Quantum Computing

Rechnen mit dem Unberechenbaren

Ausarbeitung zum Vortrag im Rotary-Club Frankfurt am Main Friedensbrücke

Dr. Daniel Korn 22.09.2022

1 Einleitung

Quantum Computing ist ein Begriff, der in letzter Zeit immer häufiger als Wegbereiter einer informationstechnologischen Revolution in den Medien gehypt wird, obwohl kaum jemand in der Lage ist, sich darunter etwas wirklich Konkretes vorzustellen. Wer sich ein wenig näher mit den Hintergründen dieser Technologie beschäftigt, wird relativ schnell erkennen, dass das kein Zufall ist. Die besagte Schwierigkeit, sich etwas darunter vorzustellen, geht nämlich letztlich auf die physikalischen Grundlagen zurück, auf denen diese Technologie beruht – allen voran die Quantenmechanik, deren Kern in gewisser Weise aus der Erkenntnis besteht, dass sich bestimmte physikalische Vorgänge kategorisch der Vorhersagbarkeit entziehen und damit – wenn man so will – prinzipbedingt nicht verstehbar sind. Dieses Paradoxon wird gerne dem Satz veranschaulicht: „wer behauptet, er habe die Quantenmechanik verstanden, der hat sie nicht wirklich verstanden".

Letztlich basiert Quantum Computing also darauf, dass man sich das geradezu mystische Verhalten der Elementarteilchen auf Quantenebene zunutze macht, um die Ergebnisse komplexer Berechnungen sozusagen „herbeizuzaubern", die auf konventionellem Wege nahezu unendlich viel Zeit in Anspruch nehmen würden. Das Potenzial dieser Technologie ist demnach enorm, denn sie ermöglicht grundsätzlich eine Berechnungsgeschwindigkeit, mit der bisher praktisch unlösbare Problemstellungen quasi im Handumdrehen gelöst werden könnten und stößt damit die Tür zu einer vollkommen neuen Welt der Informationstechnologie auf.

Es lohnt sich also, einen etwas genaueren Blick auf diese potenziell bahnbrechende Technologie zu werfen, weswegen sich dieser Vortrag genau dies zum Ziel gesetzt hat. Dazu soll mit einer kurzen Einführung in die Grundlagen des konventionellen computergestützten Rechnens begonnen werden, an die sich dann eine ebenso kurze Einführung in die für das Quantum Computing wesentlichen Aspekte der Quantenmechanik anschließt. Darauf basierend sollen dann die wesentlichen Prinzipien des Quantum Computings vorgestellt werden, bevor der Vortrag mit einem kurzen Ausblick auf das Potenzial dieser Technologie und ihren gegenwärtigen Entwicklungsstand seinen Abschluss findet.

2 Rechnen auf konventionellen Computersystemen

2.1 Binärdarstellung

So ziemlich jeder, der heutzutage ein Tablet, Desktop-Rechner, Laptop oder Smartphone besitzt, hat schon mal etwas von sogenannten Bits und Bytes gehört – meist in Form von Angaben über Speicherkapazität (z.B. „128 Giga**byte**“) oder Übertragungsgeschwindigkeiten für digitale Daten (z.B. „100 Mega**bit** pro Sekunde“). Was genau diese Bits und Bytes sind und welche Rolle sie für den Aufbau digitaler Rechnersysteme spielen, wissen hingegen die Wenigsten von uns. Im Folgenden soll daher ein kurzer Überblick darüber gegeben werden, was sich hinter diesen Begriffen verbirgt und welche Bedeutung sie für das maschinelle Rechnen haben.

Das Wort „Bit“ steht eigentlich für „**Bi**nary Digi**t**“ („Binärziffer“) und bezeichnet damit eine einzelne Ziffer innerhalb der sogenannten Binärdarstellung einer gegebenen Zahl. Diese unterscheidet sich von unserer alltäglich gewohnten Dezimaldarstellung für Zahlen dadurch, dass es statt der uns vertrauten zehn Ziffern „0“, „1“, „2“, … , „9“ lediglich zwei Ziffern gibt – die „0“ und die „1“.

Um beliebige Zahlen in der uns vertrauten Dezimaldarstellung darzustellen, zählt man zunächst die Ziffern einer gegebenen Stelle so lange hoch, bis die höchste verfügbare Ziffer – also die „9“ – erreicht ist. Dann setzt man die aktuelle Stelle wieder auf „0“ und erhöht die nächsthöhere Stelle auf deren Folgeziffer. Beispiel „18“, „19“, „20“.

In der Binärdarstellung verfährt man im Prinzip genauso, nur eben, dass man schon bei der „1“ an der höchsten verfügbaren Ziffer angekommen ist. Die uns vertrauten Dezimalzahlen „0“, „1“, „2“, „3“, „4“ und „5“ sehen daher in der Binärdarstellung so aus: „**0**“, „**1**“, „**10**“, „1**1**“, „**100**“ und „10**1**“. Schon bei der „1“ angekommen, sind uns die verfügbaren Ziffern ausgegangen. Daher zählt man die nächsthöhere Stelle um eins hoch (also von der gedachten „**0**“ auf die „**1**“) und setzt die aktuelle Stelle wieder auf „**0**“. Das ergibt „**10**“ und steht für die uns als Zwei bekannte Zahl. Man zählt dann wieder die kleinste Stelle um eins hoch und gelangt zur „1**1**“ – die Binärdarstellung der Zahl Drei. Nun muss man wieder die aktuelle Stelle auf „**0**“ setzen und die nächsthöhere um eins hochzählen. Da diese aber schon bei der höchsten Ziffer „**1**“ angekommen ist, setzt man auch diese wieder auf „**0**“ und erhöht die Folgestelle um eins. Im Ergebnis gelangt man zu „**100**“ – die Binärdarstellung unserer Vier. Die Binärdarstellung der Fünf entsteht dann dadurch, dass man die niedrigste Stelle wieder um eins hochzählt, wodurch man zu „10**1**“ gelangt.

