

Here you can insert the title of your seminar paper

Ben Konrad Meyer Mike Springer
Kai Kawamura Julian Heidenreich

Modul: Verteilte Systeme

Lecturer: Name of the lecturer

February 26, 2025

Abstract

This template can be used for seminar papers. For more tips and tricks regarding the use of figures, tables, quotations, references, footnotes, enumerations, etc. please download the Masterthesis template.

Contents

1	Einleitung	2
1.1	Drei Prinzipien des Quanten Computing	3
1.2	Verschränkung	3
1.3	Quantengatter & Quantenschaltkreise	5
1.4	Umkehrbare Berechnungen	7
1.5	Gestörte Berechnungen	8
1.6	Grenzen	9
1.6.1	NP-vollständige Probleme	9
1.6.2	Die perfekte Uhr	9
1.7	Zukunft	10
1.7.1	Quantum Machine Learning	10
1.7.2	Simulationen	11

1 Einleitung²

1.1 Drei Prinzipien des Quanten Computing

Zusammenfassend lässt sich Quanten Computing auf 3 wesentliche Prinzipien herunterbrechen.

•Prinzip 1 - **Das Quantenregister**: Ein Quantenregister, das aus n -Qubits besteht, wird durch einen 2^n -dimensionalen Vektorraum über komplexen Zahlen beschrieben. Der Zustand eines solchen Registers ist eine Überlagerung (Superposition) aller möglichen Basiszustände. Das bedeutet, dass das Register eine Kombination vieler möglicher Werte gleichzeitig annehmen kann. Diese Fähigkeit der Superposition ist eine der Hauptstärken von Quantencomputern, da sie es ermöglichen, mehrere Berechnungen parallel durchzuführen.

•Prinzip 2 - **Rechenschritte**: Rechenschritte in einem Quantencomputer basieren auf unitären Transformationen. Diese Transformationen sind umkehrbar, was bedeutet, dass die Berechnung ohne Informationsverlust rückgängig gemacht werden kann. Jede Operation kann lokal beschrieben werden, wobei nur zwei Qubits gleichzeitig beteiligt sind. Diese Reversibilität der Rechenschritte stellt einen fundamentalen Unterschied zu klassischen Computern dar, bei denen Informationen während der Berechnung verloren gehen können.

•Prinzip 3 - **Messungen**: Misst man den Zustand eines Quantenregisters, so erhält man als Ergebnis einen der Basiszustände mit einer Wahrscheinlichkeit, die aus der Amplitude dieses Zustands abgeleitet werden kann. Die Messung verändert den Zustand des Systems auf den gemessenen Wert, so dass die ursprüngliche Superposition zerstört wird.

In diesen Prinzipien unterscheidet sich das Quanten Computing wesentlich von klassischen Computern.

1.2 Verschränkung

Eine der interessantesten Eigenschaften von Quantenregistern ist die Verschränkung. Bei der Verschränkung teilen sich zwei Qubits denselben Zustand. Das heißt, messen wir den Zustand von Qubit 1, wissen wir auch sofort den Zustand von Qubit 2, ohne dieses gemessen zu haben. Und was das Ganze noch faszinierend macht: Selbst über große Entfernungen zwischen den verschränkten Qubits bleibt die Eigenschaft der Verschränkung erhalten. Dies bildet auch die Grundlage für die Quanten-Teleportation, auf die wir später noch zurückkommen.

Kommentar

Die Verschränkung war mir bisher ein unbekanntes Konzept, welches sich nur sehr schwer greifen lässt. Dementsprechend schwierig war es auch, die Verschränkung zu verstehen und in eigenen Worten zu erklären. Besonders, dass diese unabhängig von der räumlichen Entfernung der Qubits erhalten bleibt.

Dazu half mir ein kleines Beispiel: Stellen wir uns zwei Würfel vor, einen roten Würfel und einen blauen Würfel. Der blaue Würfel zeigt immer dieselbe Augenzahl wie der Rote. Wenn wir nun mit dem Roten würfeln und dieser eine 6 zeigt, wissen wir auch, dass der Blaue eine 6 zeigt, ohne diesen gewürfelt zu haben. Und das unabhängig davon, wie weit die beiden Würfel voneinander entfernt sind.

