# Theorie und Implementierung des Grover Algorithmus mit Qiskit von IBM

Alexandros Soultanis

12. Dezember 2018

## Inhaltsverzeichnis

**1 Der Quantencomputer** **1**
1.1 Quantencomputer vs. klassische Computer . . . . . 2
1.1.1 »Die Natur ist nicht klassisch, verdammt, und wenn man die Natur simulieren will, muss man es deshalb quantenmechanisch machen« (Richard Feynman) . . . . . 2
1.1.2 Umsetzung . . . . . 3
1.1.3 Problem 1: von einem zu vielen Qubits . . . . . 3
1.1.4 Problem 2: Quantencomputer programmieren . . . . . 3
1.1.5 Problem 3: Empfindlichkeit . . . . . 4
1.1.6 Problem 3: Error-Korrektur . . . . . 4

**2 Die Theorie der Quanteninformatik** **5**
2.1 Zweizustandsystem . . . . . 5
2.2 Das Klassiche Bit - Cbit . . . . . 6

## 1 Der Quantencomputer

Der Quantencomputer unterliegt dem Gesetz der Quantenphysik. Doch da auch die uns bekannten Informationstechnologien wie Handys und Computer die wir im Alltag benutzen, ja sogar das ganze Universum der Quantenphysik unterlegen sind, können wir mit dieser Aussage noch nicht wirklich viel anfangen. Ihr Laptop verhaltet sich zwar nach den quantenphysikalischen Gesetzen, benutzt jedoch die Gesetze der klassischen Physik um zu rechnen. Genau da unterscheiden sich klassische Computer von Quantencomputer sowie die Informatik von der Quanteninformatik. Der Quantencomputer ist allerdings nicht mächtiger als der klassische Computer – verkörpert durch

die mathematische Abstraktion der Turing-Maschine der in der Lage sein sollte, alles zu berechnen, was im physikalischen Universum überhaupt berechenbar ist, von grundlegender Arithmetik über den Aktienmarkt bis zur Kollision Schwarzer Löcher, sondern löst "lediglichëinige Probleme wie die Suche in extrem großen Datenbanken (Grover-Algorithmus) oder die Faktorisierung großer Zahlen (Shor-Algorithmus), effizienter. Dazu operiert er auf der Basis quantenmechanischer Zustände. Hierbei sind 1. das Superpositionsprinzip (d. h. die quantenmechanische Kohärenz, analog zu den Kohärenzeffekten, siehe z. B. Holographie, in der sonst inkohärenten Optik) und 2. die sogenannte Quantenverschränkung von Bedeutung.

Die physikalischen Hintergründe werden bis zu einem Gewissen Grad mit dem Black-Box Prinzip abstrahiert, da man die Quantentheorie nicht vollständig verstehen muss um einen Quantencomputer zu programmieren.

## 1.1 Quantencomputer vs. klassische Computer

### 1.1.1 »Die Natur ist nicht klassisch, verdammt, und wenn man die Natur simulieren will, muss man es deshalb quantenmechanisch machen« (Richard Feynman)

Der Vorteil eines Quantencomputers lässt sich auf ein einzelnes Phänomen herunterbrechen: die Superposition, also die Tatsache, dass im Quantenregime bis zur Messung stets eine Überlagerung vieler Zustände, vorliegt, die von der Wellenfunktion des Systems beschrieben wird. Wenn man das klassische Bit, das stets entweder 0 oder 1 ist, in die Quantenwelt überträgt, erhält man ein viel flexibleres Bit, das alle möglichen Zustände gleichzeitig annehmen kann. Jede Operation, die man darauf anwendet, wird dadurch an allen Zuständen parallel ausgeführt. Das Bit des Quantencomputers heißt zur besseren Unterscheidung auch Qubit. Anschaulich bedeutet das, dass der Rechner nicht wie ein klassischer Computer bloß $1 + 1 = 2$ ausrechnet, sondern $x + y = z$, und zwar für alle möglichen Werte von x und y.

Man möchte zum Beispiel das chemische Verhalten eines Moleküls verstehen. Dieses chemische Verhalten hängt seinerseits vom Verhalten der Elektronen in dem Molekül ab, die sich in Superpositionen vieler Zustände befinden. Dazu kommt, dass der Quantenzustand jedes einzelnen Elektrons vom Zustand aller anderen Elektronen abhängt – über ein als Verschränkung bezeichnetes quantenmechanisches Phänomen (über Verschränkung berichten?). Die Berechnung mit einem klassischen Computer dieser verschränkten Zustände ist selbst bei den einfachsten Molekülen ein sehr Aufwändig mit exponentiell anwachsender Komplexität. Im Gegensatz dazu kann ein Quantencomputer die miteinander verschränkten Elektronen analysieren, indem er seine eigenen Quantenbits in superponierte und verschränkte Zustände bringt. Das ermöglicht es einem Quantencomputer, ungewöhnlich große Informationsmengen zu verarbeiten. Jedes hinzugefügte Qubit verdoppelt die Zahl der Zustände, die das System speichern kann: Zwei Qubits können 4, drei Qubits 8, vier Qubits 16 Zustände speichern, und das gleichzeitig.

