Hochleistungsrechner: Aktuelle Trends und Entwicklungen
Winter Term 2015/2016

Adiabatische Quantencomputer

Jon-Magnus Maier
Ludwig-Maximilian Universität München

04.02.2016

Zusammenfassung

Diese Arbeit gibt einen Überblick über das Thema (Adiabatische) Quantencomputer ohne zu sehr auf die technischen Details einzugehen. Es werden grundlegende Begriffe erklärt und Unterschiede zu herkömmlichen Computern betrachtet. Vor- und Nachteile von Quantencomputern, aktuelle Technologien und potentielle Anwendungsgebiete werden näher erläutert.

1 Einleitung

Quanten verfügen über Eigenschaften die außerhalb der klassischen Physik liegen. Es ist möglich diese Eigenschaften zu nutzen um mathematische Berechnungen durchzuführen. Diese hohe potentielle Rechenleistung kann dazu verwendet werden um Quantenphänomene zu simulieren, Probleme der Kombinatorik zu lösen oder die Grundlage einiger moderner Verschlüsselungsalgorithmen zu zerstören. Es existieren derzeit verschiedene Technologien zur Realisierung Adiabatischer Quantencomputer. Eine Technologie nutzt die Adiabatische Evolution um Probleme der Kombinatorik zu lösen. Andere Technologien nutzen Ionenfallen, Photonen oder Supraleiter um Quanten Bits (s. g. Qubits) zu erzeugen. Es existieren verschiedene Algorithmen die Quanteneigenschaften ausnutzen, wie die Primzahlzerlegung mit dem Shor-Algorithmus, die Datenbanksuche mit dem Grover-Algorithmus oder Adiabatische Algorithmen um Optimierungsprobleme zu lösen.

2 Grundlegende Begriffe

Für die Erklärung was Quantencomputer und deren neueste Entwicklungen sind, ist es erforderlich einige grundlegende Begriffe zu erläutern.

2.1 Quanten

Es existieren verschiedene Definitionen von Quantenmechanik, für die Zwecke dieser Arbeit ist die Definition von Wikipedia gut geeignet. "Die Quantenmechanik ist eine physikalische Theorie zur Beschreibung der Materie, ihrer Eigenschaften und Gesetzmäßigkeiten. Sie erlaubt im Gegensatz zu den Theorien der klassischen Physik eine Berechnung der physikalischen Eigenschaften von Materie auch im Größenbereich der Atome und darunter. [...] Im Rahmen der klassischen Mechanik lässt sich aus dem Ort und der Geschwindigkeit eines (punktförmigen) Teilchens bei Kenntnis der wirkenden Kräfte dessen Bahnkurve vollständig vorausberechnen. Der Zustand des Teilchens lässt sich also eindeutig durch zwei Größen beschreiben, die (immer in idealen Messungen) mit eindeutigem Ergebnis gemessen werden können. Eine gesonderte Behandlung des Zustandes und der Messgrößen (oder

"Observablen") ist damit in der klassischen Mechanik nicht nötig, weil der Zustand die Messwerte festlegt und umgekehrt." [22]. Quanten verfügen zumeist nicht über feste Zustände, sondern befinden sich in einer sogenannten Überlagerung aller möglichen Zustände, bis zum Zeitpunkt der Messung, dann bricht die Überlagerung zusammen und das Teilchen hat für diesen Messwert einen festen Zustand.
Zwei Teilchen im gleichen Überlagerungszustand liefern bei der Messung nicht zwingend das gleiche Ergebnis, sondern ein Ergebnis aus dem Raum der möglichen Ergebnisse nach einer Stochastischen Verteilung.
Die Messung eines Wertes zerstört die Stochastische Verteilung der anderen Werte, wodurch diese bei einer Messung einen zufälligen Wert liefern.
Quanten sind auch in der Lage sich zu "verschränken"wodurch zwei oder mehr Quanten nicht länger als einzelne Teilchen beschreibbar sind, sondern nur noch als Ganzes. Diese Verschränkung führt unter anderem dazu, dass bei einer Messung die Ergebnisse für die verschränkten Quanten korrelieren, unabhängig von deren derzeitiger Position.