Die Zusammenfassung von vier Binärstellen wird gemeinhin als „Nibble“ und zwei Nibbles zusammen (also acht zusammengefasste Binärstellen) als „Byte“ bezeichnet.

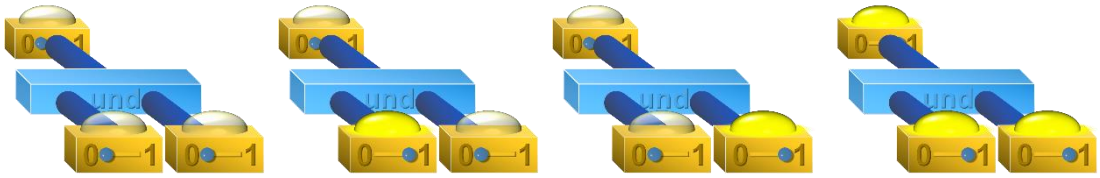
Der Nutzen der Binärdarstellung für digitale Rechnersysteme besteht nun darin, dass man jede Binärstelle durch ein einfaches elektronisches Schaltelement repräsentieren kann, so dass „0“ gleich „Schalter aus“ und „1“ gleich „Schalter ein“ bedeutet:

Würde man digitale Rechnersysteme stattdessen auf den uns vertrauten Dezimalstellen basierend aufbauen wollen, müsste jedes Schaltelement anstelle der zwei Zustände „aus“ und „an“ gleich zehn eindeutig unterscheidbare Zustände (also etwa zehn verschiedene Spannungsniveaus) annehmen können. Das führte indessen zu wesentlich aufwändigeren und fehleranfälligeren Rechnersystemen, weswegen sich das Binärsystem als Grundlage für Speicherung und Berechnung in Computersystemen universell durchgesetzt hat.

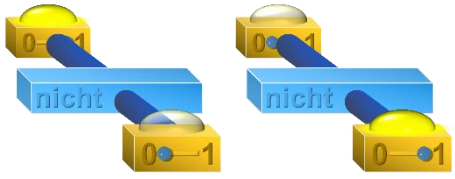
2.2 Binäre Verknüpfungen

Die eigentlichen Berechnungen mit den binären Zahlen werden in Computersystemen auf Basis der sogenannten „Boole’schen Algebra“ durchgeführt, welche die Regeln für die Verknüpfung zweier Binärwerte definiert. Als Verknüpfung zweier Werte bezeichnet man dabei den Vorgang, bei dem ein Binärwert in Abhängigkeit vom Zustand eines oder mehrerer gegebener Binärwerte (nachfolgend „Eingangswerte“ genannt) nach fest vorgegebenen Regeln den Zustand „0“ oder „1“ als Ergebniswert annimmt.

Ein Beispiel für so eine Verknüpfung ist die sogenannte „Konjunktion“ oder auch „Und“-Verknüpfung. Hier nimmt der Ergebniswert genau dann den Zustand „1“ an, wenn der erste **und** der zweite Eingabewert gleichzeitig den Zustand „1“ haben. Befindet sich mindestens einer der beiden Ausganswerte hingegen im Zustand „0“, bleibt das Ergebnis der „Und“-Verknüpfung „0“.

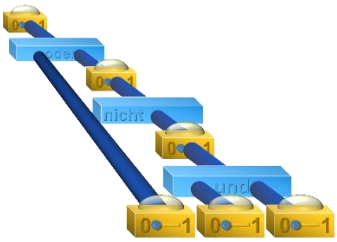


Ein anderes Beispiel ist die sogenannte „Disjunktion“ („Oder“-Verknüpfung“). Hier erhält der Ergebniswert immer dann den Zustand „1“ wenn sich mindestens einer der beiden Eingabewerte im Zustand „1“ befindet – also wenn sich der erste **oder** der zweite Wert (oder beide) im Zustand „1“ befinden. Eine weitere bekannte Verknüpfung ist die sogenannte „Negation“ oder auch „Nicht“-Verknüpfung. Sie hat nur einen Eingabewert, und ihr Ergebnis besteht gerade aus der Umkehrung dieses Wertes. Die Negation ist also immer „0“, wenn der Eingabewert **nicht** „0“ ist und immer „1“ wenn der Eingabewert **nicht** „1“ ist:

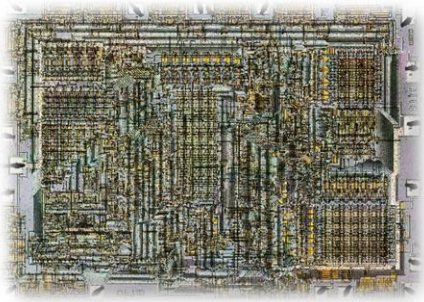


Die folgende Tabelle veranschaulicht die drei oben genannten Verknüpfungen:

Wert 1	Wert 2	Wert 1 Und Wert 2	Wert 1 Oder Wert 2	Nicht Wert 1
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0



Auf Basis solcher binären Verknüpfungen lassen sich dann letzten Endes sämtliche Rechenoperationen – wie etwa die Grundrechenarten – realisieren, indem man die Ergebniswerte solcher Verknüpfungen ihrerseits zu Eingabewerten weiterer Verknüpfungen macht, wodurch eine beliebig komplexe Verkettung verschiedener binärer Verknüpfungen erzeugt werden kann. Sämtliche digitalen Rechenwerke funktionieren nach genau diesem Prinzip und sind damit im Grunde nichts anderes als die komplexe Zusammenschaltung binärer Verknüpfungen.



