Anzahl der Qubits und damit den Umfang der durchführbaren Algorithmen. Die gleichen Probleme verhindern ebenfalls eine persistente Speicherung von Informationen in einem solchen quantenmechanischen System, da nach einer unbestimmten Zeit immer der energieärmste Zustand eingenommen würde und alle gespeicherten Informationen somit verloren gingen. Ein zusätzliches Problem ist, dass beim Messen des Zustands eines Qubits dieser Zustand gestört wird und damit die Informationen darauf nicht wiederholt abgerufen werden können, wie es in der konventionellen Informatik möglich ist.

Eine weitere Beschränkung ist das sogenannte „No-Cloning-Theorem“, nach dem Quantenzustände nicht auf ein anderes Qubits übertragen werden können, ohne das originale Qubit dabei zu verändern. Dementsprechend ist es nicht universell möglich, Quantenzustände zu kopieren und auf mehrere weitere Qubits zu übertragen [26].

Um den derzeitigen Mangel an Hardware zu kompensieren und die Entwicklung von Software in der Quanteninformatik zu erleichtern, wurden Quantencomputer mit konventioneller Hardware simuliert. Auch dabei wurde schnell eine Grenze erreicht, wie komplex die simulierte Hard- und Software sein kann, bis der Rechenaufwand nicht mehr realistisch bewältigt werden konnte. 2017 wurde deshalb von IBM ein neuer Ansatz zur Simulation mittels Zerlegung in kleinere Teilsysteme und sequentieller Verarbeitung der Bestandteile entwickelt, der die Simulation von Systemen mit mehr als 50 Qubits ermöglicht [20]. Es wird allerdings weiterhin ein Großrechner für Simulationen in dieser Größenordnung benötigt, weshalb IBM mit dem Projekt IBM Q über das Internet Rechenkapazitäten für externe Experimente zur Verfügung stellt. Weiterhin können im Zuge dieses Projektes Algorithmen auf verschiedenen zur Verfügung gestellten Quantenrechner ausgeführt werden können. 2017 wurde angekündigt, dass zukünftig ein 20-Qubit-System und ein experimentelles 50-Qubit-System nutzbar gemacht werden sollen.  
Für die Programmierung der Rechner wurden bereits dedizierte Sprachen entwickelt, beispielsweise das auf C# basierende Q# mit dem Microsoft Quantum Development Kit, dass den Übergang von klassischer Informatik zu Quanteninformatik erleichtern soll [21]. IBM hat für die eigenen Plattformen das QISKit veröffentlich, eine Sammlung von Tools zum Planen und Erstellen von Quantenalgorithmen, mit einem Compiler zur Umsetzung auf echter Hardware [22].

# Vorteile der Quantenrechner

Aufgrund der Superposition kann ein System mit n Qubits 2n Zustände einnehmen. Mit dem experimentellen Quantenrechner des IBM Q Projektes könnten also über eine Billiarde Zustände gleichzeitig bearbeitet werden, die auf konventionellen Systemen alle der Reihe nach bearbeitet werden müssten. Dieses Prinzip wird als Quantenparallelität bezeichnet und ist in Abbildung yz dargestellt.

Abbildung Quantenparallelität

Damit ist es möglich, Algorithmen über Datenstrukturen mit vielen Tausend oder auch Millionen Datensätzen zu parallelisieren und damit erheblich zu beschleunigen. Beispielsweise sollen damit Algorithmen zum Durchsuchen großer Datenbanken sowohl Optimierungsaufgaben für komplexe Funktionen bis zu einige tausend Mal schneller ausgeführt werden können als mit konventioneller Hardware. [5]

Ein weiteres Einsatzgebiet für Quantenrechner ist die Erforschung und Rekonstruktion von Wechselwirkungen zwischen Atomen und Molekülen sowie die Simulation von Biomolekülen. Aktuell wird an sogenannten „Quanten-Simulatoren“ geforscht, die Wechselwirkungen innerhalb von realen Systemen untersuchen und genauer simulieren sollen, als es mit konventionellen Algorithmen möglich wäre. So wurde beispielsweise 2017 mit einem 53-Qubit Quantensimulator Übergänge in Quantenmagneten untersucht und Wechselwirkungen entdeckt, die mit konventionellen Methoden nicht beobachtet werden konnten [25].