50 Qubits würden ausreichen, um Quantenzustände zu modellieren, für die 1,125 Billiarden klassische Bits nötig wären. (problem mit Fehlerkorrektur)

### 1.1.2 Umsetzung

In der Umsetzung ergibt sich dann zwar immer noch das Problem, das gewünschte Ergebnis geschickt auszulesen, was jedoch lösbar ist. Wieso konstruieren IBM und Co. nach wie vor immer schnellere Superrechner? Die Ursachen lassen sich in zwei Punkte zusammenfassen: Quantencomputer sind schwer zu saklierbarkeit und zu programmieren.

### 1.1.3 Problem 1: von einem zu vielen Qubits

Seit Peter Shor 1994 zeigte, dass sich mit Quantencomputern in polynomialer Zeit Primzahlen faktorisieren lassen, gewann das Thema an interesse. Schnell konnte man es auch praktisch umsetzen: zunächst mit ein, zwei, drei Bits, 2005, also vor nun zwölf Jahren, kam man bei sechs bis acht Bits an und prognostizierte, dass damit nun der Durchbruch erreicht sei. Heute können "klassische"Quantencomputer im besten Fall auf eine zweistellige Zahl von Bits zugreifen. Das hat vor allem physikalische Gründe. Quantenzustände sind sehr fragil. Passt man nicht auf, fallen sie der Dekohärenz anheim, geben also die Superposition zugunsten eines klassischen Entweder-Oder auf. Am besten kann man sie schützen, indem man das System sehr stark kühlt und von der Außenwelt isoliert. Aber das ist aufwendig. Quantenrechner, die mit Ionenfallen oder Photonen arbeiten, dürften deshalb kaum eine industrielle Zukunft haben (in der Gegenwart sind sie allerdings spannend, weil sie sich besonders gut untersuchen und manipulieren lassen). Am vielversprechendsten dürften auf supraleitenden Schaltkreisen basierende Quantencomputer sein. Sie benötigen zwar ebenfalls tiefe Temperaturen, bieten jedoch die Aussicht, sich in Siliziumtechnik integrieren und deutlich verkleinern zu lassen. Im Quantenregime sind Messungen immer rein statistischer Natur. Man benötigt deshalb ausgefeilte Fehlerkorrektur-Mechanismen, die meist direkt an die genutzte Architektur anzupassen sind. Die Effizienz eines äusgereiften"Quantencomputers würden sie kaum beeinflussen, aber so weit ist die Forschung eben noch nicht.

### 1.1.4 Problem 2: Quantencomputer programmieren

Den richtigen Umgang mit dem Quantencomputer zu erlernen, ist ein zeitraubender Prozess. Stellen Sie sich vor, Ihr Kollege Ingenieur hat einen Abakus entwickelt. Es gibt spannende Theorien darüber, was man damit alles ausrechnen kann. Addieren und Subtrahieren sind klar, einfach ein paar Kugeln hin und her schieben, fertig. Aber wie sieht es mit der Multiplikation aus? Sie wissen, wie man schriftlich multipliziert, doch auf dem Abakus funktioniert das ganz anders. Sie müssen also erst einen Algorithmus dafür finden.

Nun hat die Mathematik für eindeutige Zustände schon seit Jahrhunderten jede Menge Algorithmen parat - doch das seltsame Verhalten im Quantenreich ist auch ihr neu. Quantencomputer sind zumindest heute keine Universalmaschinen, denen man jedes beliebige Problem vorlegen kann. Vermutlich werden sie das aus sich heraus auch nie werden. Vielleicht wird man in Zukunft an einem herkömmlichen Supercomputer arbeiten, der nur passende Operationen eigenverantwortlich an ein Quantenmodul auslagert. Doch so weit ist die Forschung noch nicht - heute geht es vor allem darum,

geeignete Algorithmen zu finden und an die aktuellen Quantencomputer-Konzepte anzupassen. Dadurch relativiert sich ein wenig das Problem, dass noch keine Quantencomputer mit sehr vielen Bits zur Verfügung stehen.

### 1.1.5 Problem 3: Empfindlichkeit

In a quantum computer the physical systems that encode the individual logical bits must have no physical interactions whatever that are not under the complete control of the program. All other interactions, however irrelevant they might be in an ordinary computer – which we shall call classical – introduce potentially catastrophic disruptions into the operation of a quantum computer. Such damaging encounters can include interactions with the external environment, such as air molecules bouncing off the physical systems that represent bits, or the absorption of minute amounts of ambient radiant thermal energy. There can even be disruptive interactions between the computationally relevant features of the physical systems that represent bits and other features of those same systems that are associated with computationally irrelevant aspects of their internal structure. Such destructive interactions, between what matters for the computation and what does not, result in decoherence, which is fatal to a quantum computation.

### 1.1.6 Problem 3: Error-Korrektur

...

–> wie werden Loops umgesetzt? Da ja alle Operationen unitär sein müssen

# 2 Die Theorie der Quanteninformatik

Dieses Kapitel liefert Grundinformationen über die Quanteninformatik und ist möglichst einfach und mit vielen Beispielen gestaltet. Z.B. wird das Qbit anhand des bekannten klassischen Bits erklärt oder Quantengatter können als Matrizen dargestellt werden.

