Technology
Arts Sciences
TH Köln

Quantencomputer Verstehen

Ben Konrad Meyer Mike Springer
Kai Kawamura Julian Heidenreich

Modul: Verteilte Systeme

Dozent: Lutz Köhler

14. März 2025

Inhaltsverzeichnis

1 Einführung in die Quanteninformatik

1.1 Quantenbits

Ein Quantenbit, im Folgenden auch Qubit genannt, ist das Medium und die kleinste Einheit, auf dem in der Quanteninformatik gerechnet wird. Auf die genaue physische Realisierung wird in einem späteren Abschnitt der Quantenhardware eingegangen. Bis dahin reicht es das Quantenbit als eine Art Computer-Bit zu verstehen, das sich in einer sogenannten "Superposition" befindet. Im Zustand der Superposition kann es gleichzeitig den Wert ‚0' und ‚1' annehmen. Ein Quantenbit bleibt in dieser Superposition, bis es gemessen wird, woraufhin die Superposition zerstört wird und das Qubit einen der Zustände 0 oder 1 annimmt. Die Wahrscheinlichkeit, mit der ein Quantenbit in den einen oder anderen Zustand zerfällt, muss nicht gleich verteilt sein und kann beeinflusst werden. Dies macht Berechnungen auf Qubits erst möglich.

Mathematisch betrachtet, werden die Zustände ‚0' und ‚1' in der Quanteninformatik als Vektoren $\binom{1}{0} \equiv 0$ und $\binom{0}{1} \equiv 1$ dargestellt. Für die einfache Lesbarkeit werden diese Vektoren in der Quanteninformatik in der Bra-Ket-Notation dargestellt. Also $\binom{1}{0} \equiv |0\rangle$ und $\binom{0}{1} \equiv |1\rangle$.

Um die Wahrscheinlichkeit zu beschreiben, welchen der beiden Werte ein Quantenbit nach der Messung annimmt, werden beiden Werten eine Amplitude α oder β zugeordnet. Demnach wird ein Quantenbit in einer beliebigen Superposition als $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ dargestellt. α und β sind komplexe Zahlen für die $|\alpha|^2 + |\beta|^2 = 1$ gilt.
Ein Qbit, das nach der Messung mit gleicher Wahrscheinlichkeit in einen der beiden Zustände 0 und 1 zerfällt, würde folglich als $\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$ oder $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ dargestellt werden. Dabei gilt $\alpha = \beta = \frac{1}{\sqrt{2}}$ und erfüllt die Bedingung $\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = 1$.

Ein Vektor $\binom{\alpha}{\beta}$ wird als " Zustandsvektor" bezeichnet und stellt den Zustand der Superposition eines Qubits dar. Die Bedingung $|\alpha|^2 + |\beta|^2 = 1$ sorgt dafür, dass der Zustandsvektor immer ein Einheitsvektor ist. Dadurch kann jeder Zustand eines Qubits auf dem Einheitskreis eines zweidimensionalen Vektorsystems dargestellt werden. Somit kann ein Quantenbit unendlich viele Zustände haben, die auf einen definierten Bereich abgebildet werden können.

Kommentar

Zu dem Zeitpunkt, als wir uns das Grundwissen erarbeitet haben, war uns nicht klar, weshalb α und β komplexe Zahlen sein müssten und warum sie „Amplituden“ und nicht „Wahrscheinlichkeiten“ oder Ähnliches genannt werden. Wir gingen davon aus, dass wir früher oder später auf einen Use Case stoßen würden, in denen komplexe Zahlen und Amplituden wichtig werden. Dies war allerdings nur für letztes bedingt der Fall. Um kurz vorzugreifen: Amplituden von zwei Qubits können miteinander summiert werden. Dadurch ist es möglich, dass sich manche Amplituden gegenseitig aufheben. Dies wäre mit Wahrscheinlichkeitsverteilungen, die nicht negativ sein dürften, schwer darzustellen. Siehe dazu Erklärung des Mach-Zehnder-Interferometer (S. 255).
Warum α und β komplexe Zahlen sind, war schwer greifbar. Scheinbar hat dies mit der der Quanteninformatik zugrundeliegenden Quantenmechanik zu tun. Nach etwas Recherchearbeit stellte sich heraus, dass eine Antwort auf diese Frage einiges an Vorwissen in der Physik bedurfte. Da wir uns diese Frage am Anfang des Lernprozesses stellten und noch dabei waren in den Konzepten der Quanteninformatik Fuß fassen, entscheiden wir uns auf diese Frage zurück zu kommen, sobald komplexe Zahlen relevant werden würden. Da in der Quanteninformatik mit α und β allerdings gerechnet wird, als seien sie reelle Zahlen[a] und nur für die Umstellung der Formeln die Rechenregeln für komplexe Zahlen genutzt werden[b], trat dieser Fall nie wirklich ein.
Während der Erstellung dieses Dokuments haben uns unsere erlangten Kenntnisse beim Verstehen der Quantenmechanik nicht sonderlich weiter helfen können, um eine zufriedenstellende Antwort zu formulieren. Da es sehr zeitaufwändig geworden wäre, sämtliche Begrifflichkeiten wie aus dem Kurs Skript von John D Stack[c] zu verstehen, nur um diese Frage zu klären, entscheiden wir uns dieser nicht weiter nachzugehen. Das, was wir uns zusammen reimen konnten, ist, dass der Zustand von Partikeln in der Quantenmechanik als Wellenfunktion dargestellt wird. Um mit diesen rechnen zu können, ist der Imaginärteil der komplexen Zahlen notwendig. Es wäre sicherlich hilfreich gewesen die quantenmechanischen Hintergründe zu verstehen, bevor wir uns mit der Quanteninformatik auseinander gesetzt haben, allerdings hätte dies den Rahmen unseres Themas deutlich gesprengt.

