

Quantencomputer und KI

Steffen Köhler

7. März 2021

Inhaltsverzeichnis

1	Einleitung	3
2	Motivation	3
2.1	Klassischer Computer - Quantencomputer	4
3	Superposition	5
3.1	QuBits-Superposition	7
4	Quantenverschränkung	8
4.1	Qubits - Verschränkung	9
5	Q-Bits	9
5.1	QuBits auf Basis von Ionenfallen	10
6	Rechnen mit Quantencomputern	11
7	Quantencomputer und KI	13
8	Rechnung eines Minimalbeispiels	15
9	Stand der Technik - Ausblick	18

Abbildungsverzeichnis

1	Interferenzmuster - Quelle: https://www.studymed.at/backend/lernen/inhalt/wellenoptik (besucht am 06.03.2021)	5
2	NAND-Gatter - Quelle: http://hyperphysics.phy-astr.gsu.edu/hbase/Electronic/ietron/nand2.gif (besucht am 06.03.2021)	11
3	DNN - Quelle: https://medium.com/@MITIBMLab/estimating-information-flow-in-deep-neural-networks-b2a77bdda7a7 (besucht am 06.03.2021)	13
4	Circuit 1 - Quelle: Eigene Aufnahme	16
5	Circuit 2 - Quelle: Eigene Aufnahme	17

1 Einleitung

„Ich kann Ihnen auch nicht sagen, warum ein Stein fällt. (...) Ich kann Ihnen aber genau sagen, wie er fällt. (...) Wir kennen diese Phänomene, können sie gut beschreiben und nutzen sie nun für unsere Verarbeitung von Informationen.“ [10, Rainer Blatt]

Diese Zitat stammt von Rainer Blatt, einem der weltweit bedeutendsten Quantenphysiker, der am Institut für Quantenoptik und Quanteninformatiion forscht.

Die in der vorliegenden Arbeit behandelten Phänomene der Quantenphysik sind selbst für Physiker schwer zu verstehen. Nichtsdestotrotz lassen sich die beobachteten und erforschten Sachverhalte für den technologischen Fortschritt nutzen.

In diesem Kontext sollen in den folgenden Kapiteln grundlegende physikalische Phänomene der Quantenphysik soweit behandelt werden, um ihre Wirkung zu verstehen. Darüber hinaus soll beleuchtet werden, wie sich diese Phänomene für die Konstruktion von QuantenBits (QuBits) nutzen lassen, um daraus funktionsfähige Quantencomputer zu bauen.

Gerade in Verbindung mit Verschlüsselungsverfahren im Bereich IT-Security wird immer wieder darauf aufmerksam gemacht, dass einige der bis heute als sicher geltenden Methoden zur Verschlüsselung, wie beispielsweise das RSA-Verfahren, nicht mehr benutzbar wären, sobald es voll funktionsstüchtige Quantencomputer gibt. [9]

Der Grund hierfür ist der Tatsache geschuldet, dass Quantencomputer viele Berechnungen gleichzeitig durchführen können und somit herkömmliche Computer bei bestimmten Aufgaben hinsichtlich der Rechenzeit vernichtend schlagen.

Doch was genau ist nun ein Quantencomputer, gibt es bereits funktionsstüchtige Exemplare und wie funktioniert er? Auf diese Fragen soll die vorliegende Arbeit Antworten liefern. Zudem soll geklärt werden, inwieweit sich Quantencomputer für den Einsatz im Bereich künstlicher Intelligenz eignen.

2 Motivation

Es stellt sich zunächst die Frage nach der Notwendigkeit von Quantencomputern. Immerhin ist die Leistung herkömmlicher Computer in der letzten

Jahrzehnten drastisch gestiegen. Erst durch diesen Leistungszuwachs sind aufwändige Rechenoperationen wie zum Beispiel das Trainieren von tiefen neuronalen Netzen möglich geworden. Um auch zukünftigen Herausforderungen gewachsen zu sein, ist eine Steigerung der Leistung auch in den nächsten Jahren dringend erforderlich. Neben dem Trainieren von neuronalen Netzen sind auch die Suche in großen Datenbanken sowie die Primfaktorzerlegung Beispiele für aufwändige Rechenoperationen, die auch modernste Rechner an ihre Leistungsgrenzen bringen können.

Es ist jedoch nicht zu erwarten, dass dieser Entwicklungsfortschritt in den kommenden Jahren und Jahrzehnten ungebremst weitergehen kann [11]. Betrachtet man diesbezüglich die grundlegenden Bausteine von Computern, so findet man hier auf der untersten Hardware-Schicht Bauteile wie Widerstände, Dioden und Transistoren [2]. Diese Bauteile sind in den letzten Jahrzehnten stetig verkleinert worden. Man spricht in diesem Zusammenhang von einer Miniaturisierung. Diese hat dazu geführt, dass Transistoren zum jetzigen Zeitpunkt gerade einmal einen Durchmesser von $10nm$ aufweisen. Der Durchmesser des Corona-Virus ist mit $80 - 140nm$ dagegen vergleichsweise groß [13]. Die Leistungssteigerung von Computern ist in hohem Maße auf die Miniaturisierung der entsprechenden Bauteile zurückzuführen.

Man hat jedoch in dieser Hinsicht in gewisser Weise physikalische Grenzen erreicht. Bei Transistoren beispielsweise, die wie kleine Schalter fungieren, tritt bei derart kleiner Bauweise der sogenannte Tunneleffekt ein [11]. Das bedeutet, dass Elektronen den geschlossenen Transistor passieren können, was ihn demnach unbrauchbar macht. Zudem wird zur Herstellung dieser Bauteile in der Regel UV-Licht verwendet. Unterschreiten die Bauteile eine gewisse Größe, so wird die Wellenlänge von UV-Licht schlichtweg zu groß, um damit arbeiten zu können.

