Quantum Computing, eine Anleitung

Samuel L. Braunstein

Abstrakt:

Stell dir einen Computer vor, wessen Speicherfähigkeit seine Physikalische Größe bei weitem überschreitet; einen Computer, welcher mehrere Aufgaben gleichzeitig bearbeiten kann; ein Computer, welcher in der Dämmerungszone des Hilbert raumes berechnet. Dann würdest du an einen Quantencomputer denken. Sehr wenige und sehr simple Konzepte sind notwendig, um Quantencomputer möglich zu machen. Die Subtilität bestand darin zu lernen diese Konzepte zu manipulieren. Ist dieser Computer unvermeidlich oder ist er doch zu schwer zu bauen?

In diesem Papier werde ich eine Anleitung geben wie wir Quanten Mechanik nutzen können, um unser computing zu verbessern. Unsere Herausforderung: das lösen eines exponentiell schwierigen Problems für normale Computer – das Fabrizieren einer gigantischen Nummer. Als Einstieg, betrachten wir die standartwerkzeuge im computing, universelle Tore und Maschinen.

Diese Ideen werden dann zuerst an klassischen Computern, dissipationlosen Computern und dann an Quanten Computern. Ein schematisches Modell eines Quanten Computers sowie ein paar Feinheiten im Programmieren. Der Shor Algorithmus [1,2] für das effiziente fabrizieren von großen Zahlen ist aufteilt in 2 Schritte: die Quanten Prozedur innerhalb des Algorithmus und des klassischen Algorithmusses der den Quanten Prozess einleitet. Die mathematische Struktur des Fabrizierens des Shor Algorithmus wird besprochen. Wir schließen mit einem Ausblick auf die Umsetzbarkeit und die Aussicht auf Quantenberechnung in den kommenden Jahren ab.

Beginnen wir indem wir das vorliegende Problem beschreiben: Fabrizieren einer Nummer N in seine Hauptfaktoren (Die Zahl 51688 wird zerlegt als $2^3 \times 7 \times 13 \times 71$). Ein sehr bequemer Weg, um zu quantifizieren wie schnell ein bestimmter Algorithmus ist, kann sein ein Problem zu lösen, zu fragen, wie viele Schritte benötigt werden zum Vervollständigen des Algorithmusses der mit der Größe der Eingaben (Input) skaliert, die diesen zugeführt werden.

Für das Fakturisierungsproblem, diese Eingabe ist die Nummer N welche wir fakturieren wollen; die Länge der Eingabe ist $\log N$. (Die Basis dieses Logarhytmus ist abhängig von unserem System. Eine Basis von 2 gibt uns eine binäre länge; einer Basis von 10 dezimalen) `Reasonable' Algorithmen sind die als ein Polynom kleinen Grades in der Eingabegröße mit einem Grad von 2. Oder 3.

Auf normalen Computern läuft der beste Fabrizierungs Algorithmus in $O\left(\exp\left[(64/9)^{1/3}(\ln N)^{1/3}(\ln \ln N)^{2/3}\right]\right)$ Schritten [3].

Dieser Algorithmus, skaliert daher exponentiell mit der Eingabegröße $\log N$. Zum Beispiel, in 1994 eine 129 stellige Nummer (bekannt als RSA129 [3']) wurde sie erfolgreich faktorisiert mit Schätzungsweise 1600 Arbeitsstationen; die gesamte Faktorisierung brauchte 8 Monate [4].

Wenn wir das verwenden, um den obigen Faktor in der exponentiellen Skalierung abzuschätzen, würde dies ungefähr 800.000 Jahre dauern, eine 250 stellige Zahl mit derselben Computerleistung zu faktorisieren; ähnlich, eine 1000 stellige Zahl würde benötigen 10^{25}Jahre (Sehr viel länger als das Alter des Universums). Die Schwierigkeit große Zahlen zu faktorisieren ist sehr wichtig Kryptosysteme welche einen öffentlichen Schlüssel nutzen, wie es zum Beispiel bei Banken der Fall ist. Solche Codes sind abhängig von der Schwierigkeit des Faktorisierens von Nummern mit um den 250 stellen.

Neulich, wurde ein Algorithmus entwickelt für das Faktorisieren von Nummern auf einem Quanten Computer welcher $O(\log N^{2+\varepsilon})$ läuft, Schritte wo ε klein ist [1].

Das ist ungefähr quadratisch in der Eingabe, also würde das faktorisieren einer 1000 Stellen Nummer mit einem solchen Algorithmus nur wenige Millionen schritte benötigen. Die Implikation ist, das Kryptosysteme mit einem Öffentlichen Schlüssel, die auf Factoring basieren, geknackt werden könnten.

Um dir eine Idee zu geben wie diese Exponentielle Verbesserung möglich sein könnte, werden wir uns ein Elementares Quanten Mechanik Experiment anschauen welches uns demonstrieren wird wo solche Power versteckt liegen könnte [5].

Das zwei Schlitzige Experiment ist ein Prototyp für das Oberservieren von Quanten mechanischem Verhalten: Eine Quelle von emittierten Photonen, Elektronen oder anderen Partikeln die paarweise ankommen.

Diese Partikel erleben eine vereinigende Evolution und endgültiges messen. Wir sehen ein Interferenz Muster, mit beiden offenen Schlitzen, welche komplett verschwinden, wenn einer der Schlitze abgedeckt ist.

Die Partikel passieren die Schlitze also sozusagen parallel. Wenn eine solche Einheitliche Berechnung (oder Operation innerhalb von einer Berechnung) stattfinden würde, würde das Quantensystem solche Berechnungen parallel durchführen.

Quanten Parallelismus kommt kostenlos. Die Ausgabe dieses Systems würde durch die konstruktive Interferenz zwischen Parallelen Berechnungen gegeben sein.

Deutsch version dank an bestenwettanbieter.net