[a] Vgl. Urenda, Julio C./Vladik Kreinovich: Topological Explanation of Why ComplexNumbers Are Needed in Quantum Physics, El Paso, Texas: The University of Texas at El Paso, 2023, https://www.cs.utep.edu/vladik/2023/tr23-44.pdf (abgerufen am 31.01.2025)

[b] Vgl: Homeister, Matthias: Quantum Computing verstehen Grundlagen – Anwendungen – Perspektiven, Wiesbaden: Springer Vieweg, 2022, S. 22.

[c] Vgl: Stack, John D: Ohne Titel, Chicago, Illinois: The Grainger College of Engineering, 2013, https://courses.physics.illinois.edu/phys580/fa2013/susy_v2.pdf (abgerufen am 31.01.2025)

Um mit Quantenbits rechnen zu können, muss man den Zustand eines Quantenbits verändern können. Wie dies technisch umgesetzt wird, wird später angerissen. Aus mathematischer Sicht geschieht dies über unitäre 2×2 Matrizen.

Eine Matrix A ist dann unitär, wenn ihre inverse Matrix A^{-1} gleich ihrer adjungierten Matrix $A^\dagger$ ist. Adjungiert ist eine Matrix $A^\dagger$ dann, wenn die Matrix A komplex konjugiert – also jedes Element der Matrix $z_{ij} = a + ib$ zu $z^*_{ij} = a \breve{} ib$ komplex konjugiert – und die Matrix dann transponiert wird. Also muss für alle Matritzen A gelten:

$$A^{-1} = (A^*)^T = A^\dagger \tag{1}$$

Für die Quanteninformatik reicht oft die Bedingung $A^{-1} = A^T$, da hier meist mit α und β gerechnet wird, als seien sie reelle Zahlen. Durch diese Bedingung haben unitäre Matrizen die Eigenschaft, dass ein Zustandsvektor unverändert bleibt, wenn eine unitäre Matrix zwei Mal mit ihm verrechnet wird.
Unitäre Transformationen sind also reversibel. Diese Bedingung ist notwendig, um die Länge der Zustandsvektoren beizubehalten.
Beispielhaft kann dies an einer Matrix

$$B = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \tag{2}$$

demonstriert werden. Wendet man diese Matrix auf ein Qubit im Zustand $|0\rangle$ an, transformiert sie es in den Zustand $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Diese Transformation wird über eine Multiplikation beschrieben:

$$B|0\rangle = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \tag{3}$$

Daraus ergibt sich: $\alpha = \frac{1}{2}$ und $\beta = \frac{\sqrt{3}}{2}$. Die Bedingung $|\alpha|^2 + |\beta|^2 = 1$ trifft für beide Zustandsvektoren $\binom{1}{0}$ und $\binom{\frac{1}{2}}{\frac{\sqrt{3}}{2}}$ zu. Zudem ist B unitär, da $B = B^T = B^{-1}$, und daher eine zulässige Transformation.
Wendet man die Transformation B erneut an, ergibt sich folgendes:

$$B\begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{4}$$

Der Ursprungszustand ist mit der zweiten Anwendung der Transformation wiederhergestellt. Dies ist eine der Grundprinzipien der Quanteninformatik.

1.2 Hadamard-Matrix

Eine unitäre Transformation, die im Laufe unseres Lernprozesses immer wieder vorgekommen ist, ist die sogenannte "Hadamard-Matrix":

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{5}$$

Multipliziert mit einem Qubit im Zustand $|0\rangle$ transformiert sie es in den Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und mit einem im Zustand $|1\rangle$ multipliziert transformiert sie es in den Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Beide Folgezustände haben die gleiche Wahrscheinlichkeit bei der Messung einen der Zustände $|0\rangle$ oder $|1\rangle$ anzunehmen.

Kommentar

Beide Zustände, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ unterscheiden sich nur im Vorzeichen der β-Amplitude. Würde man die Amplituden als Wahrscheinlichkeiten darstellen (zum Beispiel als $0.5 \cdot |0\rangle + 0.5 \cdot |1\rangle$), ließe sich bei der erneuten Hadamard-Transformation nicht eindeutig feststellen, in welchem Zustand sich das Bit vor der ersten Transformation befunden hat. Da die Umkehrbarkeit der Transformationen eine der Grundprinzipien der Quanteninformatik ist, wäre eine Darstellung mit Wahrscheinlichkeitsverteilungen auch ohne die zugrundeliegende quantenmechanische Notwendigkeit für Amplituden eher unpraktisch.