Wie erzeugen wir eine solche Verschränkung? Dazu betrachten wir exemplarisch ein Zwei-Bit-Register $|b_1b_2\rangle$ im Zustand $|00\rangle$. Wir wenden auf das erste Bit die Hadamard-Transformation an und anschließend auf beide Bits die Operation CNOT.

$$CNOT : |x, y\rangle \rightarrow |x, y \oplus x\rangle \quad (1)$$

Das ergibt:

$$|00\rangle \xrightarrow{H \otimes I_2} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \quad (2)$$

$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (3)$$

Wenn wir nun das erste Bit messen, kommt mit einer Wahrscheinlichkeit 50% das Ergebnis $|0\rangle$ mit dem Folgezustand $|00\rangle$ und mit einer Wahrscheinlichkeit von 50% das Ergebnis $|1\rangle$ mit dem Folgezustand $|11\rangle$ heraus. Wir wissen also nach der ersten Messung schon, bevor wir das zweite Qubit überhaupt gemessen haben, wie der Endzustand des Quantenregisters ist. Und wie bereits zuvor erwähnt, bleibt diese Eigenschaft bei räumlicher Trennung der Qubits erhalten. Hierbei ist auch zu erwähnen, dass es egal ist, welches der Qubits zuerst gemessen wird oder ob diese überhaupt gleichzeitig gemessen werden.

Sei $|\phi\rangle$ der Zustand eines Quantenregisters aus n Bits. Der Zustand $|\phi\rangle$ heißt *unverschränkt*, wenn er das Produkt von Zuständen der einzelnen Bits ist:

$$|\phi\rangle = |\phi_{n-1}\rangle \otimes |\phi_{n-2}\rangle \otimes \dots \otimes |\phi_0\rangle.$$

Ein Zustand heißt *verschränkt*, wenn es keine solche Zerlegung gibt.

Figure 1: Definition Verschränkung

Diesen Zustand nennt man auch Bell-Zustand. Es gibt insgesamt 4 solcher Bell-Zustände. Diese beschreiben verschränkte Bits mit einer starken Kopplung (maximal verschränkt).

Daraus resultierend gibt es auch Verschränkungen mit einer weniger starken Kopplung. Ein solcher Zustand könnte beispielsweise so aussehen:

$$|\phi\rangle = 0.9 |00\rangle + 0.1 |11\rangle \quad (4)$$

Hier sind die Qubits auch wieder miteinander verschränkt, allerdings sind die Wahrscheinlichkeiten für die Messergebnisse ungleich verteilt. Das heißt, wir bekommen mit einer Wahrscheinlichkeit von 90%, also sehr sicher, den Zustand $|00\rangle$ und nur mit 10% den Zustand $|11\rangle$, also unsicher. Diese weniger stark gekoppelten Qubits kommen in der Praxis häufiger vor, etwa durch äußere Einflüsse wie Rauschen oder Dekohärenz auf ehemals maximal verschränkte Qubits. Das geht mit Leistungseinbußen einher, weshalb versucht wird, den Zustand der maximalen Verschränkung möglichst lange zu erhalten.

1.3 Quantengatter & Quantenschaltkreise

„Klassische Schaltkreise bestehen aus Leitungen und Gattern. Ganz analog bestehen Quantenschaltkreise aus Quantenleitungen und Quantengattern. Jede Quantenleitung entspricht einem Quantenbit und ein Quantengatter führt eine unitäre Transformation aus.“

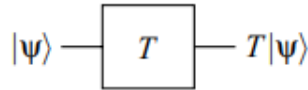


Figure 2: Quantenschaltkreis

Wenn wir eine Berechnung mit mehreren Qubits ausführen, ergibt sich der Endzustand $|x, y, z\rangle$ aus dem Tensorprodukt der einzelnen Gatter:

$$(I_2 \otimes W \otimes I_2)(U \otimes V) |x, y, z\rangle \quad (5)$$

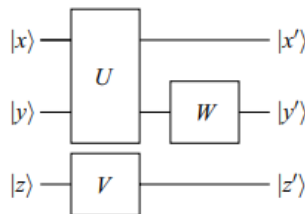


Figure 3: Quantenschaltkreis mit Tensorprodukt

Da bei Quantenschaltkreisen die Umkehrbarkeit der Berechnungen garantiert werden muss, ist die Summe der Eingabe-Qubits = Summe der Ausgabe-Qubits und pro Gatter dürfen höchstens 3 Qubits einbezogen werden. Um dies zu gewährleisten, nutzen wir das Toffoli-Gatter, welches im nächsten Kapitel erläutert wird. Außerdem können Qubits nicht kopiert werden, deshalb dürfen sich die Quantenleitungen nicht verzweigen und das Ergebnis eines Gatters nicht mehrfach verwendet werden. Auf den Grund dafür kommen wir später nochmal zurück.

