Der Quantencomputer

Christoph Ernst und Jens Schröter im Gespräch mit David Gross, kommentiert von Martin Warnke

CE/JS: Eine erste Frage zum Problem, einen Quantencomputer überhaupt technisch-materiell zu realisieren: Welche verschiedenen Architekturen von Quantencomputern heute kann man unterscheiden, welche Lösungen gibt also? Und daran anknüpfend: Standards auf Ebene von Architekturen sind natürlich immer nur historische Momentaufnahmen, aber könnten Sie sich vorstellen, dass sich in den nächsten Jahren schon so etwas ein erster ›Standard‹ für eine Quantencomputerarchitektur ausbildet, oder ist das alles noch viel zu früh?

DG: Es sind noch viele mögliche Architekturen im Rennen. Welche gerade vorne liegt, das hat sich in den letzten Jahren immer mal wieder geändert. Erste Experimente wurden z.B. mit Photonen gemacht, also Quantenzuständen des Lichts. Photonen wechselwirken nur schwach miteinander und mit der Umgebung – das war zunächst ein Vorteil, da die Quanteninformation, die sie tragen auf diese Art geschützt war. Später wurde es zum Nachteil, da es schwierig ist, viele photonische Qubits miteinander wechselwirken zu lassen. Danach waren gefangene Ionen die erfolgreichste Plattform – heute liegt die Hoffnung auf Festkörperqubits, die sich mit den gleichen Methoden wie Mikrochips produzieren lassen. Man kann die Entwicklung mit der Frühphase klassischer Computer vergleichen. Mechanische Schalter, Relais, Vakuumröhren, Transistoren und integrierte Schaltkreise wurden nacheinander entwickelt. Erst nach einigen Jahrzehnten hatten sich siliziumbasierte Halbleiter als Standardarchitektur durchgesetzt.

MW: Die Einsicht, dass ›Quantencomputer‹ sich noch in einem sehr frühen Entwicklungsstadium befinden, möchte ich unterstreichen, bis dahin, den Begriff selbst probehalber in Anführungszeichen zu setzen. Denn unsere Vorstellung von Computern ist doch sehr von ihrer Nützlichkeit und Universalität bestimmt, und davon kann ja im Falle der Quanten-›Computer‹ noch keine Rede sein. David Gross führt das ja völlig zu Recht weiter unten aus. Wir sollten jedenfalls vorsichtig damit sein, unsere ausgearbeiteten Überzeugungen zu Computern allzu schnell auf die neue Technik zu übertragen.

ZfK – Zeitschrift für Kulturwissenschaften 2|2022
urn:nbn:de:hbz:6:3-zfk-2022-44931

CE/JS: Könnten Sie genauer »Festkörperqubits« erläutern? Was sind »adiabatische Quantencomputer«?

DG: Festkörperqubits: Prozessoren in handelsüblichen klassischen Computern enthalten Milliarden von Schaltelementen, die in hochentwickelten Prozessen in Siliziumchips geätzt werden. Diese Technologie würde man auch gerne verwenden, um Quantenbits herzustellen. Insbesondere verspricht man sich davon die Möglichkeit, wie auch in klassischen Chips, eine sehr große Anzahl von Qubits auf einmal produzieren zu können. In Bezug auf das Siliziumsubstrat spricht man von Festkörperqubits.
Adiabatische Quantencomputer: Digitale Computer lösen Rechenprobleme, in dem sie eine Eingabe Schritt für Schritt nach einfachen Regeln verarbeiten. Adiabatische Rechenprozesse funktionieren anders. Das Ziel ist, ein schwieriges Optimierungsproblem zu lösen. Also z.B. »ein Carsharing-Anbieter hat 1000 Autos und 100.000 Kunden – wie verteilt man die Fahrzeuge so, dass Wartezeiten minimiert werden?«. Ein adiabatischer Computer würde mit einer leichten Version des Problems anfangen. Zum Beispiel mit Kunden, die alle nur nacheinander ein Auto brauchen. Der Computer würde das leichte Problem lösen. Dann erhöht man den Schwierigkeitsgrad nach und nach – einzelne Buchungsanfragen überlappen sich. Ausgehend von der einfachen Lösung, sucht der adiabatische Computer nun eine Lösung des etwas schwierigeren Problems. Auf diese Weise hofft man, am Ende eine Lösung des echten Problems zu erhalten. Ich schreibe ›man hofft‹ – denn es ist oft nicht beweisbar, dass diese Algorithmen tatsächlich in vernünftiger Zeit das optimale Ergebnis finden.