2.2 Quantencomputer

Die Arbeitsweise eines herkömmlichen Computers basiert auf Bits, die einen Wert von 1 oder 0 haben können. Ein Quantencomputer arbeitet auf Basis von Qubits, die einen Wert von 1, 0 oder eine Überlagerung von 1 und 0 haben können. Zwei Bits haben 4 mögliche Werte, 11,10, 01 und 00. Hingegen haben zwei Qubits (die nur auf einem Messwert basieren) 16 mögliche Werte, aber bei einer Messung nur die 4 Werte, die auch das herkömmliche Bitpaar haben kann. Diese Überlagerungen sind der große Vorteil gegenüber den herkömmlichen Bits. Da ein Qubit die verschiedene Zustände gleichzeitig haben kann, können Rechenoperationen für jeden Zustand gleichzeitig durchgeführt werden[11].

2.3 Adiabatischer Quantencomputer

Die mathematische Grundlage für Adiabatische Quantencomputer ist der Hamiltonoperator. Ein Hamiltonoperator ist ein Energieoperator, der die möglichen Energiewerte eines Systems angibt.
Bei einem Adiabatischen Quantencomputer wird zuerst ein Hamiltonoperator gefunden, welcher mit seinem Grundzustand die Lösung des betrachteten Problems beschreibt. Anschließend wird das System mit einem einfachen Hamiltonoperator initialisiert und dieser mittels Adiabatischer Evolution in den anderen Hamiltonoperator umgewandelt. Nach dem adiabatischen Theorem, welches besagt, dass "Nummeriert man die Zustände eines Systems mit den Nummern der entsprechenden Energieniveaus,[...] dass, falls das System sich Anfangs in einem Zustand mit einer bestimmten Nummer befand, bei einer adiabatischen Änderung die Wahrscheinlichkeit des Übergangs des Systems in einen Zustand mit einer anderen Nummer unendlich klein ist. Obwohl die Energieniveaus nach der Änderung sich von ihren Anfangswerten um endliche Größen unterscheiden können"[5], verbleibt ein System dass sich in seinem Grundzustand befunden hat in seinem Grundzustand, und da der Grundzustand des komplexeren Hamiltonoperators eine Lösung des Optimierungsproblems darstellt, erhält man so eine Lösung.
Zum besseren Verständnis soll anhand der Aufgabe "suche das Minimum einer Binomischen Formel", z. B.

$$f(x) = x^2 + 2x + 3 \tag{1}$$

das Ganze beispielhaft dargestellt werden. Hier die allgemeine Form der Binomischen Formel

$$f(x) = ax^2 + bx + c \tag{2}$$

Bezogen auf die Aufgabenstellung ist a = 1, b = 2 und c = 3. Die klassische Lösungsweise wäre die Anwendung der Lösungsformel. Bei einem Adiabatischen Vorgehen jedoch würde man mit einer einfacheren Formel beginnen, z. B. mit a = 1, b = 0 und c = 0. Dies reduziert die Formel auf

$$f(x) = x^2 \tag{3}$$

Bei dieser (einfachen) Formel ist die Lösung (0) bekannt. Die Werte für a, b und c würden dann schrittweise geringfügig verändert, bis die Formel

der Problemformel entspricht. Nach dem Adiabatischen Theorem verbleibt das System dabei auf seinem minimalen Energiezustand (welcher das Minimum der Formel darstellt), solange die Änderung langsam genug vollzogen wird.

2.4 Quantenalgorithmus

So wie klassische Computer über Algorithmen verfügen, verfügen Quantencomputer über Quantenalgorithmen. Zwar sind alle herkömmlichen Algorithmen auch auf Quantencomputern lauffähig, aber Quantenalgorithmen bezeichnen solche Algorithmen, die explizit Nutzen aus den Quanteneigenschaften wie Überlagerung oder Verschränkung ziehen.
Quantenalgorithmen sind, abhängig vom Problem, zum Teil exponentiell schneller als herkömmliche Algorithmen, wodurch auch NP-harte Probleme in praktikabler Zeit gelöst werden können.
Quantenalgorithmen werden allgemein nicht als Pseudocode, sondern als Quantenschaltbild beziehungsweise als Hamiltonoperator im adiabatischen Fall dargestellt.

