

Quantum Computing

Vorlesung H.G. Dosch und U. Marquard, Mi. 11.15-13 Uhr

Bauteile gegenwärtiger Computer erreichen die Größenordnung von Atomen. Da für die atomare und subatomare Physik die Quantenmechanik die akzeptierte und bestens bestätigte Theorie ist, wurde ein Vorschlag von Feynman aus dem Jahr 1982 immer aktueller: nämlich Computer zu bauen und Algorithmen zu implementieren, die nach den Prinzipien der Quantenmechanik funktionieren.

Beim Bau von Quantencomputern und ihrer Nutzung wurden große Fortschritte erzielt und es gibt Hinweise dafür, dass sie in Zukunft gewisse Aufgabenstellungen wesentlich effizienter lösen können als klassische Computer. Ein viel diskutiertes und beachtetes Beispiel dafür ist die Entschlüsselung aktuell verwendeter, bisher als sicher geltender Verschlüsselungsverfahren.

Es ist nicht überraschend, dass gerade die der Anschauung am stärksten widersprechenden und daher im Anfangsstadium der Theorie am heftigsten kritisierten Konzepte der Quantenmechanik, wie die Superposition und Verschränkung von Zuständen in verschiedenen Anwendungen einen Quantencomputer einem klassischen Computer überlegen machen.

Die Vorlesung ist folgendermaßen aufgebaut:

- Wir beginnen mit einer Vorstellung aktueller Herausforderungen der Digitalisierung und bekannter Grenzen klassischer Computer. Nach einer kurzen Einführung in Rechenmodelle, Algorithmen und reversibles Rechnen werden das Quantenbit und Rechenschritte darauf definiert, Quantenregister und Quantenschaltkreise eingeführt, erste einfache Algorithmen untersucht und gezeigt, wie diese implementiert werden können.
- Danach wird der formale Aufbau der Quantenmechanik noch einmal ausführlich vorgestellt. Dabei werden die Aspekte, die für die Funktionsweise eines Quantencomputers wesentlich sind, besonders hervorgehoben, z.B. Messprozess, E. Schmidt'scher Formalismus, Quantenkanäle, Superoperatoren und die Quanten-Fouriertransformation.
- In einem dritten Teil wird die Komplexitätstheorie der Informatik kurz dargestellt, um mögliche entscheidende Vorteile eines Quantencomputers aufzeigen zu können.
- Der nächste Teil der Vorlesung besteht in einer ausführlichen Beschreibung und Diskussion des Shor'schen Algorithmus. Er beruht auf Ergebnissen der Zahlentheorie und der Quanten-Fouriertransformation. Er ist nicht nur der Algorithmus, der aktuell für die größte Aufmerksamkeit sorgt, sondern an ihm lassen sich auch die wesentlichen Vorteile des Quantencomputers und die Elemente der Quantenkomplexität sehr gut darstellen.
- Ein weiterer essentieller Punkt für die Entwicklung der Quantencomputer war die Entdeckung von Verfahren zur Fehlerkorrektur, die wir in diesem Teil der Vorlesung betrachten werden.
- Die Eigenschaften der Quantenmechanik erlauben die Implementierung abhörsicherer und verschlüsselter Kommunikation. Diese wurde bereits über viele 100 km erfolgreich getestet (Nobelpreis für Physik 2022) und ist wesentliche Voraussetzung für ein Quanteninternet.
- Abschließend sollen verschiedene Ansätze zum Bau von Quantencomputern und zur Realisierung von Gates vorgestellt werden.

Falls Zeit bleibt, werden noch einige Aspekte der Quantenlogik und der Quanteninformationstheorie (Entropie) näher untersucht.

Zielgruppe: Studentinnen und Studenten, die sich für Theoretische Quantenmechanik und Informatik interessieren.

Voraussetzung: Kenntnis der Quantenmechanik, z.B. Vorlesung Quantenmechanik (Theoretische Physik IV)