Um trotzdem eine Leistungssteigerung zu erzielen, muss demnach völlig neu gedacht werden. Ein vielversprechender Ansatz sind Quantencomputer.

2.1 Klassischer Computer - Quantencomputer

Eine der häufigsten Phänomene, die im Zusammenhang mit Quantencomputern erwähnt werden, sind die Zustände der sogenannten QuBits (eine genauere Erläuterung folgt in Kapitel 5). Während sich herkömmliche Bits in gängigen Computern in genau zwei Zuständen befinden können, sind die in Quantencomputern verbauten QuBits nicht auf zwei Zustände beschränkt, sondern können gleichzeitig mehrere Zustände einnehmen [11], was Tabelle

Klassischer Computer	Quantencomputer
Bit	QuBit
0 - 1	0 - 1 - 0/1
entweder oder	sowohl als auch

Tabelle 1: Vergleich der möglichen Zustände im klassischen- und im Quantencomputer

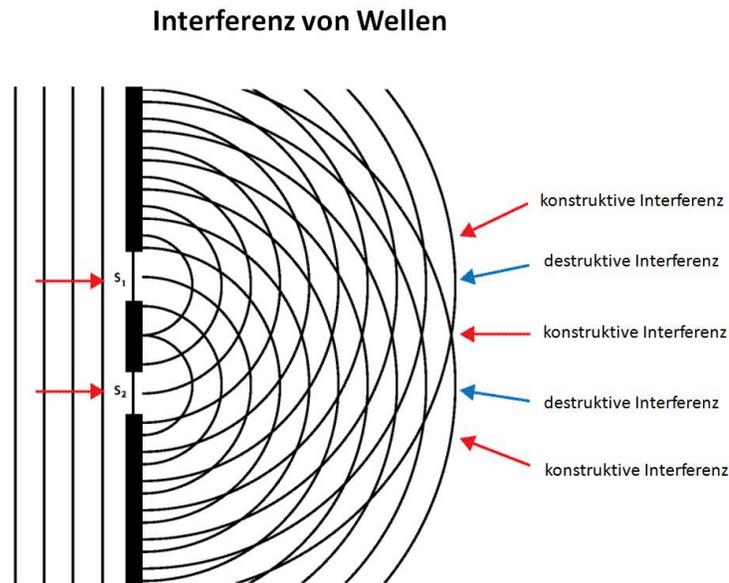


Abbildung 1: Interferenzmuster von Wellen durch einen Doppelspalt

1 verdeutlicht.

Der seltsam anmutenden Zustand „sowohl als auch“ wird als Superposition bezeichnet. Dieses Phänomen ist grundlegend für die Funktionsweise von Quantencomputern und wird im nächsten Kapitel behandelt.

3 Superposition

[12] beschreibt zum Phänomen der Superposition zunächst ein Experiment, bei dem Kugeln durch einen Spalt auf eine Wand geschossen werden. Durch die Streuung der Kugeln entsteht auf der dahinter liegenden Wand ein Strei-

fen mit den Einschlaglöchern.

Führt man ein vergleichbares Experiment mit einer Wasserwelle durch, die durch einen Spalt auf eine Fläche trifft, so ist die Amplitude dieser Welle an einem Punkt am größten und nimmt zu beiden Seiten hin ab [6].

Wird das Experiment der Wasserwellen mit einem Doppelspalt durchgeführt, so entsteht an der hinter dem Spalt befindlichen Wand ein Interferenzmuster. Dies lässt sich relativ einfach durch die Überlagerung der Wellen erklären.

Wie in Abbildung 1 dargestellt, löschen sich die beiden Wellen an bestimmten Stellen gegenseitig aus (Wellenberg und Wellental treffen aufeinander), an anderen Stelle addieren sie sich (zwei Wellenberge bzw. Welltäler treffen aufeinander).¹

Beim beschießen eines Doppelspalts mit Metallkugeln ist jedoch von diesem Interferenzmuster nichts zu sehen. Wie erwartet entstehen dabei einfach zwei Streifen auf der hinter dem Spalt befindlichen Wand.

Führt man den gleichen Versuch nun im sehr kleinem Maßstab durch und ersetzt die Metallkugeln beispielsweise durch Elektronen, welche durch einen einzelnen Spalt geschossen werden, so erhält man einen Streifen auf der rückseitigen Wand. Soweit entspricht das der Erwartungshaltung, schließlich handelt es sich sowohl bei Elektronen als auch bei Metallkugeln um Materie. Wird der Einzelspalt jedoch durch einen Doppelspalt ersetzt, findet man auf der rückseitigen Wand ein Interferenzmuster vor, wie es auch beim Doppelspaltversuch mit Wasserwellen entstanden ist. Dies ist äußerst verblüffend, schließlich wurden kleine Materieteilchen durch den Spalt geschossen. Anfänglich hatten sich Physiker dieses Phänomen damit erklärt, dass die Elektronen mit jeweils anderen Elektronen in irgendeiner Form interagieren und sich dabei gegenseitig beeinflussen. Daher wurde der Versuch wiederholt, indem die Elektronen mit einem gewissen zeitlichen Abstand einzeln durch den Spalt geschossen wurden. Ein Interagieren zwischen den Elektronen konnte somit ausgeschlossen werden. Trotzdem entstand ein Interferenzmuster.

Das einzelne Elektron muss also durch beide Spalte gleichzeitig geflogen sein und sich dabei selbst beeinflusst haben. Anders formuliert geht das Elektron also durch beide Öffnungen, durch keine der beiden Öffnungen und

¹Eine gute Möglichkeit, dieses Phänomen interaktiv nachzuvollziehen, findet sich unter https://phet.colorado.edu/sims/html/wave-interference/latest/wave-interference_de.html.

Bit		QuBit	
00	10	00	10
01	11	01	11

Tabelle 2: Mögliche Kombinationen von zwei Bits bzw. QuBits. Grün: Beispielhafte Zustände, die gleichzeitig angenommen werden können

erst durch den einen Spalt und dann durch den anderen. Dieses schwer zu verstehende Phänomen wird als Superposition bezeichnet.