3 Vergleich herkömmlicher und Quantencomputer

Quantencomputer unterscheiden sich aufgrund der ihnen zu Grunde liegenden Physik stark von herkömmlichen Computern.

3.1 Deterministisch

Im Gegensatz zu herkömmlichen Computern sind Quantencomputer nicht deterministisch, was dazu führt, dass Quantencomputer, selbst bei einem korrekten Algorithmus, der zudem korrekt ausgeführt wurde, nur mit einer gewissen Wahrscheinlichkeit das korrekte Ergebnis liefern. Dieses Problem resultiert aus der Natur der den Qubits zu Grunde liegenden Quanten, welche sich nur zum Zeitpunkt einer Messung in einem einzigen Zustand befinden, ansonsten sind sie in einer Überlagerung.

3.2 Dekoherenz

Quanten ändern bei einer Messung ihren Zustand, wobei Messung ein relativ weit zu fassender Begriff ist. Bei einem Quantencomputer wird zumeist nur am Ende der Berechnung die Messung durchgeführt. Allerdings ist auch die Kollision mit einem anderen Teilchen, sei es nun ein atomares Teilchen oder ein Quantenteilchen, wie etwa elektromagnetische Strahlung, eine Messung. Dadurch können Wechselwirkungen mit anderen (nicht zum System gehörenden) Quanten Überlagerungszustände oder Verschränkungen störend beeinflussen. Dies führt zu einer deutlich stärkeren Störanfälligkeit als bei klassischen (elektrizitätsbasierten) Computern. Bei denen durch zumeist Effekte der klassischen Physik Fehler auftreten können. Bei Quantencomputern ist dieses Problem schwerwiegender, da die Fehler leichter auftreten und schwerer zu verhindern sind.
Adiabatische Quantencomputer sind deutlich toleranter gegenüber Dekoherenzeffekten als nicht-Adiabatische Quantencomputer. Da sie sich in ihrem Grundzustand befinden, können sie nicht durch äußere Effekte auf ein niedrigeres Energieniveau fallen. Mit sinkendem Energieniveau der Umgebung des Quantensystems sinkt die Wahrscheinlichkeit, dass das Quantensystem durch äußere Effekte auf ein höheres Energieniveau gehoben wird.

3.3 Skalierbarkeit

Die Skalierbarkeit von klassischen Computern ist verschiedenen Faktoren der klassischen Mechanik unterworfen, die wesentlichen sind Energiebedarf, Hitzeentwicklung und Datenübermittlungsrate. Jede Rechenoperation benötigt, abhängig von der verwendeten Technologie, eine gewisse Menge an Energie. Da diese Energie nicht vollständig genutzt werden kann entsteht Wärme, welche um die Komponenten nicht zu beschädigen, abgeführt werden muss. Quantencomputer verfügen über die gleichen Probleme wie klassische Computer, allerdings treten bei höheren Systemgrößen zusätzlich auch noch quantenmechanische Phänomene auf. Welche im System zusätzliches Rauschen erzeugen, das die Messergebnisse beinträchtigt.

3.4 Betriebsbedingungen

Herkömmliche Computer funktionieren bei Raumtemperatur und einem breiten Spektrum an Luftfeuchtigkeiten. Herkömmliche Supercomputer benötigen zumeist Temperaturen etwas unter Raumtemperatur und haben ein schmaleres Spektrum an Luftfeuchtigkeit. Ein Quantencomputer benötigt zumeist extreme Umweltbedingungen um zu funktionieren. Supraleiter basierte Systeme zum Beispiel benötigen Temperaturen nahe dem absoluten Nullpunkt, Hochvakuum und eine sehr gute elektromagnetische Abschirmung.

3.5 Parallelisierbarkeit

Bei klassischen Computern ist die Parallelisierbarkeit durch die Anzahl der Prozessorkerne bestimmt. Bei Quantencomputern ist es möglich alle Belegungen für eine gegebene Menge von Qubits Berechnungen für alle Belegungen dieser Qubits gleichzeitig durchzuführen. Dieses Maß an Parallelisierbarkeit ist einer der Hauptvorteile von Quantencomputern. Der Grad der Parallelisierbarkeit bei klassischen Computern steigt linear mit der Anzahl der Prozessorkerne, bei Quantencomputern steigt diese quadratisch mit der Zahl der Qubits.