Eine der wichtigsten Operationen in der Quanteninformatik ist die Negation, genauer die kontrollierte Negation CNOT. Dieses Gatter wird für alle Quantenoperationen benötigt, so zum Beispiel bei der Verschränkung. Darstellen lässt es sich wie folgt:

$$CNOT : |x, y\rangle \rightarrow |x, y \oplus x\rangle \quad (6)$$

oder als Matrix:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (7)$$

Dieses CNOT-Gatter negiert nur dann das zweite Qubit, wenn das erste Qubit im Zustand $|1\rangle$ ist.

Weitere wichtige Operationen sind die Hadamard-Transformation, die wir bereits kennen, sowie die Pauli-Matrizen. Die Pauli-Matrizen negieren ebenfalls, mithilfe einer unitären Transformation auf einem Bit. Die bekannteste ist der „Bitflip“ X:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (8)$$

Die zwei weiteren Pauli-Matrizen sind der „Phasenflip“ Z:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (9)$$

und der „Y-Flip“ Y:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (10)$$

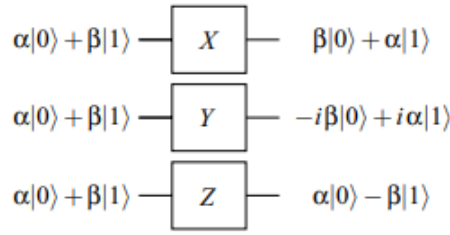


Figure 4: Pauli-Matrizen

Durch die Kombination dieser drei Gatter CNOT, Hadamard-Transformation, sowie Pauli-Matrizen lassen sich alle Quantenberechnungen abbilden. Sie bilden die grundlegendsten Rechenoperationen eines Quantencomputers. Mit einem wesentlichen Unterschied zu logischen Gattern: bei diesen lässt sich der Endzustand nicht unbedingt wieder in den Anfangszustand überführen. Bei Quantengattern ist dies eine zwingende Voraussetzung, sie müssen umkehrbar sein.

1.4 Umkehrbare Berechnungen

Wie bereits zuvor erwähnt, muss jede Rechenoperation eines Quantencomputers umkehrbar sein. Es dürfen also keine Informationen gelöscht werden, wie es beispielsweise bei der Anwendung einer logischen AND-Operation passiert: aus zwei Eingabewerten wird ein Ausgabewert kombiniert. So folgt aus $1 \text{ AND } 0 = 0$, jedoch ebenfalls aus $0 \text{ AND } 0 = 0$. Sehen wir den Endzustand 0, wissen wir also nicht, welchen Zustand die beiden Bits zu Beginn hatten. Das bedeutet, wir können Quantenrechenprozesse nicht auf dieselbe Art verarbeiten wie klassische Rechenprozesse.

Allerdings kann jede klassische Operation in eine umkehrbare Operation umgewandelt werden. Veranschaulichen wir uns dies anhand des Toffoli-Gatters.

Das Toffoli-Gatter ist ein universelles, umkehrbares Gatter, welches AND, OR und NOT Operationen ersetzen kann. Es besteht aus drei Eingabebits a , b , c und drei Ausgabebits a , b und $c \oplus (a \wedge b)$:

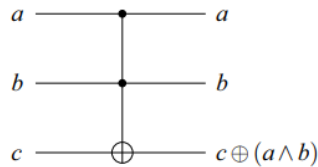


Figure 5: Toffoli-Gatter

Exemplarisch für AND: Wollen wir zum Beispiel ein Bit negieren, mit der Eingabe $(a, b, c) = (1, 1, 0)$. Dann ergibt die Rechnung über das Toffoli-Gatter $(1, 1, 1)$, denn $(1 \wedge 1) \oplus 0 = 1$. Hier ist nun auch zu sehen, dass die Berechnung

umkehrbar ist, wenn wir die Schritte einmal rückwärts gehen. Dies ist genauso für die anderen Operatoren möglich, bedarf gegebenenfalls nur Umformung und den Einsatz mehrerer Toffoli-Gatter.