Es muss in diesem Zusammenhang auf ein weiteres Phänomen eingegangen werden. Um das Resultat des genannten Experiments besser zu verstehen wurde ein Messgerät an einem der Spalte angebracht. Dieses schlug aus, sobald ein Elektron den entsprechen Spalt passierte. Das Ergebnis dieses Experiments war jedoch ebenfalls gänzlich unerwartet; an der hinter dem Doppelspalt befindlichen Wand entstanden nun wieder nur zwei Streifen anstatt eines Interferenzmusters. Der Vorgang des Messens hatte also die Verhaltensweise der Elektronen verändert.

Selbst für Experten der Quantenphysik ist es schwer, das Phänomen der Superposition im einzelnen zu verstehen. Nichtsdestotrotz kann sich der Mensch diesen Sachverhalt zunutze machen, beispielsweise im Zusammenhang mit QuBits.

3.1 QuBits-Superposition

QuBits besitzen die Eigenschaft, dass sie mehrere Zustände gleichzeitig annehmen können. Im Gegensatz zu herkömmlichen Computern, deren Bits sich im Zustand 0 oder 1 befinden können, sind hier also viel mehr Zustände möglich. Wie aus dem Kapitel 3 hervorgeht, kollabiert jedoch der Zustand eines QuBits in 0 oder 1, sobald eine Messung stattfindet [5][17][18].

Die Tatsache, dass QuBits viele Zustände gleichzeitig annehmen können, führt zudem zu einem größeren Informationsgehalt [11]. Die Möglichkeiten, zwei herkömmliche Bits zu kombinieren, sind in Tabelle 2 dargestellt. Die möglichen Kombinationen sind bei QuBits natürlich die gleichen, jedoch kann bei herkömmlichen Bits zu einem bestimmten Zeitpunkt immer nur einer der vier Zustände eingenommen werden. Bei QuBits hingegen können zu einem bestimmten Zeitpunkt alle vier Zustände gleichzeitig eingenommen werden.

Dies führt zu einem deutlich höheren Informationsgehalt. Wie in [17] erläutert wird, enthalten 2 QuBits den Informationsgehalt von 4 regulären

Bits. Allgemeiner ausgedrückt ergibt sich hinsichtlich des Informationsgehaltes für N Bits bzw. QuBits der Zusammenhang:

$$N\text{QuBit} \equiv 2^N \text{Bit}$$

4 Quantenverschränkung

Ein weiteres, äußerst faszinierendes Phänomen der Quantenphysik ist die Quantenverschränkung. Diese Erscheinung soll am Beispiel von zwei Elektronen beschrieben werden. Elektronen besitzen einen sogenannten Spin [17]. Vereinfacht ausgedrückt lässt sich dieser mit der Rotation im Uhrzeigersinn oder gegen der Uhrzeigersinn vergleichen [1]. Gesetzt den Fall, zwei Elektronen sind miteinander verschränkt, so besitzen die beiden Elektronen den exakt gleichen Spin, allerdings in entgegengesetzter Richtung. Dies ist auf die Tatsache zurückzuführen, dass der Gesamtspin im Universum konstant sein muss [18]. Das eigentlich faszinierende ist jedoch, dass sich ein Elektron bei Änderung des Spins seines Partnerelektrons in exakt diesem Augenblick an den neuen Spin anpasst. Anders ausgedrückt kann man die Geschwindigkeit oder die Richtung des Spins am einen Elektron verändern und bewirkt dadurch automatisch die exakt gleiche Änderung des Partnerelektrons im selben Augenblick. Dies geschieht, zum großen Erstaunen der Physiker, völlig unabhängig der Entfernung, was durch eine Vielzahl an Experimenten bewiesen werden konnte [18]. Die beiden verschränkten Elektronen können sich jeweils am anderen Ende des Universums befinden und viele Lichtjahre voneinander entfernt sein, der Effekt der Quantenverschränkung tritt dennoch augenblicklich ein.

Es stellt sich die Frage, wie solch eine Verschränkung von Quanten gezielt hervorgerufen werden kann. Um dies zu beantworten sollen als Beispiel Photonen anstatt Elektronen dienen. Diese Lichtteilchen entstehen unter anderem dann, wenn ein Elektron von einem hohen Energieniveau auf ein niedrigeres Energieniveau herabsinkt [4]. Wenn man dementsprechend ein Calcium-Atom auf ein sehr hohes Energieniveau bringt und dessen Elektron anschließend wieder auf ein niedrigeres Energieniveau zurückfällt, so ist es diesem Elektron nicht möglich, nur ein einzelnes Photon zu emittieren. Stattdessen werden direkt zwei Photonen emittiert, die von Geburt an miteinander verschränkt sind.

Wie sich vermuten lässt, sind Photonen als QuBits denkbar ungeeignet. Schließlich bewegen sie sich mit Lichtgeschwindigkeit fort und sind aufgrund

ihrer Flüchtigkeit äußerst schwer kontrollierbar. Es konnte jedoch festgestellt werden, dass sich Licht absorbierende Atome ebenfalls miteinander verschränken lassen, wenn verschränkte Photonen auf sie treffen [4].

4.1 Qubits - Verschränkung

Die eben beschriebene Quantenverschränkung ist, ähnlich wie die Superposition, eine fundamentale Eigenschaft für die Funktionsweise von Quantencomputern. Die Möglichkeit, QuBits zu verschränken, ist in diesem Kontext Grundlage vieler Rechenoperationen. Verschränkte QuBits verhalten sich so, als ob eine Verbindung zwischen ihnen besteht. Dabei spielt die Entfernung der beiden QuBits theoretisch überhaupt keine Rolle [1]. Ein QuBit nimmt bei Manipulation des Partner-QuBits augenblicklich dessen invertierten Zustand an. Dieses Phänomen lässt sich beispielsweise nutzen, um QuBit-Zustände zu messen [2].