3.6 Logic Gates

Herkömmliche Computer verfügen über Logic Gates die sich mittels der Logischen Operatoren AND, OR und NOT darstellen lassen. Quantencomputer verfügen über diese Logic Gates und weitere quantenspezifische, welche unter anderem Verschränkungen herstellen oder auflösen oder Überlagerungszustände beeinflussen.

3.7 Flexibilität

Bei einem herkömmlichen (Hochleistungs-) Rechner existiert ein vielschichtiges System, das flexible Änderungen an der verwendeten Software erlaubt. Zum Beispiel die Installation eines neuen Programms. Bei Quantencomputern ist die Durchführung einer Berechnung, die sich von der aktuellen unterscheidet schwieriger. Abhängig von der verwendeten Technologie muss das komplette System neu initialisiert werden oder es ist gar ganz unmöglich. Bei Adiabatischen Systemen ist dieses Problem weniger ausgeprägt.

4 Anwendungsgebiete von Quantencomputern

Quantencomputer sind für einige Anwendungsgebiete besonders geeignet, nachfolgend werden die wichtigsten kurz beschrieben.

4.1 Simulation von Quantenphänomenen

Klassische Computer sind ungeeignet um Quantenphänomene in Mehrteilchensystemen zu simulieren [14]. Da Quantencomputer selbst auf Quantenphänomenen basieren ist es naheliegend mit ihnen auch Quantenphänomene zu simulieren. Allerdings ist dieses Anwendungsgebiet aktuell rein theoretisch, da die real existierenden Quantencomputer noch über sehr wenig Rechenleistung verfügen.

4.2 Optimierungsprobleme

Für einen Quantencomputer gilt, wenn es möglich ist, dass jede mögliche Lösung eines Optimierungsproblems mit den gegebenen Qubits dargestellt werden kann, dann ist es auch möglich die betreffenden Qubits in eine Überlagerung aus allen möglichen Lösungen zu bringen. Oder mit anderen Worten gesagt, wenn n Qubits beliebige Instanzen einer möglichen Lösung des Optimierungsproblems O darstellen können, dann ist es auch möglich n Qubits in einen Überlagerungszustand zu bringen, welcher aus allen dieser bis zu 2^n Lösungen besteht. Operationen die mittels Quantenlogic-Gates durchgeführt werden arbeiten auf allen dieser in Überlagerung befindlichen Belegungen gleichzeitig. Adiabatische Quantencomputer können mittels Adiabatischer Evolution sehr gut Lösungen zu kombinatorischen Optimierungsproblemen finden, da diese gut mittels Hamiltonoperatoren dargestellt

werden können, welche die Grundlage von Adiabatischen Quantencomputern bilden.

4.3 Cryptographie

Bei der Quantencryptographie wird sowohl zwischen Cryptographie und Cryptoanalyse, als auch zwischen Methoden die lediglich die Rechenleistung von Quantencomputern nutzen und solchen die auf Quanteneigenschaften beruhen, unterschieden.

4.3.1 Cryptoanalyse

Quantencomputer sind (theoretisch) dazu in der Lage Primfaktorzerlegungen von großen Zahlen (600 Stellen und mehr) in einem Bruchteil der Zeit (bis zu 15 Größenordnungen schneller) durchzuführen. Was die Sicherheit von Cryptoalgorithmen wie RSA und DSA beeinträchtigt. Ähnliches gilt auch für andere Cryptoalgorithmen die auf Falltürfunktionen basieren. Allerdings sind aktuelle Algorithmen und Quantencomputer noch weit davon entfernt die derzeitigen Cryptoalgorithmen zu bedrohen. Mittels Adiabatischer Quantencomputer ist es aktuell möglich 5 stellige Zahlen in ihre zwei Primfaktoren zu zerlegen. Allerdings benötigt dieser Algorithmus lediglich 4 Qubits. Dies ist eine weit geringere Zahl an Qubits als derzeit in Quantencomputern zur Verfügung stehen. Jedoch verfügen Quantencomputer und Algorithmen über eine schlechte Skalierbarkeit[3].