Mit dieser Gleichverteilung der Wahrscheinlichkeiten ließe sich beispielsweise ein Münzwurf simulieren. Der Schaltkreis eines Münzwurf Algorithmus sieht folgendermaßen aus[1]:

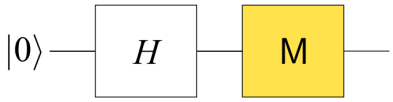

Abbildung 1: Schaltkreis für den Münzwurf Algorithmus

Schaltkreise eigenen sich dafür Quantenalgorithmen zu veranschaulichen. Auf diese wird später genauer eingegangen.

Zuerst wird ein Quantenbit in den Zustand $|0\rangle$ gebracht. Man könnte es auch in den Zustand $|1\rangle$ versetzen. Das macht für diesen Algorithmus keinen Unterschied. Danach wendet man die Hadamard-Transformation darauf an, um das Quantenbit in eine Superposition zu bringen, in der die Wahrscheinlichkeit $|0\rangle$ oder $|1\rangle$ zu messen gleich verteilt ist. Anschließend wird gemessen und die Superposition zerfällt zufällig in einen der Zustände $|0\rangle$ oder $|1\rangle$.
Formal beschrieben sieht der Algorithmus so aus:

$$\begin{aligned} |x\rangle &\leftarrow |0\rangle \\ |x\rangle &\leftarrow H\,|x\rangle \\ &Miss\,|x\rangle \end{aligned}$$

„$|x\rangle$“ ist dabei die Bezeichnung des Quantenbits auf dem gerechnet wird.
Mit diesem Algorithmus ist es möglich echte Zufallszahlen zu generieren, da es physikalisch unmöglich ist vorauszusagen, in welchen Zustand die Superposition zerfallen wird. Dies steht im Gegensatz zu einem echten Münzwurf, bei dem man das Wurfergebnis theoretisch berechnen könnte, wenn man sämtliche Variablen, wie z.B. Wurfhöhe, Drehmoment der Münze, Luftwiederstand, ect. kennen würde. Oder im Gegensatz zu einem herkömmlichen Computer, der nur Pseudozufallszahlen generieren kann.

[1] Vgl: Homeister, 2022, S. 27.

1.3 Quantenregister

Ein Quantenregister ist eine Aneinanderreihung mehrerer, voneinander unabhängiger Quantenbits. Diese werden benötigt, um Quantenschaltkreise zu realisieren, damit auf ihnen logische Operationen durchgeführt werden können.
Der Zustand eines Quantenregisters der Länge m wird als m-faches Tensorprodukt aller Zustände der einzelnen Quantenbits des Registers dargestellt. Ein Quantenregister R mit 2 Qubits $|x_0\rangle$ und $|x_1\rangle$ in beispielsweise den Basiszuständen $|x_0\rangle = \binom{0}{1}$ und $|x_1\rangle = \binom{1}{0}$ befindet sich im Zustand:

$$R = |x_0\rangle \otimes |x_1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \tag{6}$$

Alternativ würde man $R = |1\rangle \otimes |0\rangle = |10\rangle$ schreiben. Manchmal werden die Basiszustände zur Übersichtlichkeit auch in Dezimalform dargestellt. $|10\rangle$ wäre demnach $|2\rangle$.

Wie auch die einzelnen Qubits, kann sich das gesamte Quantenregister in einer Superposition befinden. Sind die Qubits aus dem obigen Beispiel in den Zuständen $|x_0\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ und $|x_1\rangle = \gamma_0 |0\rangle + \gamma_1 |1\rangle$ ist der Zustand des Quantenregisters

$$\begin{aligned} R = |x_0\rangle\, |x_1\rangle &= (\beta_0 |0\rangle + \beta_1 |1\rangle) \cdot (\gamma_0 |0\rangle + \gamma_1 |1\rangle) \\ &= \beta_0\gamma_0\, |0\rangle |0\rangle + \beta_0\gamma_1 |0\rangle |1\rangle + \beta_1\gamma_0 |1\rangle |0\rangle + \beta_1\gamma_1 |1\rangle |1\rangle \end{aligned} \tag{7}$$

Substituiert man $\beta_i\gamma_j = \alpha_{ij}$, ergibt sich der Zustand

$$R = \alpha_{00} |0\rangle |0\rangle + \alpha_{01} |0\rangle |1\rangle + \alpha_{10} |1\rangle |0\rangle + \alpha_{11} |1\rangle |1\rangle \tag{8}$$

Und kann als

$$R = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \tag{9}$$

Oder

$$R = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle \tag{10}$$

geschrieben werden.

Da aus $|\beta_0|^2+|\beta_1|^2 = 1$ und $|\gamma_0|^2+|\gamma_1|^2 = 1$ sich $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2 = 1$ ergibt, bildet α die Amplitude für den jeweiligen Zustand $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$.