5 Q-Bits

Die in der vorliegenden Arbeit bereits mehrfach erwähnten QuBits müssen einige Eigenschaften erfüllen, um sich für den Bau eines Quantencomputers zu eignen. Dabei gibt es viele unterschiedliche Ansätze, um QuBits zu erzeugen.

In den letzten Jahren wurden hier von einigen Forschungseinrichtungen und Firmen unterschiedliche Methodiken erforscht [7]. Google und IBM arbeiten beispielsweise an einem Verfahren, bei dem Supraleitende Streifenleitungsresonatoren zum Einsatz kommen. Das zu manipulierende Element ist dabei eine Elektronenwolke in einem Mikrowellen-Oszillator [3]. Dieser muss auf 15 mK, also nahe des absoluten Nullpunkts, gekühlt werden. Durch Anpassung der Oszillator-Frequenz können hier mehrere QuBits in Resonanz und damit in einen verschränkten Zustand gebracht werden. Zudem können somit die in Kapitel 6 beschriebenen Quantengatter angewendet werden.

Ein weiterer Ansatz besteht darin, QuBits auf einem Silizium-Chip zu erzeugen. Hier basiert das QuBit auf einem modifiziertem Standardtransistor bei dem das zu manipulierende Element ein einzelnes Elektron ist, dessen Spin sich beeinflussen lässt. Vorteil laut [7] in diesem Zusammenhang ist die Tatsache, dass bereits großes Wissen um die Herstellung von Silizium-Chips existiert und man mit vergleichsweise geringen Mitteln die bestehende Infrastruktur auf die Herstellung von QuBits anpassen könnte.

Alternativ zu diesem Vorgehen gibt es zudem einen Ansatz, bei dem ein Stickstoff-Atom in einem Diamant platziert wird [7]. Neben diesem Stickstoff-Atom entsteht dadurch ein Raum, das sogenannte NV-Zentrum, in dem sich ein einzelnes Elektron befindet, welches wiederum als QuBit genutzt werden kann.

Alle bereits beschriebenen Ansätze haben den Nachteil, dass die QuBits relativ instabil und ungenau sind. Beim Bau von größeren Quantencomputern mit zahlreichen QuBits wird diese Ungenauigkeit zu einem echten Problem, da sich entstehende Fehler hochpotenzieren und im Extremfall zu unbrauchbaren Ergebnissen führen. Aus diesem Grund gibt es laut [7] eine Forschungsgruppe der Firma Microsoft, die an einem völlig anderen Ansatz forscht, welcher mit „Verknotete Quantenbits auf exotischem Materialmix“ betitelt werden kann. Funktionstüchtige QuBits hat dieses Vorgehen bislang nicht hervorgebracht, jedoch erhofft sich das Forscherteam auf lange Sicht wesentlich stabilere und zuverlässigere QuBits.

Um ein genaueres Bild eines QuBits zu erhalten, wird im folgenden Kapitel ein weiteres Verfahren genauer beleuchtet.

5.1 QuBits auf Basis von Ionenfallen

Zusätzlich zu den bereits beschriebenen Verfahren gibt es die Möglichkeit, QuBits auf Basis von Ionenfallen herzustellen. Benötigt werden hierfür Ionen, also geladene Atome. Diese werden von einem Magneten in der Schwebe gehalten und befinden sich zudem im Vakuum. Dies ist notwendig, um völlige Isolation herzustellen und das System somit vor Störeinflüssen zu schützen. Dieses Ion wird nun von einem Laser auf bestimmte Art und Weise angestrahlt, wodurch das Ion zum Stillstand gebracht wird. Man spricht in diesem Zusammenhang auch von Kühlung [10]. Durch weitere Laserbestrahlung lässt sich das Ion zudem manipulieren; es wird in diesem Sinne programmiert. Dadurch lassen QuBits miteinander verschränken, wodurch ein Informationsaustausch möglich wird. Ist der Rechengang abgeschlossen, so lassen sich die Ionen auslesen. Bei diesem Vorgehen ist ein visuelles Auslesen möglich, da die Ionen nun hell oder dunkel sind. Diese Hell-Dunkel-Zustände lassen sich zuletzt wieder in für Menschen verständliche Information umrechnen. Sowohl [16] als auch [10] eignen sich gut, um eine Vorstellung eines Quantencomputers auf Basis von Ionenfallen zu erlangen.

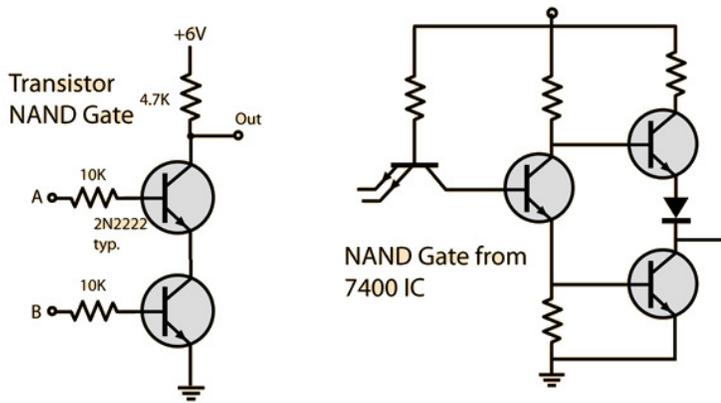


Abbildung 2: Aufbau eines NAND-Gatters

6 Rechnen mit Quantencomputern

Ist es gelungen, mit den zuvor beschriebenen Verfahren QuBits herzustellen und auf dessen Basis einen Quantencomputer zu bauen, so stellt sich die Frage wie sich damit Rechenoperationen durchführen lassen.