MW: Ursprünglich gingen die Überlegungen, wie man mit Quantensystemen rechnen könnte, noch vom Wunsch aus, die Leistung klassischer Computer drastisch zu steigern. Es wurden Schaltelemente ersonnen, mit denen klassische Computer-Bauelemente nachzubauen wären, aber eben tendenziell mit vervielfachter Leistungsfähigkeit. Auf diese Weise könnte man das, was man über den Bau von Computerhardware weiß, auf die Quantensysteme übertragen. Das war die Hoffnung.
Nun aber entstehen Systeme, die nach völlig anderen Prinzipien arbeiten, und das ist eigentlich auch nicht sehr verwunderlich: andere Medien treiben andere Formen hervor. Adiabatische Verfahren könnten ganz einfach auf Quantensysteme sehr viel besser passen als logische Schaltungen, und das heißt, in gewisser Weise fängt man wieder von vorn an mit dem Verständnis eines *computing*. Das ist ein weiterer Grund, hier mit Begriff des Computers vorsichtig zu sein, auch mit dem des Algorithmus.

CE/JS: Anknüpfend an die Frage zu den Architekturen: Was sind gegenwärtig die größten Schwierigkeiten, die sich bei der Realisierung von Quantencomputern ergeben – und noch etwas zugespitzter: Welche Schwierigkeiten erwartet man eigentlich zukünftig noch? Gibt es also Schwierigkeiten, von denen man ahnt, dass sie noch bevorstehen, aber – gegeben den heutigen Stand der Entwicklung – noch ›vor uns‹ liegen und zukünftig bewältigt werden müssen?

DG: Die größte Herausforderung liegt in der fragilen Natur von Quanteninformation. Kleinste Störungen machen den Quantenvorteil zunichte. Das ist kein prinzipielles Problem: Es gibt Methoden zur Quantenfehlerkorrektur, die Störungen kompensieren können. Praktisch sind wir aber weit davon entfernt, diese einsetzen zu können. Das Problem ist, dass man eine sehr große Anzahl von Qubits bräuchte, um heute realisierbare Fehlerraten abfangen zu können. Also muss man entweder die Qualität der einzelnen Qubits deutlich verbessern, oder sie in sehr viel höheren Mengen produzieren. Beides sind sehr schwierige Aufgaben.

CE/JS: Könnten Sie genauer erläutern was eine »Quantenfehlerkorrektur« ist und wie sie funktioniert? Könnten Sie genauer erläutern, welche Rolle »Verschränkung« für das Funktionieren von Quantencomputern hat?

DG: Quantenfehlerkorrektur: Stellen Sie sich vor, aus diesem Text würden einzelne Buchstaben herausgelöscht. Wahrscheinlich könnten Sie ihn trotzdem fehlerfrei entziffern. Das funktioniert, da menschliche Sprache *redundant* ist: Wir benutzen mehr Worte als strenggenommen nötig. Datenträger in Computern machen das genauso, und auch Rechenprozesse kann man fehlertolerant gestalten. Da Quantencomputer besonders empfindlich gegen äußere Störungen sind, ist die Entwicklung von Fehlerkorrekturmechanismen besonders wichtig. Sie ist aber auch besonders schwierig, da man den Inhalt von Quantenbits nicht einfach kopieren kann. Lange war daher unklar, wie man Redundanz für Quanteninformation realisieren kann. Das Problem ist mittlerweile zumindest theoretisch gelöst – praktischen Implementierungen bleiben aber sehr schwierig.
Verschränkung: Uff, ich glaube, das geht über diesen Artikel hinaus.

MW: Fehlerkorrektur ist eine Strategie, die eng mit dem Digitalen und der diskreten Kodierung verknüpft ist. Ob das tatsächlich eine Methode bleiben wird, die dem medialen Substrat von Quantensystemen angemessen ist, bleibt abzuwarten. Es könnte durchaus sein, dass »Fehlerkorrektur« irgendwann als Relikt erkannt wird, weil das, was unter dem Blickwinkel von heute als Fehler gilt, sich morgen als das Eigentliche herausstellt, was auszunutzen ist. Aber ich habe natürlich gut Reden, aus sicherer Entfernung zur konkreten technischen Entwicklung!