3 Quantenmechanische Grundlagen

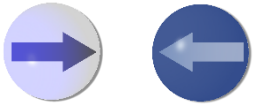
Die Anfang des 20. Jahrhunderts entstandene Quantenmechanik geht überwiegend auf die Werke von Werner Heisenberg, Max Born und Pascual Jordan sowie auf deren Weiterentwicklung durch Erwin Schrödinger zurück. Nachdem man festgestellt hatte, dass sich subatomare Teilchen – wie etwa Elektronen – in wesentlichen Bereichen grundlegend anders verhalten, als es mit den Mitteln der klassischen Physik erklärbar wäre, kam man zu dem Schluss, dass man bei diesen kleinsten Teilchen auf Phänomene gestoßen war, die einer entsprechenden Erweiterung der klassischen Physik bedurften.

3.1 Zustandsüberlagerung

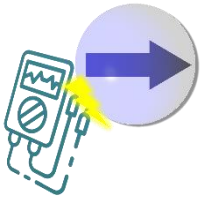
Das für das Quantum Computing wichtigste dieser Phänomene ist die sogenannte Überlagerung mehrerer Zustände, in denen sich solche kleinsten Teilchen zur gleichen Zeit befinden können. Dies steht im krassen Widerspruch zu unserer Alltagsintuition, laut derer sich jedes Ding zu einer gegebenen Zeit an einem gegebenen Ort in einem vorhersagbaren Zustand befindet. Wenn also beispielsweise ein Zug an einem bestimmten Ort um eine bestimmte Zeit mit vorgegebener Geschwindigkeit in eine bestimmte Richtung losfährt, können wir exakt vorausberechnen, wann er an welchem Ort ankommen wird. Insbesondere kann er nicht zur selben Zeit an zwei unterschiedlichen Orten sein.

Im Gegensatz dazu lassen sich Ort und Geschwindigkeit eines Elektrons gemäß der von Werner Heisenberg postulierten „Unschärferelation“ nicht gleichzeitig feststellen. Misst man den Ort, verändert man die Geschwindigkeit, misst man die Geschwindigkeit verändert man den Ort. Mehr noch: während man den Ort gemessen hat, hat das Elektron *zur gleichen Zeit beliebig viele Geschwindigkeiten auf einmal*, von denen manche mit höherer, manche mit geringerer

Wahrscheinlichkeit festgestellt werden, wenn man sie das nächste Mal misst. Während der Geschwindigkeitsmessung befindet sich das Elektron dagegen *gleichzeitig an beliebig vielen Orten*, an denen es mit unterschiedlichen Wahrscheinlichkeiten bei der nächsten Ortsmessung angetroffen wird.

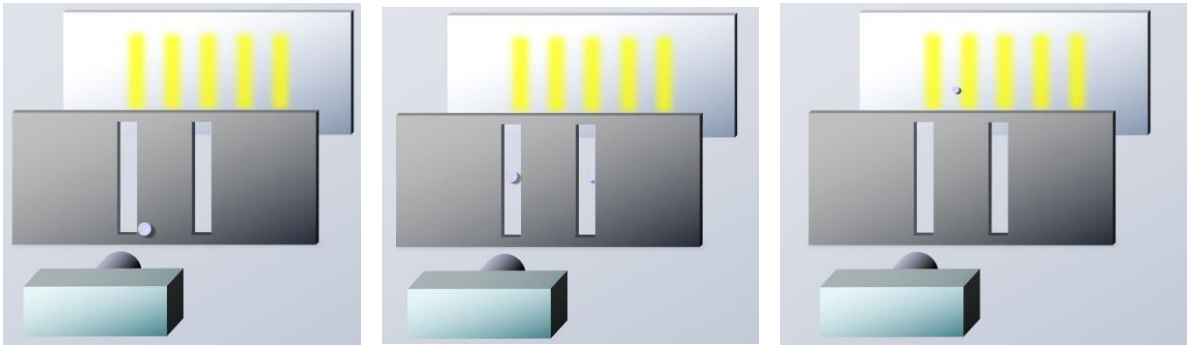


Ähnlich verhält es sich mit dem sogenannten „Spin“ eines Elektrons. Bei diesem handelt es sich um eine physikalisch nicht vollständig erklärbare Eigenrotation eines Elektrons, deren Existenz jedoch als Erklärung für eine bestimmte Form der Aufspaltung von Lichtwellen vorausgesetzt werden muss. Ein solcher Spin kann zwei unterscheidbare Richtungen haben. Auch hier gilt jedoch, dass die Spin-Richtung eines Elektrons erst dann feststeht, wenn sie gemessen wird. Ansonsten befindet sich jedes Elektron in einer Überlagerung beider Spin-Richtungen, dreht sich also gewissermaßen gleichzeitig in beide Richtungen.



Diese vollkommen kontraintuitiven Sichtweisen wurden von Albert Einstein Zeit seines Lebens abgelehnt („Gott würfelt nicht“), gelten aber heutzutage als gemeinhin anerkannt, obwohl niemand genau sagen kann, wie es möglich ist, dass sich ein und dasselbe Ding gleichzeitig in mehreren Zuständen befinden kann. Letztlich sind aber Elementarteilchen nicht einfach nur „kleine Murmeln“, sondern eine Art Zwitter aus Masse und Energie, so dass für sie andere Gesetzmäßigkeiten gelten, als für Masse, wie wir sie aus dem Alltag kenne.