Die Möglichkeiten der Quanteninformatik sind auch für die Kryptographie äußerst interessant. Einerseits bieten Quantencomputer mit der Quantenteleportation eine Möglichkeit, Informationen sicher auch über große Distanzen zu versenden, beispielsweiße schon 2014 über 143 km zwischen den kanarischen Inseln La Palma und Teneriffa und 2017 bis zu 1400 km weit zu einem Satelliten [23,24]. Außerdem wurde bereits 1994 ein Algorithmus zur Faktorisierung von großen Zahlen geschrieben, der potentiell mithilfe von Quantenrechnern eine ganze Reihe von modernen Verschlüsselungen wie das Public-Key-Verfahren RSA entschlüsseln kann, mit denen heute beispielsweise die gesicherte Kommunikation via Whatsapp oder die gesicherten Verbindungen via SSL realisiert werden [2].

# Zusammenfassung

Quantenrechner sind komplexe Einheiten, die quantenmechanische Effekte in einem System aus Qubits ausnutzen, um Informationen zu speichern und zu verarbeiten. Mithilfe dieser Technologien sollen Probleme, die selbst mit aktuellen Supercomputern mehrere Jahrzehnte oder Jahrhunderte dauern würden, in praktikabler Geschwindigkeit ausgeführt werden können. Typische Beispiele für solche Probleme sind die Trennung von Zahlen in ihre Primfaktoren, die Simulation von komplexen Systemen oder die Ermittlung von Extremwerten in hochkomplexen Funktionen. Auch einige gewöhnliche Arbeitsschritte wie das Durchsuchen von großen Datenbanken sollen erheblich beschleunigt werden. Weitere Anwendungsgebiete sind beispielsweise die Kryptographie oder die Erforschung und Simulation von Molekülen und deren Wechselwirkungen im realen System.

Die tatsächliche Realisierung der Quantencomputer ist zum Zeitpunkt dieses Artikels allerdings nur in kleinem Maßstab möglich. Es konnte bisher noch kein universeller, Turing-kompletter Quantencomputer gebaut werden. Stattdessen wurden spezialisierte Varianten umgesetzt, mit denen bereits ein Teil der erwarteten Funktionalitäten ausgeführt werden konnten. So sind bereits Quantenrechner für die Lösung von Optimierungsaufgaben kommerziell erhältlich und es konnten bereits reale Anwendungsfälle damit gelöst werden. Weiterhin konnte bereits eine nicht abhörbare Übertragung von Quantenzuständen über große Distanzen realisiert und mittels Quantensimulatoren Wechselwirkungen in Quantenmagneten untersucht werden, die mit konventionellen Techniken nicht zu erfassen waren.

Quantenrechner sollen konventionelle Rechner allerdings nicht verdrängen, da für die meisten, alltäglichen Anwendungsfälle ein konventioneller Rechner auf Basis von Halbleitertechnik absolut ausreicht und ein Quantenrechner im Vergleich dazu viel größere technische Anforderungen hat, weitaus empfindlicher ist und bisher keine Möglichkeit gefunden wurde, Daten in Qubits persistent zu speichern. Experten gehen eher davon aus, dass Quantenrechner eines Tages als Subsysteme in konventionellen Rechnern integriert sein werden, ähnlich der aktuellen Nutzung von Graphikkarten als Coprozessoren.

Neue Quellen:

[20] E. Pednault: Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits, arXiv:1710.05867 [quant-ph], 2017

[21] Microsoft: Welcome to the Microsoft Quantum Development Kit Preview, Microsoft Documentation, 2017

[22] D. Gil: The future is quantum, IBM Research, 2017

[23] T. Herbst et al.: Quantum Teleportation over a 143 km free-space Link, Proc. SPIE 10563, 2014

[24] J. Ren et al.: Ground-to-satellite quantum teleportation, Nature 549, 70–73, 2017

[25] J.Zhang et al: Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator, Nature 551, 601–604, 2017

[26] V. Bužek, M. Hillery: Quantum copying: Beyond the no-cloning theorem, Phys. Rev. A 54, 1996