CE/JS: Quantencomputer sind – zumindest in unserem laienhaften Verständnis – ja eine Technologie, für die zwar auf gesellschaftlicher Ebene schon eine Reihe von möglichen Anwendungsszenarien entworfen wurden – etwa wenn man Diskussionen über die Kryptografie und Sicherheit denkt. Wo sehen Sie Anwendungsgebiete von Quantencomputern in näherer und in fernerer Zukunft?

DG: Zur Kryptografie: Da hätten – das muss an ehrlich sagen – Quantencomputer zunächst negative Auswirkungen. Die bisherigen Methoden um Kommunikation im Internet zu schützen würden ihre Sicherheit verlieren, wenn große Quantencomputer gebaut werden könnten. Für Geheimdienste attraktiv – für Verbraucher aber schlecht.

Die am besten verstandene positive Anwendung läge in der Materialforschung und der Chemie. Quantencomputer könnten chemische Reaktionen oder exotische Materialen simulieren.

MW: Eine positive Anwendung könnten noch die abhörsicheren Übertragungskanäle sein, bei denen die Wahrscheinlichkeit, ein Anzapfen zu entdecken, beliebig gesteigert werden kann. Die Wiener Quantenoptiker um Anton Zeilinger haben das ausprobiert, und es gibt auch schon kommerzielle Lösungen.

CE/JS: Könnten Sie die Verfahren der Quantensimulation noch etwa detaillierter darstellen? Wie unterscheidet Sie sich von Verfahren der Simulation mit klassischen Computern?

DG: Für den Anwender unterscheiden sich Quantensimulationen nicht von klassischen Simulationen. In beiden Fällen wird das Verhalten z.B. von einem Werkstoff am Computer berechnet, sodass man die Eigenschaften studieren kann, ohne es bauen zu müssen. Für viele Materialen wäre ein Quantensimulation aber ungleich schneller als eine klassische Simulation. Der Grund ist letztendlich, dass die Materialien selbst durch die Gesetze der Quantenmechanik beschrieben werden.

MW: Arturo Rosenblueth, Norbert Wiener und Julian Bigelow schrieben 1945 in *Behavior, Purpose and Teleology*: »The ultimate model of a cat is of course another cat, whether it be born of still another cat or synthesized in a laboratory.«

CE/JS: Vielleicht ist es eine Fehlwahrnehmung, wenn man von außen auf das Feld guckt, aber derzeit scheint weitestgehend Einigkeit darin zu bestehen, dass Quantencomputer ein immenses Potenzial und möglicherweise auch die oft zitierten ›revolutionären‹ Effekte haben werden. Vor diesem Hintergrund einmal naiv gefragt: Was sind eigentlich die heute absehbaren Vor- und Nachteile von Quantencomputern gegenüber klassischen Digitalcomputern?

[Siehe auch oben]

DG: In den letzten Jahrzehnten haben wir erlebt, dass Computer immer neue Anwendungsgebiete erfolgreich bearbeiten können. Da kann man leicht aus dem Blick verlieren, dass es auch Problemklassen gibt, die klassische Rechner nie werden lösen können. Ein Beispiel dafür sind allgemeine Optimierungsprobleme. Also z.B.: Finde für jede Stellung den bestmöglichsten aller Schachzüge. Die Anzahl der möglichen Lösungen ist dabei schnell größer als die Anzahl der Atome im Universum. Alle Möglichkeiten einzeln durchzuprobieren um die optimale zu finden ist daher nicht möglich. Aber häufig ist keine ›Abkürzung‹ bekannt, die es uns erlauben würde, eine erschöpfende Behandlung aller Möglichkeiten zu vermeiden. Man glaubt auch (bewiesen ist das übrigens nicht), dass die klassische Physik in vielen Fällen prinzipiell keine solche Abkürzung zulässt.