Auch gibt es immer noch viele Verschlüsselungsalgorithmen, die selbst mit Quantencomputern nicht deutlich schneller gelöst werden können als mit herkömmlichen Hochleistungsrechnern. Dies kann sich ändern, wenn effizientere Algorithmen dazu gefunden werden. Bei einigen der derzeit verwendeten Algorithmen ist es auch so, dass die erwartete Beschleunigung durch Quantencomputer gering genug ist, so dass eine Erhöhung der Schlüssellänge ausreicht um hinreichende Sicherheit zu garantieren[16][6].

4.3.2 Quantencryptographie

Quantencryptographie existiert aktuell nur in einer rein theoretischen Form. Die Datenübermittlung mittels eines Quantenstroms ist prinzipiell möglich, wobei solche Verfahren eine direkte Verbindung zwischen Sender und Empfänger benötigen. Der Quantenstrom garantiert, aufgrund der physikalischen Eigenschaften von Quanten, dass er nicht unbemerkt abgehört werden kann, da ein Abhören eine Messung voraussetzt und Quanten bei einer Messung ihren Wert ändern. Kommunikation mittels Quantenverschränkung oder Quantenteleportation ist ebenso theoretisch möglich und aufgrund ihrer instantanen Natur auch für Hochleistungsrechner interessant, da physisch getrennte Teile eines Systems somit ohne Zeitverlust und über beliebige Entfernungen kommunizieren können.

5 Aktuelle Entwicklungen

Als Nächstes werden aktuelle Entwicklungen sowohl bei der Hard-, als auch bei der Software aufgezeigt.

5.1 Hardware

Bei der Hardware wird hier zwischen Adiabatischen und nicht-Adiabatischen Quantencomputern unterschieden. Bei jeder der Technologien wird zunächst erklärt, wie die Qubits erzeugt werden, gefolgt von dem aktuellen bzw. neuesten Stand der Entwicklung.

5.1.1 D-Wave

Der derzeit einzige Anbieter von kommerziellen Quantencomputern D-Wave hat dieses Jahr den D-Wave 2X auf den Markt gebracht. Dieser bietet mehr als 1000 nutzbare Qubits, wobei die genaue Anzahl bei jedem Chip anders ist. Beim D-Wave 2X handelt es sich, laut Herstellerangaben, um einen Adiabatischen Quantencomputer. Allerdings gibt es einige Experten die bestreiten, dass es sich bei den Produkten von D-Wave wirklich um Quantencomputer handelt. Die experimentellen Daten, die vorliegen, sind widersprüchlich.

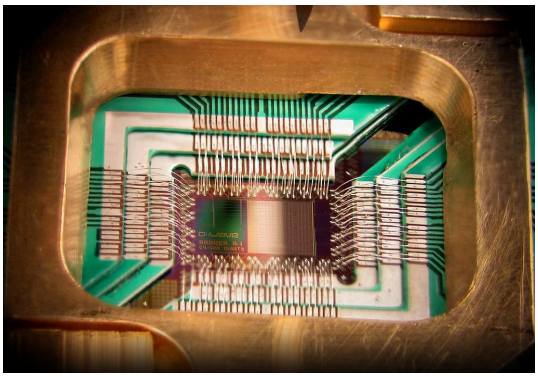

Abbildung 1: D-Wave 128 Qubit Chip

In einer Studie aus dem Jahr 2014[20] wurde keine Beschleunigung durch Quanteneffekte nachgewiesen, wenn der gesamte Datensatz betrachtet wird und es gab uneindeutige Ergebnisse für einen Vergleich nach Fall bei Fall Basis. Die Studie weist allerdings darauf hin, dass diese Ergebnisse auch an der Wahl ihres zum Benchmarking genutzten Problems liegen können. Andere Studien kommen für das Vorgängermodell zu anderen Ergebnissen[4]. Ganz aktuell gab es ein Paper[9] sowie eine Pressemitteilung von Google und der NASA, dass sie beweisen können, dass dieser Quantencomputer funktioniert . Die unabhängige wissenschaftliche Überprüfung steht allerdings noch aus.