In herkömmlichen Computern wird dies durch sogenannte Logikgatter möglich [3]. Diese bestehen aus sinnvoll angeordneten Bauteilen wie Dioden, Widerständen und Transistoren. Eines der wichtigsten Gatter ist in diesem Zusammenhang das NAND-Gatter, welches zwei Bits A und B entgegennimmt und ein C-Bit ausgibt. Dabei ist $C = 0$ sofern gilt $A = B = 1$. Ein möglicher Aufbau eines NAND-Gatters findet sich in Abbildung 2.

Laut [14, S. 100] kann durch geschickte Verschaltung mehrerer NAND-Gatter jede beliebige, wohldefinierte Berechnung ausgeführt werden.

Im Umfeld von Quantencomputer gibt es vergleichbare Konstrukte, die sich Quantengatter nennen. Es handelt sich dabei um physikalische Manipulationen der QuBits, welche im Falle von QuBits auf Basis von Ionenfallen beispielsweise durch Laserbestrahlung durchgeführt werden (siehe Kapitel 5.1).

Zu den wichtigsten Quantengattern gehören das HADAMARD-Gatter, das Phaseshift-Gatter und das CNOT-Gatter [3].

- HADAMARD wird dazu verwendet, um ein QuBit in die in Kapitel 3 beschriebene Superposition zu bringen.

- Phaseshift verändert die Wahrscheinlichkeit, mit der ein QuBit beim Messvorgang in den Zustand 0 oder 1 fällt.
- CNOT verschränkt zwei Qubits und invertiert zudem das Ziel-QuBit, wenn das Kontroll-QuBit 1 ist.

Mit diesen Quantengattern lassen sich dieselben Rechenoperationen durchführen, wie mit klassischen Logikgattern [3]. Selbstverständlich unterscheidet sich die Vorgehensweise beim Programmieren stark von herkömmlichen Programmiersprachen wie beispielsweise C oder Java. Es muss an dieser Stelle erneut betont werden, dass beim durchführen solcher Rechenoperationen alle Zustände gleichzeitig ausgeführt werden, was als Parallelität bezeichnet werden kann [11].

Dieser Tatsache ist es geschuldet, dass Quantencomputer klassischen Computern in bestimmten Bereichen deutlich überlegen sind. Ein häufig angeführtes Beispiel ist dabei die Primfaktorzerlegung. Bekanntermaßen ist das Multiplizieren großer Primzahlen für herkömmliche Computer kein Problem. Die Rückgewinnung dieser Primzahlen ist jedoch bislang unmöglich. Die Faktorisierung bei 301 Stellen würde mit einem klassischen Computer 10^{24} Schritte benötigen was eine Rechendauer von etwa 100.000 Jahre bedeuten würde. Ein Quantencomputer könnte den Shor-Algorithmus verwenden und die gleiche Rechnung in nur 10^{10} Schritten durchführen, was eine Rechendauer von weniger als 1 Sekunde benötigen würde [3].

Eine ebenfalls wichtige Problemstellung ist die Suche in großen Datenbanken [11]. Existieren in einer Datenbank beispielsweise 40.000 Einträge, so muss ein klassischer Computer im ungünstigsten Fall alle Einträge überprüfen, um den richtigen zu finden. Ein Quantencomputer könnte dies mithilfe des Grover-Algorithmus in nur maximal $\sqrt{40.000} = 200$ Schritten bewerkstelligen [3].

Zudem wären biochemische- und quantenmechanische Simulationen mithilfe eines Quantencomputers erheblich besser und schneller möglich als mit herkömmlichen Computern [11].

Ein weiteres wichtiges Themengebiet, auf dem Quantencomputer erhebliche Vorteile bieten, ist das Feld der künstlichen Intelligenz, worauf im folgenden Kapitel genauer eingegangen werden soll.

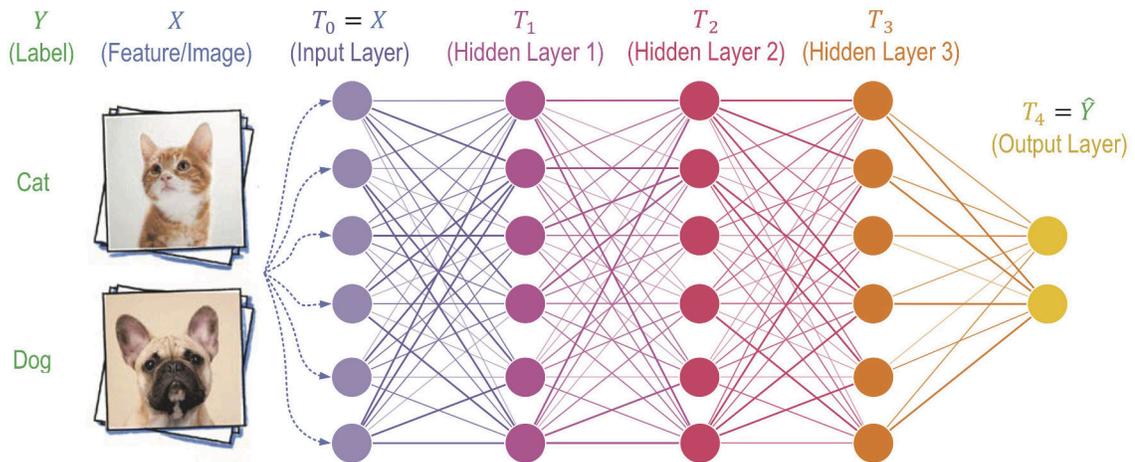


Abbildung 3: Aufbau eines tiefen neuronalen Netzes (DNN) für eine binäre Klassifikation

7 Quantencomputer und KI

„Es gibt eine natürliche Verbindung zwischen der inhärent statistischen Natur des Quantencomputing (...) und dem maschinellen Lernen.“ [8, Johannes Otterbach]

Abbildung 3 zeigt eine beispielhafte Abbildung eines tiefen neuronalen Netzes. Diese zeichnen sich unter anderem durch zahlreiche Hidden-Layer aus. In jedem dieser Layer befinden sich eine Vielzahl von Neuronen. In einer sehr einfachen Architektur sind die Neuronen einer Schicht mit jedem Neuron der nächsten Schicht verbunden.² An jeder Verbindung befinden sich sogenannte Gewichte. Diese werden während des Trainingsvorgangs durch Backpropagation so angepasst, dass das Resultat am Output-Layer möglichst gut ist. Wie sich beim Betrachten von Abbildung 3 bereits vermuten lässt, gibt es gerade in größeren neuronalen Netzen eine Vielzahl solcher Gewichte, die in großen Matrizen gehalten werden müssen. Die Manipulation solcher Matrizen ist äußerst Rechenaufwändig.