Hier liegt nun die Hoffnung, dass Quantencomputer Informationen über exponentiell viele Lösungsmöglichkeiten auf einmal nutzen können. ›Exponentiell viele‹ heißt dabei, dass die Anzahl der Qubits gleich der Anzahl der Nullen der Zahl ist, die die gleichzeitig durchschrittenen Lösungswege angibt. Etwa 80 Qubits würden dabei ausreichen, um so viele Wege zu beschreiten, wie es Atome im Universum gibt.

Sie merken vielleicht, dass ich mich vorsichtig ausdrücke. Die Details sind schwierig, und bislang ist nur für eine kleine Menge sehr spezieller Probleme verstanden, wie dies umzusetzen ist. Das berühmteste Beispiel ist leider für Verbraucher keine gute Nachricht: Das Knacken kryptografischer Codes, ohne dass man alle möglichen Schlüssel nacheinander durchprobieren müsste.

MW: David Gross' Vorsicht ist ganz sicher angebracht. Wenn man mag, könnte man den Simulationsgedanken weiterspinnen: eine Simulation des Universums müsste auch alle Quantencomputer umfassen, die es im Universum gibt. Die Rekursivität dieses Anspruchs lässt sofort jede Hoffnung auf komplette rechnerische Vorwegnahme von allem implodieren.

CE/JS: Dieses Knacken kryptografischer Codes ist interessant. Was würde eine solche Technologie z. B. in der Hand von Kriminellen denn bedeuten? Würde Homebanking dann obsolet? Es gibt aber offenbar doch auch quantencomputersichere Verschlüsselungsverfahren (z. B. Daniel J. Bernstein: Introduction to post-quantum cryptography, 2009)? Könnten Sie dazu etwas sagen? Wieso sind diese Verfahren offenbar sicher gegen Angriffe mit Quantencomputern?

DG: Über Kriminelle würde ich mir bis auf weiteres keine Sorgen machen. Wohl aber über Staaten, deren Geheimdienste Kommunikation im Internet dann nach Belieben entschlüsseln können. Home Banking wäre dann tatsächlich nicht mehr so leicht zu sichern wie bisher. Aber nicht nur die Verbindung mit Ihrer Bank wäre betroffen. Ihre Suchanfragen im Internet oder Ihre Emails könnten genauso mitgelesen werden.

Post-quantum cryptography ist der Versuch, Verfahren zu entwickeln, die auch gegen Quantencomputer sicher sind. Alle bislang bekannten Verfahren sind aber noch zu aufwendig für die Praxis. Und »offenbar sicher« gegen Quantencomputer sind sie nicht! Es sind lediglich keine Quantenattacken bekannt. Kryptographie ist immer ein Katz- und Mausspiel zwischen Benutzern und Angreifern. Post-Quantum-Krypto ist nur die nächste Runde.

MW: Genau. Flapsig: der Quantenigel überholt (vielleicht) den Quantenhasen.

CE/JS: Wie kann man sich den kommerziellen Einsatz von Quantencomputern vorstellen? Sie werden ja mutmaßlich in einem ›Ökosystem‹ gemeinsam den klassischen Digitalcomputern bestehen und eingesetzt? Wie muss man sich diese Integration laienhaft vorstellen: Werden sie etwa als »Quantenchips« in konventionellen Rechnern eingesetzt werden? Oder wird man bestimmte Berechnungen über das Netz an Quantencomputer

geben und von dort wieder die Lösung bekommen? Kurzum: Wie muss man sich diese Verknüpfung von ›alten‹ und ›neuen‹ Rechnerprinzipien vorstellen?

DG: Die derzeitig absehbaren Anwendungsgebiete – Kryptoanalyse, Materialwissenschaften – sind sehr spezialisiert. Auch wird sich die Hardware auf absehbare Zeit von normalen Computern stark unterscheiden – z.B. durch die Notwendigkeit bei Temperaturen knapp über dem absoluten Nullpunkt zu arbeiten. Quanten-Koprozessoren im Mobiltelefon sind nach unserem Kenntnisstand daher weder realistisch noch nützlich.

Andererseits drückt sich hierbei vielleicht ein Mangel meiner Fantasie aus. Man sagt, IBM hätte in den 50er Jahren einen Weltmarkt für einige Hand voll von Computern gesehen … Also mal sehen …

MW: Ja, spannender Punkt. Dass Graphikkarten einmal so wichtig werden, weil sie für das Schürfen von Bitcoins und für künstliche neuronale Netze nützlich sind, das hätte bis vor kurzem auch niemand erwartet.