5.1.2 nicht Adiabatische Technologien

- Ionenfallen: Einer der Ansätze für Quantencomputer basiert auf Ionenfallen. Bei diesem Ansatz werden Qubits durch den elektronischen Zustand gefangener Ionen gebildet und mittels Coulomb Interaction verbunden. Für diesen Typ von System wurden die für Quanten Berechnungen nötigen elementaren Eigenschaften bewiesen, aber es existieren theoretische und technische Probleme die das Skalieren für größere Systeme schwierig machen[12].

  Der aktuelle Stand ist ein 14 Qubit System, das von Blatt et. al. gebaut wurde. Es existieren theoretische Ansätze für Systeme die gut skalierbar sind[2].

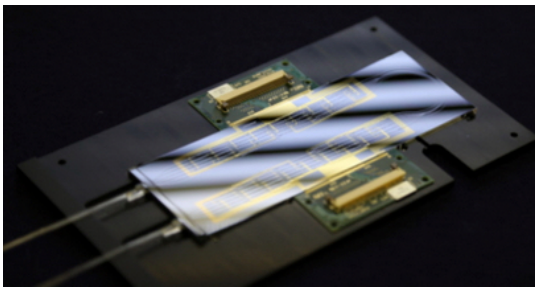

Abbildung 2: Photo des Linear Optics Processor (credit: University of Bristol)

- Kernspin: Kernspin basierte Systeme nutzen den Spin verschiedener Atome eines Moleküls als Qubits. Kernspin Systeme sind allerdings noch schlechter skalierbar als andere Quantencomputer Technologien. Das 12 Qubit System das vom Perimeter Institute for Theoretical Physics im Jahre 2006 gebaut wurde, ist das derzeit am weitesten entwickelteste basierend auf Kernspin[18].

- Photonen:

  Photonen basierte Systeme arbeiten mittels der Polarisierung einzelner Photonen. Photonen haben wenig Dekoherenz Probleme und Photonen basierte Systeme lassen sich zumindest theoretisch gut skalieren. Aktueller Stand der Technik ist ein 6 Qubit Chip, der sich, im Vergleich zu anderen Quantentechnologien, einfach und schnell programmieren lässt [7]. Der Aufbau des Chips ist in Abbildung 3 zu erkennen.

- Supraleiter: Supraleiter basierte Quantencomputer nutzen supraleitende Ringe als Qubits. Diese haben verschiedene Vorteile, zum einen eine relativ geringe Dekoherenz, zum anderen sind die zu ihrer Herstellung nötigen Techniken schon, aus der klassischen Elektrotechnik, recht weit entwickelt. Der aktuelle Stand der Technik im Fall der Supraleiter basierten Systeme der 4 Qubit Chip von IBM, bei dem al-

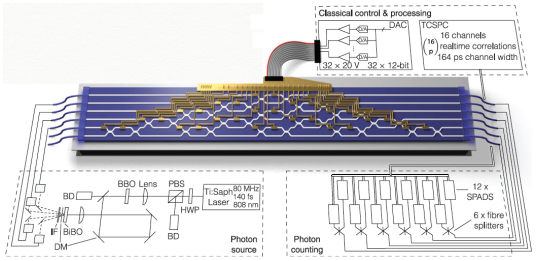

Abbildung 3: Schematische Darstellung des Linear Optic Processors

lerdings nur 2 Qubits für die Berechnung bereitstehen und die anderen Zwei zur Fehlerdetektion dienen, dies ist gut in Abbildung 4 zu erkennen. Mit diesem Chip aus dem Jahre 2015 ist es möglich sowohl Bit-Flip als auch Phase-Flip Quantenfehler zu erkennen (simultan). Diese Möglichkeit zur Fehlererkennung (und damit Korrektur) ist ein wichtiger Schritt hin zu größeren Quantencomputern [10].