Auf diese Weise können wir jede klassische Rechenoperation umkehrbar gestalten, sodass diese auch für unsere Quantenschaltkreise nutzbar sind.

1.5 Gestörte Berechnungen

Wie wir bisher sehen konnten, scheint alles, was wir mit klassischen Computern berechnen, genauso effizient mit Quantencomputern berechenbar. Warum also steht nicht bei jedem ein Quantenrechner zu Hause (wenn wir die Kosten mal außen vor lassen)?

Einer der Gründe dafür ist die Fehleranfälligkeit. Während klassische Bits die Zustände 0 oder 1 abbilden, können Quantenbits bis zur Messung $|0\rangle$ oder $|1\rangle$ oder beide Zustände gleichzeitig annehmen. Verdeutlichen wir, was das in der Praxis bedeutet: Nehmen wir an, der Zustand 0 eines klassischen Bits wird durch 0V und der Zustand 1 durch 5V dargestellt. Nun kann es zu Spannungsschwankungen kommen und wir geben 4V statt 5V. Da wir aber keinen Zustand für 4V haben, aber nur 2 Zustände abbilden können, können wir auch sagen, der Zustand 0 wird durch eine Spannung $<2,5V$ abgebildet und der Zustand 1 durch $>2,5V$. So liefert der Rechner uns auch weiterhin ein zuverlässiges Ergebnis, trotz Störung.

Die ist allerdings nicht für Quantenbits möglich, da wir nicht nur diese zwei Zustände abbilden. Was bedeutet also hier eine Spannungsschwankung von 5V auf 4V? Das wissen wir nicht, da bis zur Messung der Zustand nicht feststeht, so können wir also auch kein zuverlässiges Ergebnis mehr liefern. So können selbst kleinste Störungen Quantenberechnungen verfälschen. Zu beachten ist, dass bei einem gestörten Quantengitter sich der Fehler nur addiert. Das heißt, der Fehler eines Gatters bleibt zwar in weiteren Berechnungen erhalten, jedoch wird er nicht größer.

Würden wir zum Beispiel ein Qubit durch 3 Quantengatter nacheinander umformen, wobei jedes dieser Gatter einen Fehler von 2% hinzufügt, so beträgt der Fehler des Endzustands 6%. Das heißt, bei 50 Quantengattern, welche einen Fehler von 2% hinzufügen, beträgt der Fehler des Endzustands 100%. Wenn die Fehler nun aber exponentiell wachsen würden, hätten wir nach 3 Gattern einen Fehler von 8%, nach 50 Gattern (theoretisch) einen Fehler von $2^{50}\%$.

Um die Frage vom Beginn des Kapitels nochmal aufzunehmen: Einer der Gründe weshalb nicht jeder einen Quantencomputer zu Hause stehen hat, ist die Fehleranfälligkeit der Berechnungen. Es bedarf großen Aufwands solche Fehler zu vermeiden und zu korrigieren.

1.6 Grenzen

Angenommen in 10 Jahren ist das Problem der Dekohärenz gelöst, werden Quanten Computer die Lösung aller mathematischen Probleme sein? Obwohl Quanten Computing noch mitten in der Entwicklung stecken, lässt sich jetzt schon absehen: Die Antwort darauf ist „Nein“.

1.6.1 NP-vollständige Probleme

Eine der zentralen Fragen der Komplexitätstheorie beschäftigt sich mit NP-vollständigen Problemen. Sie beschreibt Probleme, welche sich zwar leicht überprüfen lassen, doch algorithmisch mindestens eine exponentielle ($O(2^n)$), häufig sogar faktorielle ($O(n!)$) Laufzeit haben. Und würde man für ein NP-vollständiges Problem eine Lösung finden, also ein Algorithmus mit polynomieller $O(n^x)$ Laufzeit, so könnten alle dieser Probleme darauf umgeformt und gelöst werden.

Doch selbst Quantencomputer scheinen keine Lösung für diese Probleme finden zu können. Das liegt daran, dass selbst Quantenalgorithmien, wie etwa der bekannte Shor-Algorithmus (zur Faktorisierung großer Zahlen), oder der Grover-Algorithmus (zur unstrukturierten Suche in Datenbanken), zwar eine deutliche Geschwindigkeitsverbesserung im Vergleich zu klassischen Algorithmen bieten, jedoch keine exponentielle Reduktion der Komplexität bei NP-vollständigen Problemen ermöglichen. Hier stoßen Quantencomputer also auf dieselben grundlegenden Herausforderungen wie klassische Computer.