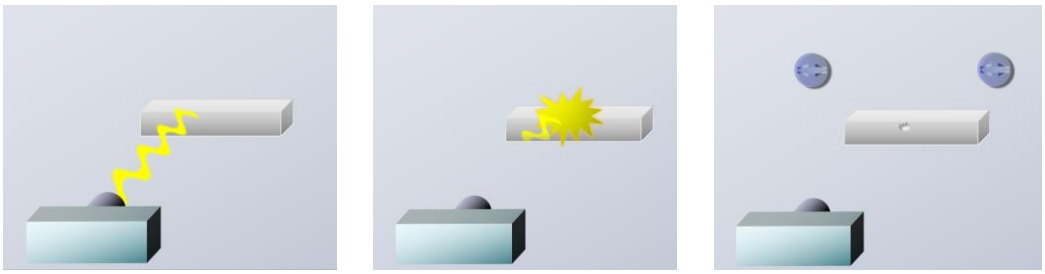
Ob man es verstehen bzw. akzeptieren will oder nicht – die Folgen dieser Phänomene lassen sich jedenfalls experimentell nachweisen. So kann man beispielsweise zeigen, dass ein Elektron, welches auf eine Scheibe mit zwei Schlitzen geschossen wird, gleichzeitig durch beide Schlitze hindurchgeht, sich also zur gleichen Zeit an mehreren Orten aufgehalten haben muss:



Aus Sicht des Quantum Computing genügt es jedenfalls, wenn man voraussetzt, dass es Objekte gibt, die sich gleichzeitig in mehreren Zuständen befinden können – und zwar so, dass jeder mögliche Zustand bei einer Zustandsmessung mit einer vorgegebenen Wahrscheinlichkeit gemessen wird. Was das konkret bedeuten soll, wird im nächsten Abschnitt genauer betrachtet.

3.2 Verschränkung

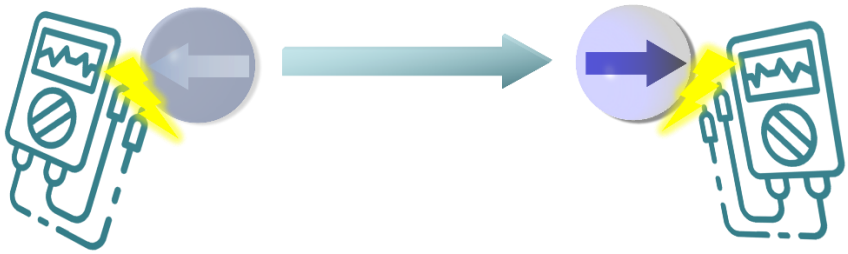
Noch erstaunlicher als die Zustandsüberlagerung ist die sogenannte Verschränkung der Zustände zweier ansonsten unabhängiger Objekte. Diese entsteht beispielsweise, wenn zwei Teilchen in einer bestimmten Weise gemeinsam aus einem Energieimpuls heraus erzeugt werden:



Sie haben dann die Eigenschaft, dass der Spin des einen Teilchens immer die gegensätzliche Richtung derjenigen des anderen Teilchens hat, sofern der Spin für beide Teilchen auf dieselbe Weise gemessen wird – und zwar unabhängig davon, wie weit diese beiden Teilchen bei den jeweiligen Messungen voneinander entfernt sind. Die Spin-Zustände beider Teilchen sind also auf sondersame Weise miteinander verschränkt.

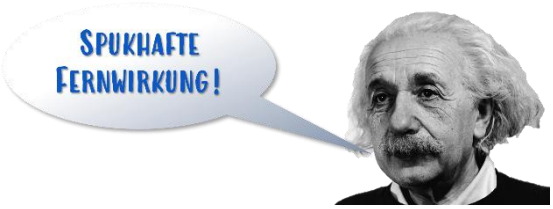
Im Klartext bedeutet das, dass sich beide Teilchen bis zur Messung ihres Spins jeweils in einem Überlagerungszustand beider Spins befinden – sich also jeweils in beide möglichen Richtungen gleichzeitig drehen:

Misst man jetzt den Spin des einen Teilchens und legt hin dadurch erst fest, so steht bereits an diesem Punkt fest, dass bei der Spin-Messung des anderen Teilchens die entgegengesetzte Richtung festgestellt werden wird, selbst wenn dieses Teilchen sich noch im überlagerten Zustand beider Spin-Richtungen befindet:



Das zweite Teilchen scheint also auf mysteriöse Weise zu „wissen“ welcher Spin sich bei der Messung des ersten Teilchens ergeben hat und sorgt auf ebenso mysteriöse Weise dafür, dass es bei der Messung des eigenen Spins die entgegengesetzte Drehrichtung einnehmen wird.

Auch gegen dieses Phänomen hat sich Albert Einstein Zeit seines Lebens gewehrt und darin eine „spukhafte Fernwirkung“ gesehen. Es steht aber heute durch immer wieder reproduzierbare Experimente fest, dass es eine solche Wirkung gibt, auch wenn sie nicht auf zufriedenstellende Weise erklärt werden kann.