## 2.1 Zweizustandsystem

Das Wort Bit ist eine Wortkreuzung aus binary digit – englisch für „binäre Ziffer“. Die kleinstmögliche Unterscheidung, die ein digitaltechnisches System treffen kann, ist die zwischen zwei Möglichkeiten, in der Informatik auch als Zustände bezeichnet. Zum Beispiel kann ein Lichtschalter Ein oder Aus sein was ein Bit und somit einen Zustand repräsentiert. Somit sind mit *einem* Bit *zwei*, mit *zwei* Bit *vier* und mit $n$ Bit $2^n$ Zustände möglich. In der digitalen Schaltungstechnik werden Transistoren (BILD) und von QBit transistor einheit) zum Steuern elektrischer Spannungen und Ströme verwendet. Liegt die Spannung im hohen Bereich, so liegt der Zustand H (high) vor, im unteren Bereich L (low). Notiert wird der Zustand eines Bits als

- boolesche Variablen mit "wahr"bzw. "falsch"
- Binärstelle einer numerischen Variablen mit "0"bzw. "1"

Somit kann z.B. mit H–>1 und L–>0 eine Zuordnung gemacht werden. Analog

zum klassichen Bit gibt es in der Quanteninformation ebenfalls eine kleinste Einheit, das Qubit. Als Zweizustands-Quantensystem ist das Qubit das einfachste nichttriviale Quantensystem überhaupt. Der Begriff „Zweizustandssystem“ bezieht sich hierbei nicht etwa auf die Zahl der Zustände, die das System annehmen kann. In der Tat kann jedes nichttriviale quantenmechanische System prinzipiell unendlich viele verschiedene Zustände annehmen. Allerdings kann im Allgemeinen der Zustand eines Quantensystems durch Messung nicht sicher bestimmt werden, sondern durch die Messung wird zufällig einer der möglichen Messwerte ausgewählt, wobei die Wahrscheinlichkeit jedes Messwertes durch den vor der Messung vorliegenden Zustand bestimmt wird. Da zudem die Messung den Zustand ändert, kann dieses Problem auch nicht durch mehrmaliges Messen am gleichen System umgangen werden.

Jedoch gibt es zu jeder Messung bestimmte Zustände, bei deren Vorliegen vor der Messung der Messwert mit absoluter Sicherheit vorausgesagt werden kann, die sogenannten Eigenzustände der Messung. Dabei gibt es zu jedem möglichen Ergebnis mindestens einen solchen Zustand. Die maximale Anzahl möglicher Messwerte erhält man dabei für Messungen, bei denen es jeweils nur genau einen Zustand gibt, der diesen Messwert sicher liefert. Darüber hinaus liegt nach jeder Messung ein zum erhaltenen Messwert zugehöriger Eigenzustand vor (Kollaps der Wellenfunktion); liegt jedoch bereits vor der Messung ein Eigenzustand der Messung vor, so wird dieser nicht verändert.

Zwei Zustände, die man durch Messung sicher unterscheiden kann, nennt man auch orthogonal zueinander. Die maximale Anzahl der möglichen Messwerte bei einer Messung, und somit auch die maximale Anzahl orthogonaler Zustände, ist eine Eigenschaft

des Quantensystems. Beim Qubit als Zweizustandssystem kann man also durch Messung genau zwei verschiedene Zustände sicher unterscheiden. Will man demnach ein Qubit einfach als klassischen Speicher verwenden, so kann man darin genau ein klassisches Bit speichern. Allerdings liegen die Vorteile des Qubits gerade in der Existenz der anderen Zustände.

Ein Beispiel hierfür ist die Polarisation eines Photons. Die Polarisation übernimmt die gleiche Aufgabe wie die Spannungsunterschiede im normalen Computer. Die Polarisation von Licht gibt an, in welche Richtung Licht schwingt. Obwohl die Polarisation eigentlich eine Welleneigenschaft ist, kann sie auch für das einzelne Photon definiert werden, und alle Polarisationen sind auch für einzelne Photonen möglich. Es gibt sozusagen zwei „Ausgänge“, einen für parallel und einen für senkrecht polarisierte Photonen. Stellt man an beide Stellen einen Photon-Detektor, dann kann man so feststellen, ob das Photon parallel oder senkrecht zur optischen Achse polarisiert. Photonen, die eine andere Polarisation aufweisen, kommen aber ebenfalls an diesen „Ausgängen“ heraus. An welchem „Ausgang“ ein solches Photon herauskommt, ist in diesem Fall jedoch nicht voraussagbar; nur die Wahrscheinlichkeit kann vorhergesagt werden.

Wie bei klassischen Bits können auch mehrere Qubits zusammengefasst werden, um größere Werte zu speichern. Ein n-Qubit-System hat dabei genau $2^n$ zueinander orthogonale Zustände. Was dies bedeutet wird später erläutert. In $n$ Qubits lassen sich somit genau $n$ klassische Bits speichern.

## 2.2 Das Klassiche Bit - Cbit