Allgemeiner gefasst befindet sich ein Quantenregister R der Länge n im Zustand

$$R = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \tag{11}$$

für den die Bedingung

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1 \tag{12}$$

gilt. Dabei entspricht $i = 0, ..., 2^n - 1$ der Dezimaldarstellung der Bits im Quantenregister und $|\alpha_i|^2$ der Wahrscheinlichkeit, dass sich das Register nach einer Messung im jeweiligen Zustand $|i\rangle$ befindet.

Es ist möglich Transformationen nicht nur auf einzelnen Quantenbits durchzuführen, sondern auch auf ganze Register. Um eine Transformation auf einem Register durchzuführen, muss zuerst ein n-faches Tensorprodukt der Transformationsmatrix mit sich selbst berechnet werden. n ist dabei die Länge des Registers. Da ein Tensorprodukt nur zwischen Matrizen derselben Größe berechnet werden kann, ist es nur möglich Transformationen auf 2^n langen Registern durchzuführen.

Die Transformationen $A_1, \ldots, A_{2^n}$ auf die Qubits $|x_1\rangle, \ldots, |x_{2^n}\rangle$ mit jeweils A_i auf $|x_i\rangle$ entsprechen also der Transformation $A_1 \otimes, \ldots, \otimes A_{2^n}$ auf das Register $|x_1, \ldots, x_{2^n}\rangle$.
Möchte man die Hadamard-Transformation H auf ein Register $R = |00\rangle$ anwenden, müsste man zuerst die Hadamard-Transformation auf Registerebene

$$H \otimes H \;=\; H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{13}$$

bilden. Daraus ergibt sich

$$H_2 R \;= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \tag{14}$$

beziehungsweise

$$\frac{1}{2} \left(|00\rangle + |01\rangle + |10\rangle + |11\rangle \right) \tag{15}$$

oder

$$\frac{1}{2} \left(|0\rangle + |1\rangle + |2\rangle + |3\rangle \right). \tag{16}$$

Dabei bleibt die Bedingung

$$\sum_{i=0}^{2^n - 1} |\alpha_i|^2 = 1 \tag{17}$$

Mit n = 2 und $\alpha_i = \frac{1}{2} \forall i$ erfüllt. Die Wahrscheinlichkeit, dass jeder Basiszustand nach der Messung auftritt, ist gleichverteilt. Diese Berechnung kann genutzt werden, um echte Zufallszahlen zwischen 0 und 3 zu generieren. Formal beschrieben sieht der Algorithmus aus, wie folgt:

$$\begin{aligned} R &= |x_1 x_0\rangle \leftarrow |00\rangle \\ R &= H_2 R \\ &MissR \end{aligned}$$

Dieser Algorithmus kann auf eine beliebige Registergröße 2^n erweitert werden. Allerdings ist das Rechnen auf Registerebene bisher nur mathematisch sinnvoll.

Tatsächlich werden sämtliche Rechenschritte in lokalen unitären Transformationen durchgeführt. „Lokal“ heißt in diesem Fall, dass maximal drei Qubits an der Berechnung beteiligt sind, da es physikalisch einfacher ist Transformationen auf drei Qubits auszuführen als auf 2^n mit beliebig hohen n. Zudem sind mindestens drei Qubit notwendig, um klassische Rechenverfahren in Quantenalgorithmen zu überführen. Dies wird später aufgegriffen.

In den beiden Münzwurfbeispielen wurde die Hadamard-Transformation nur auf Quantenbits oder -register angewendet, bei denen sich alle Bits im Zustand $|0\rangle$ befunden haben. Ein n langes Quantenregister R, dessen Bits sich alle im Zustand $|0\rangle$ befunden haben und auf das die Hadamard-Transformation angewandt wurde, kann wie folgt dargestellt werden:

$$R = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |\, i\rangle \tag{18}$$

Diese Darstellung reicht allerdings nicht aus, um Quantenregister abzubilden, dessen Quantenbits sich vor der Hadamard-Transformation teilweise im Zustand $|1\rangle$ befunden haben. Wendet man die Hadamard-Transformation auf ein Register $|xy\rangle$ an, das sich im Zustand $|01\rangle$ befindet, sähe das Quantenregister vor dem Ausmultiplizieren wie folgt aus:

$$|\,01\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle\,) \cdot \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle\,). \tag{19}$$

Man kann an dieser Stelle die Information, ob sich die jeweiligen Quantenbits vorher im Zustand $|0\rangle$ oder $|1\rangle$ befunden haben, in das Vorzeichen ziehen:

$$|\,xy\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|\,0\rangle + (-1)^x\,|\,1\rangle\,) \cdot \frac{1}{\sqrt{2}}(|\,0\rangle + (-1)^y\,|\,1\rangle\,). \tag{20}$$

Ausmultipliziert ergibt dies:

$$\frac{1}{2}\left(|\,00\rangle + (-1)^x\,|\,01\rangle + (-1)^y\,|\,10\rangle + (-1)^{x\oplus y}\,|\,11\rangle\right). \tag{21}$$