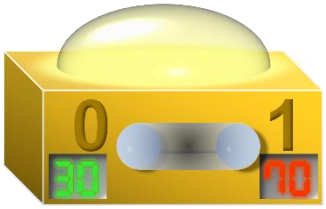
Aus Sicht des Quantum Computings genügt es wiederum, davon auszugehen, dass man Teilchenpaare erschaffen kann, die sich jeweils in einer Überlagerung zweier Zustände befinden,

so dass die Messung des Zustands eines Teilchens eine sichere Vorhersage darüber erlaubt, in welchem Zustand sich das andere Teilchen befindet.

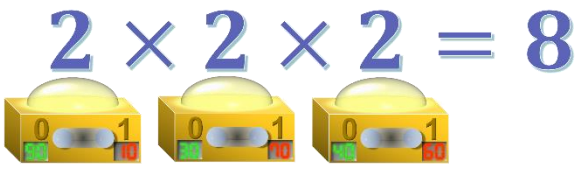
4 Prinzipien des Quantum Computings

4.1 Qubits

Während konventionelle Rechnersysteme letztlich auf Bits in Form binärer Schaltzustände beruhen, die mittels elektronischer Schaltungen miteinander verknüpft werden, bauen Quantenrechner demgegenüber auf sogenannten Qubits auf. Anstelle eines Bits, das sich zu jeder Zeit in einem der beiden definierten Zustände „an“ oder „aus“ (bzw. „1“ oder „0“) befindet, verwendet man im Quantenrechner Qubits, die sich bis zur Messung ihres Zustands ein einem überlagerten Zustand aus „an“ und „aus“ bzw. „1“ und „0“ befinden. Qubits sind also bis zur Messung ihres Zustands gleichzeitig „0“ und „1“. Man kann lediglich jedem Qubit eine Wahrscheinlichkeit dafür zuordnen wie häufig es sich bei der Messung im Zustand „1“ bzw. „0“ befinden wird. Diese Wahrscheinlichkeiten kann man zudem durch geeignete Operationen auf solchen Qubits beeinflussen.



Interessant werden die Qubits dann, wenn man mehrere von ihnen gleichzeitig betrachtet. So können sich zwei Qubits zusammen gleichzeitig in vier verschiedenen Zuständen befinden, nämlich „00“, „01“, „10“ und „11“. Eine Kombination aus drei Qubits kann sich demnach gleichzeitig in acht verschiedenen Zuständen befinden. Allgemein kann sich eine Kombination aus n Qubits daher gleichzeitig in 2^n Zuständen befinden.



Dieses Phänomen macht man sich bei Quantencomputern dahingehend zunutze, dass man die Qubits zur Berechnung bestimmter Fragestellungen in einer Weise miteinander verknüpft, die zunächst keine Zustandsmessung der Qubits voraussetzt. Damit wird prinzipiell erreicht, dass etwa bei einer Eingabelänge von n Qubits die gewünschte Berechnung gleichzeitig für alle 2^n verschiedenen Zustände der Eingabedaten durchgeführt werden kann.

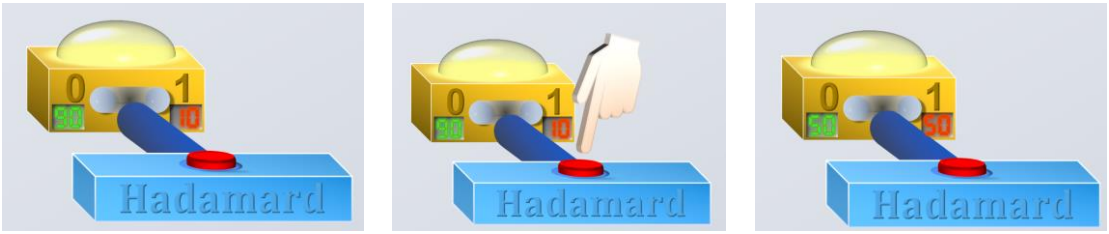
Wie das grundsätzlich funktioniert, soll im folgenden Abschnitt betrachtet werden.

4.2 Quantenberechnung

Ähnlich wie bei konventionellen Rechnersystemen können Qubits als Eingabewerte für bestimmte Operationen verwendet werden, durch die entweder sie selbst oder ein anderes Qubit in Abhängigkeit vom eigenen Zustand verändert wird. Allerdings werden diese Operationen bzw. Verknüpfungen so gewählt, dass sie nicht vom eigentlichen Zustand der Eingabe-Qubits abhängen, denn dazu müsste dieser ja gemessen werden, wodurch die Überlagerung der Zustände aufgelöst und damit die gleichzeitige Betrachtung vieler Zustände unmöglich gemacht

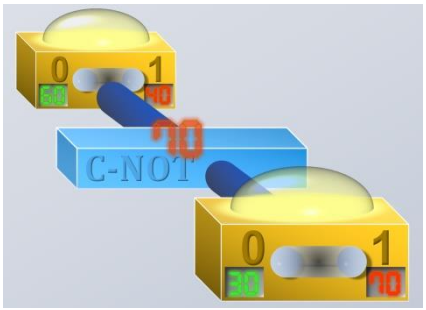
würde. Vielmehr zielt man mit den Qubit-Verknüpfungen darauf, die Wahrscheinlichkeiten zu beeinflussen, mit denen bei einer späteren Zustandsmessung ein bestimmter Zustand festgestellt wird. Dafür gibt es verschiedene Operationen und Verknüpfungen, von denen im Folgenden einige Beispiele präsentiert werden sollen.

1. **Hadamard-Gatter**
   Das Hadamard-Gatter versetzt ein gegebenes Qubit in eine Zustandsüberlagerung, die so beschaffen ist, das beide Zustände „0“ und „1“ mit identischer Wahrscheinlichkeit gemessen werden. Die Wahrscheinlichkeit, bei einer Zustandsmessung „0“ bzw. „1“ zu erhalten, beträgt bei derart manipulierten Qubits also jeweils 50%.