- Anyonen: Anyonen sind zweidimensionalen Quasipartikel, welche einen "Zopf"bilden können, dessen Topologie als Qubit genutzt werden kann. Es existieren theoretische Modelle, Quantencomputer basierend auf Anyonen zu konstruieren. Diese Modelle sind allerdings rein theoretisch, da die zuverlässige Erzeugung und Manipulation von Anyonen noch in einem genauso theoretischen Stadium ist. Anyonen basierte Systeme hätten den Vorteil, dass die Topologie eines Anyonen Zopfes wesentlich stabiler ist als die meisten anderen Eigenschaften von einzelnen Quanten, wodurch Dekoherenzeffekte aufgrund schwacher Außeneffekte verhindert werden. [8][17].

5.2 Software

Bei Quantenalgorithmen ist bei aktuellem Stand nicht die Entwicklung neuer Algorithmen wichtig, sondern die praktische Umsetzung bekannter Algorithmen, da viele theoretische Algorithmen für

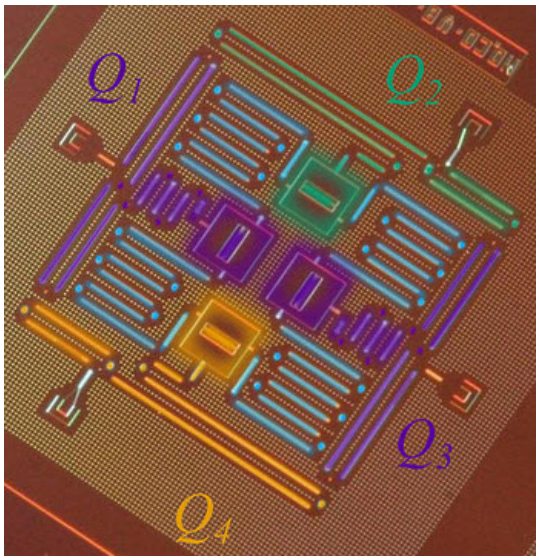

Abbildung 4: Photo des 4 Qubit Chips von IBM, mit farblich hervorgehobenen Elementen, Q1 und Q3 sind die Code Qubits, Q2 und Q4 sind die Fehlerdetektions-Qubits

Quantencomputer existieren, die meisten von ihnen stammen aus den 80er und 90er Jahren des letzten Jahrhunderts.

5.2.1 Shor-Algorithmus

Der Shor-Alortihmus liefert, meistens, einen nichttrivialen Teiler der Eingabe zurück. Dafür benötigt er mindestens log(n) Qubits, wobei n die Anzahl der Stellen der Eingabe ist.
Die derzeitige praktische Umsetzung des Shor-Algorithmus liegt allerdings weit hinter dem theoretisch Möglichen zurück. Erfolgreiche Faktorisierungen wurden für die Zahlen 15 und 21 durchgeführt [21].

5.2.2 Grover-Algorithmus

Der Grover-Algorithmus ist als ein Datenbanksuchalgorithmus konzipiert. Er liefert im Gegensatz zu vielen anderen Quantenalgorithmen lediglich eine quadratische Beschleunigung gegenüber

herkömmlichen Computern im Gegensatz zu exponentiellen Beschleunigungen. [15].

5.2.3 Adiabatische Algorithmen

Nachdem es zu allen nicht-Adiabatischen Quantenalgorithmen einen Adiabatischen Algorithmus gibt, der polynominell äquivalent ist [1], ist es möglich alle nicht Adiabatischen Algorithmen auch auf einem Adiabatischen Quantencomputer umzusetzen. Allerdings liegt die Stärke Adiabatischer Quantencomputer in der Lösung von kombinatorischen Optimierungsproblemen[13]. Eine Implementierung eines Primfaktorzerlegungsalgorithmus für bis zu 5 stellige Zahlen (derzeit der am weitesten fortgeschrittene Quantenalgorithmus zur Primfaktorzerlegung) existiert ebenfalls. [19].