Quantencomputer könnten hier Abhilfe schaffen, da sie in der Lage sind, große Datenfelder in nur einem einzigen Schritt zu manipulieren. Dabei liegt

²Es gibt diesbezüglich zahlreiche Varianten wie beispielsweise Drop-Out-Layer, die dafür sorgen, dass ein Neuron nicht mit jedem Neuron der nächsten Schicht verbunden ist. Häufig werden solche Verfahren benutzt, um Overfitting zu vermeiden.

die Speicherkapazität des Quantensystems in der kollektiven Eigenschaft der QuBits. Aus 2 QuBits lassen sich beispielsweise 4 verknüpfte Zustände generieren:

- an an
- an aus
- aus an
- aus aus

Dabei kann jeder Zustand mit einem bestimmtem Gewicht, seiner Amplitude, vertreten werden [8]. Dieser Zustand repräsentiert ein Neuron. Demzufolge können 3 QuBits bereits 8 Neuronen repräsentieren, 4 QuBits entsprechen schon 16 Neuronen. Dieser exponentielle Zusammenhang sorgt dafür, dass auch Quantencomputer mit vergleichsweise wenigen QuBits sinnvoll im Bereich KI eingesetzt werden können.

Der gleiche Zusammenhang besteht in der Speicherkapazität des Systems, welcher exponentiell mit der Zahl der QuBits wächst. Führt man beispielsweise eine Operation an 4 QuBits durch, so werden in Summe 16 Zahlen auf einen Schlag verarbeitet. Ein klassischer Computer hingegen müsste alle 16 Zahlen nacheinander verarbeiten.

Es kann an dieser Stelle vorgegriffen werden, dass es aktuell noch keinen Quantencomputer gibt, der ausreichend viele QuBits besitzt um von der Industrie kommerziell eingesetzt zu werden. Im Zusammenhang mit KI jedoch hat Kristan Temme folgende Aussage gemacht: „Quantensysteme könnten bereits Vorteile bieten, bevor wir einen vollständig universellen, fehlertoleranten Quantencomputer besitzen.“ [8, Kristan Temme]

Es wird darüber hinaus davon ausgegangen, dass Quantencomputer dazu in der Lage sind, subtilere Muster aus den vorhandenen Daten zu extrahieren, für die klassische Computer blind sind [8]. Ein weiterer Vorteil ist, dass Quantencomputer nicht an unvollständigen oder unsicheren Daten scheitern.

Es darf jedoch nicht verschwiegen werden, dass es auch einige Herausforderungen beim Zusammenspiel zwischen Quantencomputern und künstlicher Intelligenz gibt. Ein Quantencomputer arbeitet mit Quantenzuständen, welche für Menschen nicht lesbar sind. Um mit diesem System arbeiten zu können, müssen die für Menschen lesbare Daten zunächst übersetzt werden. Diese Übersetzung muss schlussendlich wieder rückgängig gemacht werden.

Der Übersetzungsvorgang stellt dabei bislang ein echtes Problem dar und kann gegebenenfalls zum Verlust der Vorteile des Quantensystems führe. Mit anderen Worten ausgedrückt ist das Quantensystem zwar in der Lage, komplizierte Rechenoperationen äußerst effizient zu lösen, aber die Tatsache, dass die Kommunikation dieses Systems mit seiner Umgebung äußerst schwierig ist, kann zu seiner Unbrauchbarkeit führen. Vergleichen kann man dies mit einem hochmodernen und leistungsstarken Smartphone, welches sich in einer Umgebung mit sehr schlechtem Netz befindet, wodurch es kaum sinnvoll eingesetzt werden kann [8].

Um die Frage vorwegzunehmen, ob es denn nun aktuell funktionierende Quantencomputer gibt, wird im folgenden Kapitel ein Minimalbeispiel auf einem echten Quantencomputer von IBM vorgeführt.

8 Rechnung eines Minimalbeispiels

Wie in Kapitel 5 bereits erwähnt, forscht die Firma IBM am Bau von Quantencomputern. Wie einige andere Firmen und Forschungseinrichtungen ist es ihnen bereits gelungen, einige funktionstüchtige Quantencomputer zu bauen. IBM hat diesbezüglich bestimmte Quantencomputer über das Internet zugänglich gemacht, sodass man als Privatnutzer mit einem kostenlosen Account Beispielrechnungen auf diesen Quantencomputern durchführen kann.³ Um die folgende Passage optimal nachzuvollziehen wird der Nachbau des in Abbildung 4 dargestellten Circuits empfohlen.

In diesem Beispiel werden zwei QuBits verwendet (q_0 und q_1). Zunächst sollen beide QuBits in Superposition gebracht werden, was durch das HADAMARD-Gate (H) erreicht wird. Zu beachten sind dabei die Measurement-Probabilities im unteren Bildbereich. Es gibt zum jetzigen Zeitpunkt eine Gleichverteilung der möglichen Ausgänge dieser Rechnung. Das System fällt mit jeweils der gleichen Wahrscheinlichkeit, also 25%, in den Zustand 00, 01, 10 oder 11.