Allgemeiner gefasst:

$$\frac{1}{2}\left((-1)^{(0,0)\oplus z}\,|\,00\rangle + (-1)^{(0,1)\oplus z}\,|\,01\rangle + (-1)^{(1,0)\oplus z}\,|\,10\rangle + (-1)^{(1,1)\oplus z}\,|\,11\rangle\,\right), \tag{22}$$

mit $z = (x, y)^T$.
Anhand der letzten Darstellung kann man ein Quantenregister der Länge n im Zustand $x \in \{0,1\}^n$, auf das die Hadamard-Transformation angewandt wurde, wie folgt darstellen:

$$H_n\,|\,x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in 0,1^n} (-1)^{x\cdot y}\,|\,y\rangle\,. \tag{23}$$

Dabei ist $x \cdot y$ das Skalarprodukt $\oplus_{i=1}^{n} x_i y_i$ der Vektoren $x, y \in \{0,1\}^n$.
Auch die Hadamard-Transformation ist reversibel. Nehmen wir das vorherige Beispiel:

$$|\,01\rangle \xrightarrow{H_2} \frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle\,) \cdot \frac{1}{\sqrt{2}}(|\,0\rangle - |\,1\rangle\,). \tag{24}$$

Wendet man die Hadamard-Transformation erneut an, ergibt sich:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \cdot \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
&\xrightarrow{H_2} \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) + \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right) \cdot \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) - \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|0\rangle + |0\rangle\right)\right) \cdot \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left(|1\rangle + |1\rangle\right)\right) \\
&= \frac{1}{2}\left(|0\rangle + |0\rangle\right) \cdot \frac{1}{2}\left(|1\rangle + |1\rangle\right) \; = \frac{1}{4}\left(|01\rangle + |01\rangle + |01\rangle + |01\rangle\right) = |01\rangle \; .
\end{aligned} \tag{25}$$

Die Reversibilität der Hadamard-Transformation ist für komplexere Algorithmen von Bedeutung. Bevor auf diese und deren Darstellung in Form von Quantenschaltkreisen eingegangen werden kann, muss noch der Vorgang des Messens genauer beschrieben werden.

1.4 Messen

Die Messung „Miss$|x\rangle$“ ist die einzige Transformation in der Quanteninformatik, die nicht reversibel, beziehungsweise unitär ist. Beim Messen verliert ein Quantenbit seine Superposition und fällt zufällig, je nach Wahrscheinlichkeitsverteilung, in einen der Basiszustände, in deren Kontext gemessen wurde. Aus diesen Zuständen ist nicht zu errechnen in welchem Zustand sich das Quantenbit vor der Messung befunden hat.
Bisher wurde davon ausgegangen, dass ein Quantenbit nur in die Zustände $|0\rangle$ oder $|1\rangle$ zerfallen kann. Dies geschieht allerdings nur dann, wenn $|0\rangle$ und $|1\rangle$ die Basis der Messung bilden. Genauer gesagt, wenn diese die Basis bilden, in deren Vektorraum der Zustand des Quantenbits abgebildet wird. In der Quanteninformatik müssen diese Basen die Eigenschaften der Orthonormalbasen erfüllen. Die Basis zur Abbildung eines Quantenbits $\{|0\rangle, |1\rangle\}$ erfüllt diese Voraussetzungen. Diese wird Standardbasis genannt. Die Basis zur Abbildung eines Registers mit zwei Quantenbits $\{|00\rangle, |01\rangle\, |10\rangle, |10\rangle\}$ erfüllt diese Bedingung ebenfalls. Diese wird schließlich aus dem einfachen Tensorprodukt der Standardbasis mit sich selbst gebildet. Misst man als Beispiel das Register mit zwei Quantenbits, zerfällt der Zustand des Registers in einen der zugehörigen Basiszustände und man erhält ein Messergebnis. Mathematisch ausgedrückt bestimmen beim Messen des 2 Bit-Quantenregisters “die Projektionen auf die eindimensionalen Unterräume

$$Span\{|00\rangle\}, Span\{|01\rangle\}, Span\{|10\rangle\} \text{ und } Span\{|11\rangle\}$$

das Ergebnis.” [2]
Diese oben genannte Folge von Unterräumen, die aus der disjunkten Zerlegung der Orthonormalbasis: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, entstehen, nennt man “Observable”. Diese Unterräume enthalten jeweils einen Basisvektor, der jeweils einen der Zustände bildet, der nach dem vollständigen Messen des Registers *beobachtet* werden kann.

Zwei zusätzliche Dinge sind beim Messen möglich. Man kann zum einen nur einzelne Bits messen, statt des gesamten Registers. Zum anderen kann man

[2] Homeister, 2022, S. 47.

zum Messen eine andere Basis verwenden, als zum Projektieren des Zustandes in einen Vektorraum verwendet wird.
Das Messen einzelner Bits in einem Register ist in manchen Algorithmen wichtig, um anhand eines Zwischenergebnisses zu bestimmen, welche Folgetransformationen durchgeführt werden müssen. Quantenteleportation ist ein Beispiel dafür. Auch dazu später mehr.