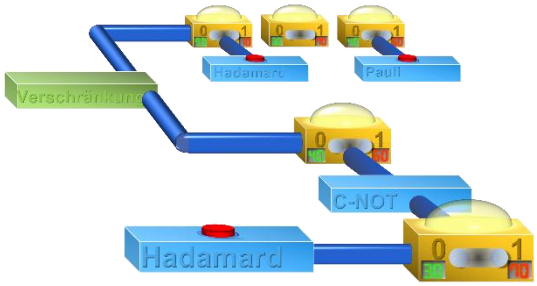


2. **Pauli-Gatter**
   Das Pauli-Gatter vertauscht für ein gegebenes Qubit die Wahrscheinlichkeiten der Messung von „0“ und „1“. War also etwa vor der Anwendung des Pauli-Gatters die Wahrscheinlichkeit eine „0“ zu messen bei 40% und demzufolge die Wahrscheinlichkeit, eine „1“ zu messen, bei 60%, so ist nach Anwendung des Pauli-Gatters die Wahrscheinlichkeit, eine „0“ zu messen, bei 60% und demnach die Wahrscheinlichkeit, eine „1“ zu messen, bei 40%.

3. **Kontrolliertes NOT-Gatter**
   Das kontrollierte NOT-Gatter wirkt im Prinzip auf ein gegebenes Qubit wie ein Pauli-Gatter, vertauscht also wiederum für ein gegebenes Qubit die Wahrscheinlichkeiten der Messung von „0“ und „1“. Allerdings tut es das in Abhängigkeit von einem weiteren Qubit, dem sogenannten Kontroll-Qubit, und zwar so, dass das zu manipulierende Qubit nur vom „1“-Zustand des Kontroll-Qubits beeinflusst wird. Die Wahrscheinlichkeiten für die Zustandsmessungen werden also nur in Höhe der Wahrscheinlichkeit vertauscht, mit der die Zustandsmessung des Kontroll-Qubits „1“ ergeben würde. Das kontrollierte NOT-Gatter ist also ein Gatter, das tatsächlich zu einer gewissen Verknüpfung von zwei Qubits führt.



Mit Hilfe solcher Gatter kann man also die Eingabe-Qubits der gewünschten Berechnung Schritt für Schritt so beeinflussen bzw. miteinander verknüpfen, dass die Zustandsmessung



der Ausgabe-Qubits am Ende einer entsprechenden Gatter-Struktur mit einer hohen Wahrscheinlichkeit das Ergebnis liefern, das man letztlich mit der Gatter Struktur berechnen möchte. Die Kunst besteht hier also darin, die Gatterstruktur so zu wählen, dass eben diese gewünschte hohe Wahrscheinlichkeit für die Messung des angestrebten Berechnungsergebnisses entsteht. Eine derart konstruierte Gatterstruktur nennt man daher „Quanten-Algorithmus“, da er im Wesentlichen dem entspricht, was Algorithmen auf konventionellen Computern bewerkstelligen.

Im krassen Gegensatz zu den Algorithmen konventioneller Computer ist man bei Quantenalgorithmen indessen derzeit noch in einem Stadium, das den frühesten konventionellen Rechenautomaten entspricht, die mal also durch das Zusammenschalten von Logikgattern programmiert hat. Von symbolischen Programmiersprachen – geschweige denn von abstrakten Programmiersprachen – kann hier also noch lange nicht die Rede sein. Zwar gibt es durchaus programmiersprachliche Umsetzungen für die Zusammenstellung eines Quantenalgorithmus, aber sie stellen letztlich nur ein programmiersprachliches Werkzeug zur Beschreibung der besagten Gatterstrukturen dar. Für die Programmierung von Quantencomputern muss man nach wie vor sehr stark im Sinne von Qubits, Zustandswahrscheinlichkeiten und Gattern und damit sehr weit entfernt von der Begriffswelt des zu berechnenden Problems denken, während die Programmierung konventioneller Rechner heute mittels sehr viel abstrakterer Konzepte erfolgt, die gezielt darauf zugeschnitten sind, die Begriffswelt der zu berechnenden Problemstellungen wiederzugeben.

5 Chancen des Quantum Computings

Wie im vorangegangenen Abschnitt dargelegt, sind Quantencomputer grundsätzlich in der Lage, Berechnungen für sämtliche möglichen Zustandskombinationen der Eingabe-Qubits gleichzeitig anzustellen. Bei gegebenen n Eingabe-Qubits können damit alle 2^n möglichen Kombinationen an Zuständen der Qubits in einem Zug untersucht werden. Das verschafft Quantencomputern also prinzipiell einen exponentiellen Geschwindigkeitsvorteil gegenüber konventionellen Rechnersystemen!