6 Schluss

Das Feld der (adiabatischen) Quantencomputer steckt noch in den Kinderschuhen, keiner der derzeit real existierenden Quantencomputer kann mit derzeitigen Hochleistungsrechnern mithalten. Die meisten liegen mit ihrer Leistung weit unter der eines handelsüblichen Mobiltelefons. Allerdings steckt sehr viel Potential in Quantencomputern und die derzeitigen Entwicklungen, besonders im Bereich der Photonen, Supraleiter und Adiabatischen Quantencomputer zeigen vielversprechende Erfolge, welche wichtige Grundbausteine für zukünftige Technologien darstellen. Photonen basierte Quantencomputer verfügen über einen frei programmierbaren Quantenchip, Supraleiter basierte verfügen über effektive Fehlerdetektion und Adiabatische Quantencomputer über eine hohe Zahl an Qubits (falls D-Wave kein Schwindel ist). Jede dieser Entwicklungen ist ein wichtiger Grundbaustein für einen nutzbaren Quantencomputer. Leider baut jede dieser Entwicklungen auf einer anderen Technologie auf. Welche dieser Technologien am Ende das Rennen macht, falls überhaupt eine (allein), wird nur die Zukunft zeigen.

Literatur

[1] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM Journal of Computing, Vol. 37, Issue 1, p. 166-194 (2007), conference version in Proc. 45th FOCS, p. 42-51 (2004).*

[2] J M Amini, H Uys, J H Wesenberg, S Seidelin, J Britton, J J Bollinger, D Leibfried, C Ospelkaus, A P VanDevender, and D J Wineland. Simulating physics with computers. *New Journal of Physics*, Maerz 2010.

[3] Daniel J. Bernstein. *Introduction to post-quantum cryptography.* 2009.

[4] Sergio Boixo, Troels F. Rnnow, Sergei V. Isakov, Zhihui Wang, David Wecker, Daniel A. Lidar, John M. Martinis, and Matthias Troyer. Evidence for quantum annealing with more than one hundred qubits. *Nature Physics 10, 218224 (2014)*, 2014.

[5] M. Born and V. Fock. Beweis des adiabatensatzes. *Zeitschrift fr Physik*, Maerz.

[6] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *The Royal Society*, 1998.

[7] Jacques Carolan, Christopher Harrold, Chris Sparrow, Enrique Martn-Lpez, Nicholas J. Russell, Joshua W. Silverstone, Peter J. Shadbolt, Nobuyuki Matsuda, Manabu Oguma, Mikitaka Itoh, Graham D. Marshall, Mark G. Thompson, Jonathan C. F. Matthews, Toshikazu Hashimoto, Jeremy L. OBrien, and Anthony Laing. Universal linear optics. *Science,Vol. 349 no. 6249 pp. 711-716*, August.

[8] Graham P. Collins. Computing with quantum knots. *SCIENTIFIC AMERICAN*, April 2006.

[9] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. Martinis, and H. Neven. What is the Computational Value of Finite Range Tunneling? *ArXiv e-prints*, December 2015.

[10] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting Qubits: A Short Review. *eprint arXiv:cond-mat/0411174*, November 2004.

[11] D. P. Divincenzo. Quantum Computation. *Science*, 270:255–261, October 1995.

[12] Eltony and Amira M. (Amira Madeleine). Scalable trap technology for quantum computing with ions. *Massachusetts Institute of Technology. Department of Electrical Engineering and Computer Science*, 2015.

[13] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. 2000.

[14] Feynman and Richard P. Simulating physics with computers. *International Journal of Theoretical Physics, Volume 21, Issue 6-7, pp. 467-488*, Juny 1982.

[15] Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, page 212, Mai 1996.

[16] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[17] Chetan Nayak, Steven H. Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys. 80, 1083 (2008).*, Maerz 2008.

[18] C. Negrevergne, T. S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D. G. Cory, and R. Laflamme. Benchmarking Quantum Control Methods on a 12-Qubit System. *Physical Review Letters*, 96(17):170501, May 2006.

[19] Oxford University) Nikesh S. Dattani (Kyoto University and Nathaniel Bryans (University of Calgary). Quantum factorization of 56153 with only 4 qubits.

[20] Troels F. Rnnow, Zhihui Wang, Joshua Job, Sergio Boixo, Sergei V. Isakov, David Wecker, John M. Martinis, Daniel A. Lidar, and Matthias Troyer. Defining and detecting quantum speedup. *Science 345, 420 (2014)*, 2014.

[21] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput. 26 (1997) 1484*, 1997.

[22] various Authors, 6.12.2015,14:30. https://de.wikipedia.org/wiki/Quantenmechanik.