Misst man in einem Register mit zwei Bits im Zustand $|\phi\rangle$ beispielsweise nur das erste Bit, bestimmen die Projektionen

$$Span\{|00\rangle\ |01\rangle\} \text{ und } Span\{|10\rangle\ |11\rangle\}$$

das Ergebnis. In dem Fall geht das Register "mit der Wahrscheinlichkeit

$$|\alpha_{00}|^2 + |\alpha_{01}|^2$$

in den Zustand

$$|\phi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

über und mit Wahrscheinlichkeit

$$|\alpha_{10}|^2 + |\alpha_{11}|^2$$

in den Zustand

$$|\phi'\rangle = \frac{\alpha_{10}\,|00\rangle + \alpha_{11}\,|01\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}.$$

Wir erfahren bei der Messung nur den Wert des gemessenen Bits, nicht die Amplituden des Folgezustandes." [3]

Das Messen in einer anderen Basis, als der, die zur Projektion ein einen Vektorraum genutzt wird, kann genutzt werden, um die Superposition des Quantenbits nach der Messung nicht vollständig zu zerstören. Misst man ein Quantenbit in der Basis $\{|+\rangle, |-\rangle\}$ mit $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ erhält man als Ergebnis entweder den Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ oder $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Dies ist immer noch eine Superposition. Daher kann nach der Messung mit dem Quantenbit noch weiter gerechnet werden. Allerdings ist es auch hierbei nicht möglich den Zustand zu ermitteln, in dem sich das Bit vor der Messung befunden hat. Die Messung bleibt irreversibel. Die Basis $\{|+\rangle, |-\rangle\}$ wird "Hadamard-Basis" genannt.

[3] Homeister, 2022, S. 47.

Zur Veranschaulichung kann die folgende Abbildung dienen[4]:

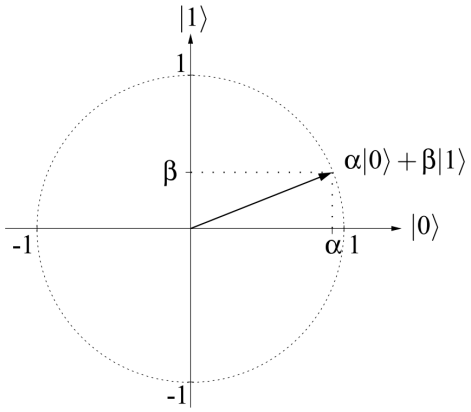

Abbildung 2: Zustandsvektor in der Standardbasis

Es wird ein Zustandsvektor in der Standardbasis dargestellt. Die Länge der Projektionen des Zustandsvektors auf den beiden Achsen bestimmen die Wahrscheinlichkeit, mit der, nach der Messung, einer der Zustände eingenommen wird. Mit der Wahrscheinlichkeit $|\alpha|^2$ wird der Zustand nach der Messung $|0\rangle$ sein und mit der Wahrscheinlichkeit $|\beta|^2$ $|1\rangle$.
In der folgenden Abbildung wird derselbe Zustandsvektor gezeigt, mit dem Unterschied, dass die Koordinatenachsen nach der Hadamard-Basis ausgerichtet sind[5].

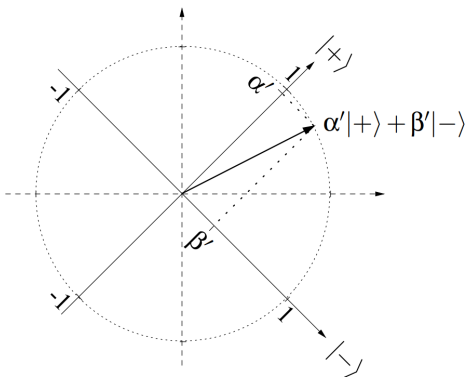

Abbildung 3: Zustandsvektor in der Hadamard-Basis

Die Projektionen der Achsen haben sich im Vergleich zur Projektion auf die Standardbasis verändert. Mit der Wahrscheinlichkeit $|\alpha'|^2$ wird nach dem Messen der Zustand $|+\rangle$ angenommen und mit der Wahrscheinlichkeit $|\beta'|^2$ $|-\rangle$.
Mathematisch sieht diese "Basistransformation" aus wie folgt:

$$\alpha\,|0\rangle + \beta\,|1\rangle = \alpha' \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) + \beta' \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right). \tag{26}$$

[4]Homeister, 2022, S. 44.
[5]Homeister, 2022, S. 45.

Allgemeiner lässt sich zusammenfassen: "Register R bestehe aus n Quantenbits und befinde sich im Zustand

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

Wir messen bezüglich der Basis $|0'\rangle, |1'\rangle, ..., |(2^n-1)'\rangle$ aus zueinander orthogonalen Vektoren der Länge 1." [6] Dies ist eine andere Basis, als die in der sich $|\phi\rangle$ befindet. "Dabei wird die Superposition von $|\phi\rangle$ zerstört. Hat $|\phi\rangle$ bezüglich der Messbasis die Darstellung

$$\sum_{i=0}^{2^n-1} \alpha_i' |i\rangle ,$$

so finden wir das Register nach der Messung mit Wahrscheinlichkeit $|\alpha_i'|^2$ im Zustand $|i'\rangle$ vor. Sämtliche anderen Informationen gehen dabei verloren." [7]

Das Messen einzelner Bits oder ganzer Register, sowie das Messen von Teilen eines Registers in der Standardbasis oder auch in einer anderen umfasst alles, was beim Messen möglich ist.