Anschließend wird auf jedem QuBit ein T-Gate platziert, welches zur Gruppe der Phaseshift-Gates gehört. Um deren Effekt im Measurement-Probabilities-Fenster zu sehen, muss jeweils ein weiteres HADAMARD-Gatter auf den QuBits angewendet werden. Dies hat zur Folge, dass die Wahrscheinlichkeiten, mit der die einzelnen QuBits in 0 oder 1 Fallen, verschoben wer-

³Unter der URL <https://quantum-computing.ibm.com/> lässt sich mithilfe des sogenannten Composers die Programmierung eines Quantencomputers vornehmen.



Measurement Probabilities ⓘ ⋮

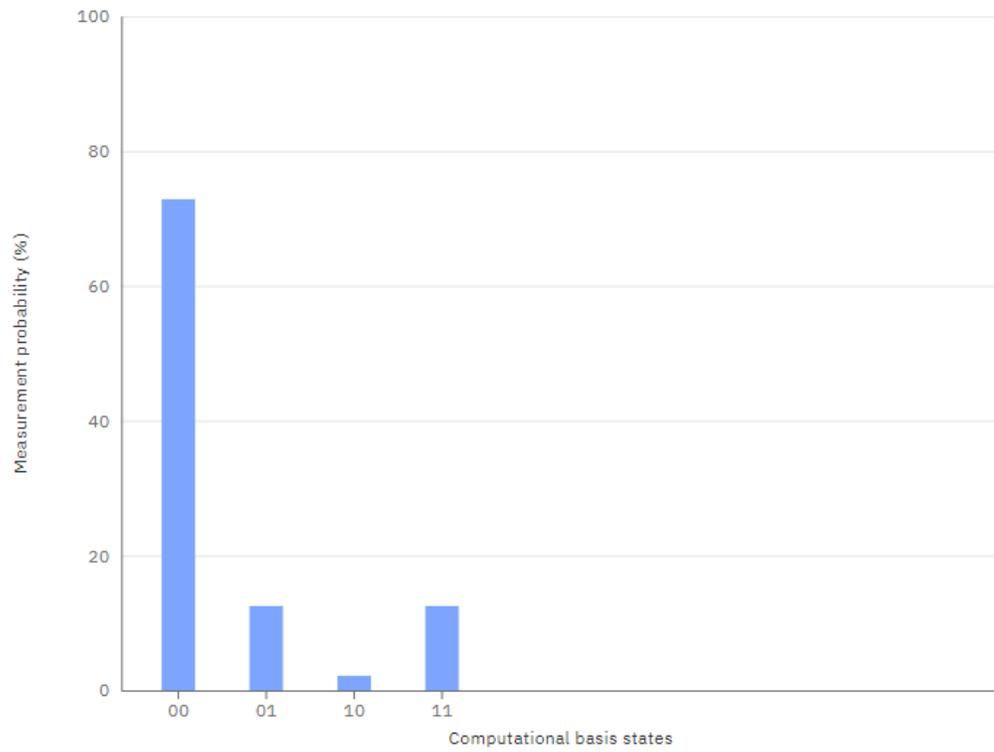


Abbildung 4: Programmierung eines Quantencomputers mithilfe von HADAMARD-, Phaseshift- und CNot-Gates



Abbildung 5: Zusätzliche Verwendung von Measurement, was für die Lauffähigkeit auf einem Quantencomputer zwingend erforderlich ist

den. In diesem Beispiel entsteht somit eine hohe Wahrscheinlichkeit für das System, in den Zustand 00 zu fallen. Die Wahrscheinlichkeit für 11 hingegen ist jetzt äußerst gering.

Abschließend soll das CNot-Gate angewendet werden, welches zwei QuBits miteinander verschränkt. Der Zustand entspricht nun der Abbildung 4. Es lässt sich erkennen, dass die Wahrscheinlichkeiten für 10 und 11 bei Anwendung dieses Gates genau vertauscht werden, was an der möglichen Invertierung des Ziel-QuBits liegt, sofern das Kontroll-QuBit 1 ist.

Damit sind drei der grundlegenden Operationen auf QuBits angewendet worden. Möchte man dieses Programm nun auf einem echten Quantencomputer laufen lassen, so muss zunächst noch ein Measurement auf jedes QuBit angewendet werden. Das Ergebnis findet sich in Abbildung 5. Wird das Programm nun an einen der von IBM zur Verfügung gestellten Quantencomputer geschickt, so wird dieser Job in der Warteschlange eingereiht. Ist die Berechnung abgeschlossen, erhält der Nutzer die ausgewerteten Messergebnisse.

Zu Beachten ist hier, dass das Programm standardmäßig 1024 mal durchgeführt wird. Nur durch das mehrfache Ausführung des Programms kommt die vom Nutzer erwartete Wahrscheinlichkeitsverteilung zustande [5]. Würde man das Programm nur ein einziges mal ausführen, würde das System entweder in 00, 01, 10 oder 11 fallen und den jeweiligen Ausgang mit einer zugehörigen Wahrscheinlichkeit von 100 % ausgeben.

9 Stand der Technik - Ausblick

Es konnte gezeigt werden, dass Quantencomputer zum jetzigen Zeitpunkt existieren und funktionstüchtig sind. Google ist es im Oktober 2019 gelungen, eine Aufgabe mithilfe eines Quantencomputers (53 QuBits) zu lösen, für die ein herkömmlicher Computer 10.000 Jahre gebraucht hätte [15][7]. Was von manchen als großer Durchbruch betitelt worden ist, beschreiben andere als Experiment akademischer Natur ohne jeden Nutzen. Zum Zeitpunkt der Erstellung der vorliegenden Arbeit werden Quantencomputer noch nicht in der Industrie eingesetzt. Viele Firmen beschränken sich aktuell darauf, gewissermaßen Fingerübungen mit Quantencomputern zu machen, um bei deren Durchbruch auf den kommerziellen Gebrauch vorbereitet zu sein.