Kommentar

Wir hatten zunächst überlegt, den Grover- oder Shor-Algorithmus genauer zu beleuchten, haben uns dann aber dagegen entschieden, da wir uns auf die Grundlagen des Quanten Computing konzentrieren und uns nicht in einem komplexen Algorithmus verlieren wollten.

Als wir mit dem Thema und der Recherche zur Quanteninformatik begonnen haben, war mir nicht bewusst, dass selbst Quantencomputer, welche noch in den Anfängen stecken und ein großes Potenzial bieten, schon jetzt an Grenzen stoßen, wie bei den NP-vollständigen Problemen. Es ist faszinierend zu sehen, dass selbst Quantencomputer, eine Technologie die man sonst nur aus Sci-Fi Serien kennt, nicht alle mathematischen Probleme lösen kann.

1.6.2 Die perfekte Uhr

Ein weiteres Problem, auf welches Quantencomputer stoßen werden, ist die perfekte Zeitmessung, also die perfekte Uhr. Jede Uhr hat zwei fundamentale Eigenschaften: Präzision und Zeitauflösung. Die Zeitauflösung gibt an, wie klein die messbaren Zeitintervalle sind (also wie oft die Uhr tickt) und die Präzision gibt an, mit welcher Ungenauigkeit bei jedem Tick zu rechnen ist. Ein

Forscherteam hat gezeigt, dass es unmöglich ist gleichzeitig die perfekte Präzision und die perfekte Zeitauflösung zu erreichen.

Warum ist das wichtig für das Quanten Computing? Aktuell haben Quantencomputer noch mit anderen Problemen, wie etwa der Dekohärenz oder Ungenauigkeiten bei den verwendeten Bauteilen zu kämpfen. Allerdings zeigen Rechnungen, dass man nicht mehr so weit davon entfernt ist, bis die physikalische Grenze der Zeitrechnung die nächste Limitation für Geschwindigkeit und Zuverlässigkeit darstellt.

Kommentar

An der Stelle nur ein kleiner Ausblick auf die perfekte Uhr. Da ich bei meiner Recherche schnell in der Thermodynamik und Quantenmechanik gelandet bin und es ein umfangreiches physikalisches Wissen voraussetzt, vertiefe ich die perfekte Uhr nicht weiter.

1.7 Zukunft

Wie sieht die Zukunft des Quanten Computing aus? Was sind oder werden Anwendungsgebiete für diese Technologie sein?

1.7.1 Quantum Machine Learning

Künstliche Intelligenz oder auch Machine Learning sind zwei der Bereiche, in denen Quantencomputer eine große Rolle spielen könnten. So schreibt die Fraunhofer-Allianz Big Data und Künstliche Intelligenz: "Verfahren der künstlichen Intelligenz und des Machine Learnings lassen sich für Quantencomputer so anpassen, dass sie mehrere Lösungswege gleichzeitig beschreiten können. Damit können Quantencomputer große Datenbestände in einem einzigen Schritt verarbeiten, Muster in den Daten aufspüren, die klassische Computer nicht entdecken und auch auf unvollständigen oder unsicheren Daten verlässliche Ergebnisse liefern." Quantencomputer könnten also die Lernverfahren von KI deutlich beschleunigen und verbessern.

Dies birgt allerdings auch ein Risiko, dessen ist sich auch das Bundesamt für Sicherheit in der Informationstechnik bewusst und gab in Kooperation mit Capgemini und dem Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme eine Studie in Auftrag, die Quantum Machine Learning (QML) im Kontext von IT-Sicherheit untersuchen soll. So hat QML beispielsweise großes Potenzial für die Malware und Spam Erkennung, sowie Kryptografie. Gleichzeitig weiß man jetzt schon, dass aktuelle Verschlüsselungsmethoden, wie RSA oder ECC, durch Quantencomputer gebrochen werden können. Daher wird bereits an quanten-resistenten Verschlüsselungsmethoden gearbeitet.

Kommentar

Die Studie des BSI ist tatsächlich sehr interessant zu lesen. Sie ist zwar von 2022, aber gibt einen guten Überblick über die Möglichkeiten und Risiken von Quantum Machine Learning. Allerdings würde es den Rahmen sprengen, hier näher darauf einzugehen, da wir uns auf die Grundlagen beschränken wollen.

1.7.2 Simulationen