[6] Homeister, 2022, S. 46.
[7] Homeister, 2022, S. 46.

2 Einführung in die Quanteninformatik 2

2.1 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, sodass die ursprüngliche Superposition zerstört wird.

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

2.2 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 faszinierender 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 $|b_1 b_2\rangle$ im Zustand $|00\rangle$. Wir wenden auf das erste Bit die Hadamard-Transformation an und anschließend auf beide Bits die Operation CNOT.

$$CNOT : |x, y\rangle \to |x, y \oplus x\rangle \tag{27}$$

Das ergibt:

$$|00\rangle \xrightarrow{H\otimes I_2} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \tag{28}$$

$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{29}$$

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.[8]

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:

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

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

Abbildung 4: Definition Verschränkung

[8] Homeister, 2022, S. 76.

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:

$$|\phi\rangle = 0.9\,|00\rangle + 0.1\,|11\rangle \tag{30}$$

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.

2.3 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.“[9]

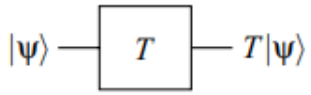

Abbildung 5: Quantenschaltkreis

Wenn wir eine Berechnung mit mehreren Qubits ausführen, ergibt sich der Endzustand $|x, y, z\rangle$ aus dem Tensorprodukt der einzelnen Gatter[10]:

$$(I_2 \otimes W \otimes I_2)(U \otimes V)\,|x, y, z\rangle \tag{31}$$

[9] Homeister, 2022, S. 76.
[10] Homeister, 2022, S. 76.

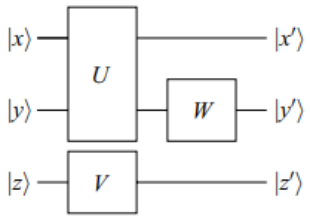

Abbildung 6: Quantenschaltkreis mit Tensorprodukt

Da bei Quantenschaltkreisen die Umkehrbarkeit der Berechnungen garantiert werden muss, ist die Summe der Eingabe-Qubits = Summe der Ausgabe-Qubits und pro Gatter dürfen höchsten 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:

$$CNOT : |x, y\rangle \rightarrow |x, y \oplus x\rangle \tag{32}$$

oder als Matrix:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{33}$$

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:[11]

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{34}$$

[11] Homeister, 2022, S. 79.

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

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{35}$$

und der „Y-Flip“ Y:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{36}$$

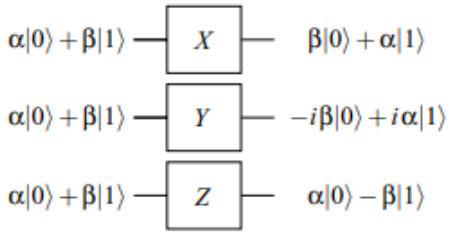

Abbildung 7: Pauli-Matrizen

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.

2.4 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 AND 0 = 0, jedoch ebenfalls aus 0 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 $c \oplus (a \wedge b)$:[12]

[12] Homeister, 2022, S. 87.

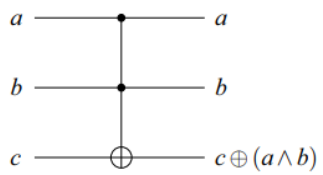

Abbildung 8: Toffoli-Gatter

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.

2.5 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 wir 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.

2.6 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“.

2.6.1 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 fakultative ($O(n!)$) 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 Quantenalgorithmen, 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.[13]
Hier stoßen Quantencomputer also auf dieselben grundlegenden Herausforderungen wie klassische Computer.

[13] Homeister, 2022, S. 165.

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.

2.6.2 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.[14]

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.

2.7 Zukunft

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

[14] Vgl. Technische Universität Wien. *Grenzen für Quantencomputer: Perfekte Uhren sind unmöglich.* tuwien.at., (abgerufen am 02. März 2025)

2.7.1 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."[15] 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.[16] 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.[17]

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.

2.7.2 Simulationen

Die Simulation von chemischen Molekülen. Etwas bei dem selbst Supercomputer an ihre Grenzen stoßen. Erstaunlicherweise ist die detaillierte Simulation von etwas so Kleinem wie Molekülen eine der größten Herausforderungen für unsere modernen Computer. Hier könnten Quantencomputer Unterstützung leisten. So schreibt das Fraunhofer Cluster of Excellence Cognitive Internet Technologies: " Mithilfe der Simulation von Molekülen könnten in Zukunft beispielsweise gezielt Katalysatoren entwickelt werden, die chemische Produktionsverfahren effizienter machen. Chancen ähnlicher Größenordnung ergeben sich für die Pharmaindustrie. Auch Forschung zu den im Angesicht des Klimawandels besondere relevanten Batterien zählt zum Anwendungsbereich der Simulation."[18] Deshalb erforscht das deutsche Zentrum für Luft- und Raumfahrt (DLR) zusammen mit

[15] Vgl. Technische Universität Wien. *Grenzen für Quantencomputer: Perfekte Uhren sind unmöglich.* tuwien.at., (abgerufen am 02. März 2025)