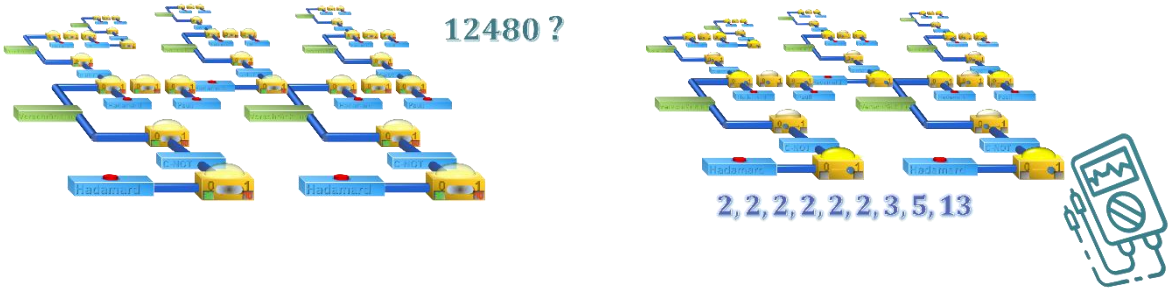
Besonders interessant ist dieses Potenzial für die sogenannten NP-vollständigen Probleme. Es handelt sich dabei um einen Begriff aus der sogenannten Komplexitätstheorie, und er beschreibt eine Klasse von Problemen, für die bis heute keine effizienten Berechnungsverfahren auf konventionellen Rechnern bekannt sind. Gleichzeitig kann man aber zu einem gegebenen Lösungsvorschlag für ein solches NP-vollständiges Problem sehr effizient feststellen, ob es sich tatsächlich um eine Lösung des betreffenden Problems handelt. Bis heute ist die Frage offen, ob es effiziente Berechnungsverfahren für die NP-vollständigen Probleme gibt, und diese Frage wurde daher vom Clay Mathematics Institute in die Liste der sieben sogenannten „Millenium-Probleme“ aufgenommen, auf deren Lösung jeweils ein Preisgeld von einer Million US-Dollar ausgelobt wurde.

Gäbe es ein effizientes Berechnungsverfahren für die NP-vollständigen Probleme, so wären beispielsweise die heute im Internet gebräuchlichen Verschlüsselungsverfahren weitgehend

wertlos, da sie auf einem solchen NP-vollständigen Problem beruhen – nämlich der Primfaktorzerlegung einer gegebenen Zahl. Für diese ist bis heute kein effizientes Verfahren bekannt, so dass man mit extrem langen Berechnungszeiten zu rechnen hätte, wenn man die sogenannten privaten Schlüssel der im Internet gebräuchlichen Verschlüsselungsverfahren knacken wollte. Hat man hingegen einen Satz Primfaktoren vorliegen, lässt sich sehr effizient prüfen, ob es sich tatsächlich um eine gültige Zerlegung einer gegebenen Zahl handelt, indem man nämlich einfach alle Faktoren miteinander multipliziert und das Ergebnis mit der zu zerlegenden Zahl vergleicht:

$$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 5 \times 13 = 12480$$

Was wäre nun aber, wenn man alle möglichen Primfaktorzerlegungen gleichzeitig durch eben jene simple Multiplikation daraufhin prüfen könnte, ob das Multiplikationsergebnis der zu zerlegenden Zahl entspricht? Dann hätte man im Nu die Lösung des Problems und unsere gängigen Verschlüsselungsverfahren wären wertlos. Und genau hier liegt das enorme Potenzial der Quantencomputer. Wenn es gelänge, einen solchen Computer mit genügend vielen Qubits zu bauen (es müssten nicht viel mehr als einige tausend sein), könnte man mit geeigneten Quantenalgorithmen praktisch alle möglichen Primfaktorzerlegungen gleichzeitig daraufhin überprüfen, ob ihre Multiplikation der zu zerlegenden Zahl gleicht.



Die Frage, ob und warum es erstrebenswert sein sollte, unsere üblichen Verschlüsselungsverfahren auf diese Weise auszuhebeln, mag dahingestellt bleiben. Letztlich ist die Primfaktorzerlegung nur ein Lehrbeispiel für das extreme Rechenleistungspotenzial, das in der Quantencomputer-Technologie steckt. Quantencomputer mit entsprechend großer Menge an Qubits und passenden Algorithmen hätten jedenfalls das Potenzial, unsere heute verfügbare Rechenleistung exponentiell zu steigern – zumindest für Problemstellungen, bei denen das extreme Parallelisierungspotenzial der Quantencomputer sinnvoll ausgespielt werden kann. Mögliche Anwendungsgebiete dieser Art wären etwa bestimmte Such- und Optimierungsverfahren, bestimmte Probleme des maschinellen Lernens oder Simulationen biochemischer Stoffe, für die konventionelle Rechner prinzipbedingt niemals genügend Rechenleistung werden aufbringen können.

6 Gegenwärtiger Entwicklungsstand

Obwohl Quantencomputer – wie oben dargelegt – theoretisch ein enormes Potenzial an Rechenleistung liefern können, stellt sich der tatsächliche Bau solcher Rechner als nicht zu unterschätzendes Problem dar. Derzeit werden viele verschiedene Möglichkeiten untersucht, Qubits technisch zu realisieren. Eine davon besteht etwa darin, den Spin einzelner Elektronen von Phosphoratomen, die in ein Stück Siliziumkristall eingebettet sind, mit Hilfe hochfrequenter Mikrowellenstrahlung zu manipulieren. Phosphoratome eignen sich besonders für diesen Zweck, da ihre äußere Hülle lediglich ein einzelnes Elektron enthält. Das Auslesen des Spins kann dann mittels eines Transistors erfolgen, der um das Siliziumkristall-Stück mit dem Phosphoratom herum angelegt ist. Nachteil dieser Vorgehensweise ist sehr kurze Dauer, in der ein derart manipuliertes Elektron seinen Spin beibehält.