CE/JS: Würden Sie Quantencomputer – insbesondere auf Ebene der grundlegenden Speichereinheit der Qubits – eher als analoge oder eher als digitale Technologie bezeichnen? Oder ist die für uns heute lieb gewonnene und ja inzwischen inflationär gewordene Unterscheidung eigentlich für Quantencomputer gar nicht sinnvoll anwendbar?

DG: Analog oder digital – darüber gab es in der Frühzeit der Quantencomputer eine intensive Debatte. Der Vorteil einer digitalen Architektur ist, dass sie Fehlertolerant ist. Wenn man einen 0-Zustand ein wenig stört, bleibt er weiterhin als 0 erkennbar. Bei analogen Computern wirkt sich jeder kleine Fehler hingegen auf das Endergebnis aus. Zunächst dachte man, dass Quantencomputer in dem Sinn analog sind, dass jeder Fehler das Ergebnis beeinflusst. Nach der Entwicklung der Theorie der Quantenfehlerkorrektur wurde aber klar: Das muss nicht so sein. Fehlerkorrigierte Quantencomputer werden daher heute als ›digital‹ klassifiziert.

MW: Ich gebe zu bedenken: auch ein fehlertoleranter Quantencomputer, der stabile Ergebnisse aus stabilen Inputs liefert, erzeugt bei jedem seiner Läufe ein anderes Ergebnis, wie ja auch der Durchgang eines Photons durch den Doppelspalt immer ein ›oben durch‹ oder ›unten durch‹ ergibt oder die Bestimmung des Spins eines Elektrons immer einen scharfen Wert *up* oder *down* und nichts dazwischen, aber in statistischer Verteilung. Das Ergebnis jeder Quantenoperation ist ja ein Einzelereignis einer statistischen Verteilung, etwa die Fifty-fifty-Aufteilung des Doppelspalts. Um so eine Verteilung abzutasten, zu samplen, muss man dann die Quantenberechnung entsprechend oft ausführen, mit den jeweils präzisen Ergebnissen am Ende, die allerdings ein statistisches Ensemble darstellen. Deshalb sind, so meine Überzeugung, Quantensysteme *immer* analog.

CE/JS: Derzeit erlebt die Forschung zu künstlicher Intelligenz bekanntlich (wieder einmal) einen ›Sommer‹, in dem die Zukunft grenzenlos und offen erscheint. Wie würden

sich das mögliche Verhältnis von Quantencomputern und den derzeitigen Verfahren der Herstellung so genannter ›künstlicher Intelligenz‹ beschreiben?

DG: KI ist ein weites Feld. Seit einigen Jahren, ist KI in der öffentlichen Diskussion eng verbunden mit der Methode der ›tiefen neuronalen Netze‹, die z.B. in der Bild- und Spracherkennung und Synthese große Fortschritte erfahren haben. Es gibt Arbeiten, die untersuchen, ob man das Trainieren solcher neuronalen Netze auf Quantenhardware effizienter realisieren könnte. Das ist aber noch spekulativ. Kurz: Zwei sehr spannende Entwicklungen, deren Zusammenhang noch unklar ist.

MW: Die Wikipedia teilt uns mit, dass selbst die Zuordnung des Zitats »Prognosen sind schwierig, vor allem, wenn sie die Zukunft betreffen«, eine knifflige Sache ist. Vielleicht stammt es von Niels Bohr, was ja sehr gut hierher passte, vielleicht aber auch von Karl Valentin, was überall gut hinpasst. Vielleicht aber auch von wem anderen.

CE/JS: Eine Frage, die etwas assoziativer ist und ein etwas vageres Feld adressiert: Interessanterweise findet man heute immer wieder Querverweise auf klassische Medien, wenn es um die Nutzung von quantenphysikalischen Effekten für Kommunikationstechnologien geht, etwa die Rede von einem zukünftigen ›Quanteninternet‹. Wenn man Quantencomputer als Medien bezeichnen würde – macht das Sinn für Sie oder könnten Sie sich darunter etwas vorstellen?

