Quantum Computing

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

Durch die Miniaturisierung kommen Bauteile der gegenwärtigen Computer in die Grössenordnung von Atomen. Für die atomare und subatomare Physik ist die Quantenmechanik die akzeptierte und bestens bestätigte Theorie. Daher wurde ein Vorschlag, deneynman schon 1982 gemacht hatte, immer aktueller: nämlich Computer zu bauen, die nach den Prinzipien der Quantenmechanik funktionieren.

Inzwischen wurden beim Bau von Prototypen von Quantencomputern 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 beachtenswert, 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 (Schrödingers Katze) in gewissen Fällen einen Quantencomputer einem klassischen 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 und Algorithmen werden das Quantenbit und Rechenschritte darauf definiert, Quantenschaltkreise eingeführt und erste einfache Algorithmen untersucht.

• 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 und Quanten-Fouriertransformation

• In einem dritten Teil wird die Komplexitätstheorie der Informatik kurz dargestellt, um die möglichen entscheidenden Vorteile eines Quantencomputers aufzeigen zu können

• Ein wesentlich Teil der Vorlesung besteht in einer ausführlichen Beschreibung und Diskussion des Shore´schen Algorithmus. Er beruht auf Ergebnissen der Zahlentheorie und der Quanten-Fouriertransformation. Er ist nicht nur der Algorithmus, der z. Zt. für die größte Aufmerksamkeit sorgt, sondern an ihm lassen sich auch die wesentlichen Vorteile des Quantencomputers und die Elemente der Quantenkomplexität sehr gut darstellen.

Falls Zeit bleibt, wollen wir noch das Thema Fehlerkorrektur betrachten und einige Aspekte der Quanteninformationstheorie (Entropie) näher untersuchen.