Aus diesem Grund hat man mit Kernen von Phosphor-Atomen experimentiert, denen ebenfalls einen Spin verleihen bzw. deren Spin man messen kann. Der Kernspin ist allerdings um Größenordnungen schwächer als der Elektronenspin, so dass entsprechend mehr Aufwand zum Auslesen des Spins getroffen werden muss. Demgegenüber sind die Kernspins deutlich stabiler, so dass Qubits auf Kern-Basis entsprechend langlebiger sind.

Einen ganz anderen Weg geht man mit den sogenannten Ionenfallen. Hier werden geladene Kalzium-, Barium- oder Berylliumatome – also Ionen – dergestalt in einem kryogenen, vakuumisierten Magnetfeld gehalten, dass sie isoliert von sämtlichen umgebenden Teilchen verharren können. In diesem Zustand kann man sie durch Bestrahlung mit Mikrowellen oder Laserlicht wahlweise in einen angeregten, nicht angeregten oder auch überlagerten Zustand versetzen und damit das gewünschte Qubit-Verhalten hervorrufen. Das Auslesen des Zustands erfolgt ebenfalls über gezielten Laserbeschuss, als dessen Ergebnis sich einzelne Photonen lösen, die man über eine geeignete Optik einfangen und detektieren kann.

Einen wiederum ganz anderen Weg geht man mit den supraleitenden Qubits. Sie basieren auf mikroskopisch kleinen supraleitenden Stromkreisen aus Aluminium, die von Kondensatoren und sogenannten Josephson-Kontakten unterbrochen sind. Bei letzteren handelt es sich gewissermaßen um das supraleitende Äquivalent einer Induktionsspule (sogenannte „nichtlineare Induktoren“). Werden solche supraleitenden Kreise mit bestimmten Mikrowellenfrequenzen angeregt, beginnt der Stromfluss in ihnen zu oszillieren und wechselt damit in den nächsthöheren Energiezustand. Der energielose Zustand (also ohne oszillierenden Strom) entspricht dabei dem Zustand „0“ des Qubits und das nächsthöhere Energieniveau dem Zustand „1“ des Qubits. Diese Zustände lassen sich durch spezielle Eigenschaften der Josephson-Kontakte quantenmechanisch Überlagern. Das Auslesen solcher Qubits erfolgt durch Messung des magnetischen Flusses durch den Schaltkreis.

Es gibt noch eine Reihe weiterer technischer Realisierungen von Qubits. Allen gemeinsam ist der immens hohe technische Aufwand, der neben der aufwändigen Kühlung supraleitender Schaltkreise oder Magneten in der nicht minder aufwändigen Apparatur zur Steuerung und Auslesung der Qubits zum Ausdruck kommt. Im Vergleich zu konventionellen Rech-

nersystemen befinden wir uns also bei Quantenrechnern derzeit auf dem Niveau des Relais-Rechners von Konrad Zuse bzw. des Elektronenröhren-basierten ENIAC-Systems von John Presper Eckert und John William Mauchly aus den 1940er Jahren.

Dementsprechend ist auch die Menge an praktisch nutzbaren Qubits in aktuellen Quantenrechnern immer noch sehr gering. So ist es Google im Jahre 2018 gelungen, einen Quantenrechner mit 72 Qubits zu bauen, der mit sehr hohen Zuverlässigkeitsraten für das Auslesen und Beschreiben von Qubits aufwartet. IBM hat Ende 2021 einen Rechner mit 127 Qubits präsentiert. Die kanadische Firma Xanadu hat im Jahre 2022 einen Rechner mit 216 Qubits vorgestellt, der die sogenannte Quantenüberlegenheit demonstrieren soll – also die praktisch nachweisbare Überlegenheit von Quantencomputern gegenüber herkömmlichen Systemen. So soll der „Borealis“ getaufte Rechner ein bestimmtes Problem in nur 36 Mikrosekunden gelöst haben, für das konventionelle Rechner über 9.000 Jahre benötigen würden.

Abschließend kann festgehalten werden, dass das theoretische Potenzial von Quantencomputern derzeit noch an praxisrelevanten Problemstellungen nachgewiesen werden muss. Dazu bedarf es zuverlässiger technischer Lösungen mit genügend vielen vernetzten Qubits ebenso wie einer problemorientierteren Programmiersprache für Quantenalgorithmen.

7 Quellen

- http://www.quantencomputer-info.de/quantencomputer/quantencomputer-einfach-erklaert/
- https://de.wikipedia.org/wiki/Liste_der_Quantengatter#Quantengatter_mit_zwei_Eing%C3%A4ngen
- https://de.wikipedia.org/wiki/Quantenmechanik
- https://de.wikipedia.org/wiki/Quantenverschr%C3%A4nkung
- https://en.wikipedia.org/wiki/List_of_quantum_processors
- https://en.wikipedia.org/wiki/Quantum_computing
- https://en.wikipedia.org/wiki/Quantum_logic_gate
- https://en.wikipedia.org/wiki/Superconducting_quantum_computing
- https://physics.stackexchange.com/questions/298518/how-are-quantum-qubits-implemented
- https://physicstoday.scitation.org/do/10.1063/PT.5.026373/full/
- https://www.quantum-inspire.com/kbase/cnot/
- https://www.quarks.de/technik/faq-so-funktioniert-ein-quantencomputer/
- https://www.wissenschaft-x.com/xanadu-quantum-computer-borealis-computational-advantage
- https://www.youtube.com/watch?v=aV1wL5jsfRU

- https://www.youtube.com/watch?v=g_IaVepNDT4
- https://www.youtube.com/watch?v=uPw9nkJAwDY
- https://www.youtube.com/watch?v=zNzzGgr2mhk
- https://www.youtube.com/watch?v=ZuvK-od647c