DG: Quantentechnologie kann für Rechenaufgaben genutzt werden – aber auch für Kommunikationsaufgaben. Darauf zielt das »Quanteninternet« ab. Die möglichen Anwendungen sind noch etwas spekulativer als es für Quantenrechner der Fall ist. Es gibt das Feld der Quantenkryptografie, das auf der Erkenntnis beruht, dass gewisse kryptografische Aufgaben fundamental sicher sind, wenn Information durch Quantenzustände dargestellt wird. Aber selbst auf theoretischer Ebene ist das Verständnis von Quantennetzwerken noch sehr unvollständig.

MW: Eine medienwissenschaftliche Antwort könnte mit Luhmann lauten: natürlich sind Quantencomputer Medien, denn sie ermöglichen oder verhindern bestimmte Formbildungen. Der klassische Computer treibt eine dermaßen große Formenvielfalt aus, dass er kaum als Medium zu beobachten ist. Das ist beim Quantencomputer (noch) anders: es gibt bislang nur Ansätze und sehr wenige Realisierungen, er lässt sich (noch) gut in seinen medialen Eigenschaften festmachen.

CE/JS: Können Sie uns die Vorteile eines »Quanteninternets« – jenseits der hypothetisch möglichen absolut sicheren Kommunikation – erläutern? Was soll es können, was das Internet nicht kann? Man liest manchmal, dass »Verschränkung« nicht für kommunikative Zwecke genutzt werden kann – warum nicht?

DG: Anwendungen jenseits von sicherer Kommunikation werden aktiv erforscht. Viel ist nicht bekannt. Ein Beispiel von Anwendungen, über die man sich Gedanken macht, sind sichere Abstimmungen, bei denen alle Benutzer dem Ergebnis vertrauen können, ohne dass man nachvollziehen kann, wer wie abgestimmt hat. Verschränkung kann nicht genutzt werden, um Signale beliebig schnell zu übertragen (also zum Beispiel schneller als Lichtgeschwindigkeit). Das ist wahrscheinlich gemeint, wenn Sie lesen, dass es »nicht für kommunikative Zwecke« genutzt werden kann.

MW: Verschränkung ist ja nicht das einzige Quantenphänomen. Die gesamt Halbleitertechnik ist nur quantenmechanisch zu erklären. Ohne Quantenphänomene keine Elektronik und auch kein Computer und auch mittlerweile keine Nachrichtentechnik. Meine Oberlehreranmerkung, und, ich gebe das unumwunden zu, auch aus purer Lust am Widerspruch: das Internet ist schon immer *quantum* gewesen.

CE/JS: Zum Abschluss eine ganz andere Frage: Lesen Sie gerne Science Fiction? Kennen Sie Darstellungen von Quantencomputern in der SF, die Sie interessant finden? Haben Sie einen Lieblingscomputer?

DG: Vielleicht reichte die Phantasie der SF-Autoren nicht aus: Ich kann mich nicht an Quantencomputern in SF-Büchern erinnern. Die berühmten Rechner der Literatur schöpften ihre Stärke aus schierer Größe – Douglas Adams' *Deep Thought*, z.B., bestand wörtlich aus der ganzen Erde – statt aus fundamentaler Physik. (Bei Antrieben von Gefährten war der gleiche Autor deutlich kreativer: Das Raumschiff *Heart of Gold* wurde durch *Unwahrscheinlichkeit* angetrieben, bedient sich also eher den Begriffen der Quantenmechanik. Es entspricht dem Klischee, dass Adams, als Kind der 1960er Jahre, mehr Kreativität in Fahrzeuge investierte, als in Informationstechnologie. Über diese Phase sind wir zum Glück hinweg).

CE/JS: In Tom Hillebrands Romanen (wie Qube) oder bei Cixin Liu (Trisolaris-Trilogie) spielen Quantencomputer eine Rolle. Uns würde ihre Einschätzung interessieren, aber das ist natürlich eine Frage für die fernere Zukunft.

MW: Cixin Liu hat 2017 die Erzählung »Spiegel« geschrieben, die einen Quanten-Supercomputer in den Mittelpunkt stellt, der, wenn man ihn mit den richtigen Parametern startet, im Sinne des Hyperdeterminismus *alles* von *überall* darstellen kann. Keine Situation bleibt mehr geheim, in Vergangenheit und Zukunft. Der chinesische Geheimdienst-Offizier hat keine Aufgabe mehr und stirbt glücklich und pflichterfüllt.