Zukünftig werden Quantencomputer aller Wahrscheinlichkeit nach nur über das Internet verfügbar sein. Quanten-Laptops oder Quanten-Smartphones für den Heimgebrauch gelten gemeinhin als nahezu ausgeschlossen.

Es muss an dieser Stelle betont werden, dass Quantencomputer herkömmliche Computer nicht ersetzen werden [17]. Sequentielle Programme wie beispielsweise das Surfen im Internet oder das Schauen eines Videos können wesentlich sinnvoller auf herkömmlichen Computern realisiert werden [3].

Um Quantencomputer für echte Anwendungen benutzbar zu machen, bräuchte man größere und leistungsstärkere Modelle. Bis diese verfügbar sind könnten noch 5 - 10 Jahre vergehen, möglicherweise dauert es sogar noch länger.

Es muss im Rahmen dieser Arbeit wiederum erneut darauf hingewiesen werden, dass auch aktuelle Quantencomputer mit etwa 50 QuBits für das Einsatzgebiet der künstlichen Intelligenz von großem Nutzen sein können.

Literatur

- [1] 100SekundenPhysik. *Spukhafte Quantenverschränkung*. 2015. URL: <https://www.youtube.com/watch?v=mFW0uSKTtS8> (besucht am 05. 03. 2021).
- [2] brainfaqk. *Wie funktionieren Quantencomputer? (Teil 1/2)*. 2018. URL: <https://www.youtube.com/watch?v=u5S-hEvq9SI> (besucht am 01. 03. 2021).
- [3] brainfaqk. *Wie funktionieren Quantencomputer? (Teil 2/2)*. 2018. URL: <https://www.youtube.com/watch?v=-oTGgp3s0VI> (besucht am 05. 03. 2021).
- [4] Chad Orzel. *How Do You Create Quantum Entanglement?* 2017. URL: <https://www.forbes.com/sites/chadorzel/2017/02/28/how-do-you-create-quantum-entanglement/?sh=ae27c7e1732b> (besucht am 05. 03. 2021).
- [5] Dr. Anna-Lena Gutberlet. *Rechnen mit Qubits: So arbeitet ein Quantencomputer*. 2017. URL: <https://www.elektronikpraxis.vogel.de/rechnen-mit-qubits-so-arbeitet-ein-quantencomputer-a-648407/> (besucht am 05. 03. 2021).
- [6] ETH D-PHYS Vorlesungsexperimente. *5.10.16 Beugung von Wasserwellen im Wellentrog*. 2017. URL: <https://www.youtube.com/watch?v=gzjdKjrgbmU> (besucht am 05. 03. 2021).
- [7] Frank Grotelüschen. *Wettstreit der Systeme. Quantencomputer*. 2020. URL: https://www.deutschlandfunk.de/quantencomputer-wettstreit-der-systeme.740.de.html?dram:article_id=479940 (besucht am 05. 03. 2021).
- [8] Georg Musser. *Quantencomputer könnten künstliche Intelligenz voranbringen*. 2018. URL: <https://www.spektrum.de/news/koennen-quantencomputer-die-kuenstliche-intelligenz-voranbringen/1566450> (besucht am 01. 03. 2021).
- [9] Hanno Böck. *Das Ende von RSA und Co. QUANTENCOMPUTER*. 2014. URL: <https://www.golem.de/news/quantencomputer-das-ende-von-rsa-und-co-1401-103697.html> (besucht am 01. 03. 2021).
- [10] HYPERRAUMTV. *Rechnen mit QuBits*. 2018. URL: <https://www.youtube.com/watch?v=xRdlbjnLK6Q> (besucht am 05. 03. 2021).

- [11] Kurzgesagt – In a Nutshell. *Quantencomputer erklärt - Grenzen der menschlichen Technologie*. 2015. URL: <https://www.youtube.com/watch?v=JhHMJCUmq28> (besucht am 05.03.2021).
- [12] Quantenwelt. *Doppelspalt-Experiment - Quantenphysik einfach erklärt*. 2009. URL: <https://www.youtube.com/watch?v=3ohj0lta06Y> (besucht am 02.03.2021).
- [13] Robert-Koch-Institut. *SARS-CoV-2: Virologische Basisdaten sowie Virusvarianten*. 2021. URL: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Virologische_Basisdaten.html#:~:text=Coronaviren%20sind%20umh%C3%BC11te%20RNA%20%2DViren,et%20al.%2C%202020 (besucht am 10.03.2021).
- [14] Max Tegmark. *Leben 3.0. Mensch sein im Zeitalter Künstlicher Intelligenz*. ger. Süddeutsche Zeitung Edition. Tegmark, Max (VerfasserIn) Mania, Hubert (ÜbersetzerIn). München: Süddeutsche Zeitung, 2018. 528 S. ISBN: 9783864974649.
- [15] Ulrike Ostler. *Google erzielt mit 53 Qubits einen Durchbruch. Der Beweis für die Überlegenheit des Quantencomputers ist erbracht*. 2019. URL: <https://www.datacenter-insider.de/google-erzielt-mit-53-qubits-einen-durchbruch-a-876679/> (besucht am 05.03.2021).
- [16] Universität Innsbruck. *Quantencomputer: Innsbrucker Physikerin entwickelt Ionenfallen-Mikrochips weiter*. 2020. URL: <https://www.youtube.com/watch?v=7pWbXFT2Tdw> (besucht am 04.03.2021).
- [17] Veritasium. *How Does a Quantum Computer Work?* 2013. URL: https://www.youtube.com/watch?v=g_IaVepNDT4 (besucht am 05.03.2021).
- [18] Veritasium. *Quantum Entanglement & Spooky Action at a Distance*. 2015. URL: <https://www.youtube.com/watch?v=ZuvK-od647c> (besucht am 05.03.2021).