[16] Vgl. Bauckhage, Christian, et al. *Quantum Machine Learning in the Context of IT Security.* bsi.bund.de., (abgerufen am 02. März 2025)

[17] Vgl. Bundesamt für Sicherheit in der Informationstechnik. *Quantenmechanische Sicherheitslücken (QML) - Studien.* bsi.bund.de., (abgerufen am 02. März 2025)

[18] Vgl. Fraunhofer Cluster of Excellence Cognitive Internet Technologies. *Quantencomputing – Forschungsthemen.* cit.fraunhofer.de., (abgerufen am 02. März 2025)

dem Fraunhofer-Institut für Werkstoffmechanik IWM unter Verwendung des IBM-Quantencomputers neue Wege des Materialdesigns.[19]

Neben den genannten Anwendungsgebiete wird außerdem ein Nutzer in der Logistik (optimaler Verteilung begrenzter Ressourcen), den Ingenieurswissenschaften und dem Finanzwesen (Risikoanalysen und Optimierung von Portfolios) gesehen.[20]

[19] Vgl. Fraunhofer-Institut für Werkstoffmechanik IWM. *Quantencomputer für innovative Materialsimulation nutzen.* iwm.fraunhofer.de., (abgerufen am 02. März 2025)

[20] Vgl. Fraunhofer Cluster of Excellence Cognitive Internet Technologies. *Quantencomputing – Forschungsthemen.* cit.fraunhofer.de., (abgerufen am 02. März 2025)

3 No Cloning Theorem

Einer der faszinierendsten Aspekte der Quantenmechanik ist, dass es unmöglich ist einen beliebigen unbekannten Quantenzustand perfekt zu duplizieren. Dieses Konzept ist mit dem No-Cloning-Theorem beschrieben, einem grundlegenden Ergebnis der Quanteninformationstheorie. Das Theorem hat nicht nur tiefgreifende Auswirkungen auf die Quanteninformatik und die Quantenkommunikation, sondern auch für unser Verständnis der Natur der Information in Quantensystemen.

In der klassischen Physik ist die Vervielfältigung von Informationen einfach: Ein Kopiergerät kann ein Dokument vervielfältigen, ohne das Original zu verändern. In der Quantenmechanik wird dieser einfache Vorgang jedoch zu einer nicht trivialen und verbotenen Operation. Das No-Cloning-Theorem besagt, dass es keine universelle Quantenoperation gibt die eine identische Kopie eines beliebigen unbekannten Quantenzustands erzeugen kann.

In diesem Abschnitt werden wir das No-Cloning-Theorem aus verschiedenen Blickwinkeln betrachten, seinen Beweis diskutieren, seine Konsequenzen untersuchen und verstehen, wie es die Landschaft der Quantentechnologien prägt.

3.1 Definition

Das No-Cloning-Theorem besagt, dass es unmöglich ist, eine identische Kopie eines unbekannten Quantenzustands zu erzeugen. Mathematisch gesehen gibt es keinen unitären Operator U, der die folgende Bedingung erfüllt:

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{37}$$

wobei $|\psi\rangle$ ein beliebiger Quantenzustand und $|e\rangle$ in Hilfszustand ist, der überschrieben werden soll. Diese Gleichung drückt die Idee aus, dass, wenn wir den Operator U auf den Zustand $|\psi\rangle$ anwenden (kombiniert mit einem Hilfszustand), zwei Kopien des ursprünglichen Zustands entstehen sollten. Das Theorem sagt uns, dass es für beliebige $|\psi\rangle$ keinen solchen Operator geben kann, weil sich die Quanteninformation grundlegend von der klassischen Information unterscheidet.

3.2 Beweis

Als grundlegende Schlussfolgerung der Quantenmechanik gibt es mehrere Beweise für dieses Theorem. Ein solcher Beweis, ein Widerspruchsbeweis, der der Einfachheit halber gewählt wurde, kann wie folgt definiert werden.
Zuerst nehmen wir zwei beliebige Quantenzustände, $|\psi_1\rangle$ und $|\psi_2\rangle$. Dann werden diese beiden Zustände mit dem Klon operator U geklont, den wir im vorigen Abschnitt definiert haben und von dem wir für unseren Widerspruchsbeweis nun annehmen, dass er existiert.

$$\begin{aligned} U(|\psi_1\rangle \otimes |e\rangle) &= |\psi_1\rangle \otimes |\psi_1\rangle \\ U(|\psi_2\rangle \otimes |e\rangle) &= |\psi_2\rangle \otimes |\psi_2\rangle \end{aligned} \tag{38}$$

Mit dieser Information haben wir jetzt zwei Möglichkeiten, das Skalarprodukt von $\langle U(\psi_1 \otimes e)\rangle\, U(\psi_2 \otimes e)$ zu schreiben. Die eine verwendet das Ergebnis der

vorherigen Gleichung, während die andere die Tatsache nutzt, dass Quantenoperationen das Skalarprodukt ihrer Eingaben bewahren[21].

$$\begin{aligned} \langle U(\psi_1 \otimes e)\rangle\, U(\psi_2 \otimes e) &= \langle \psi_1 \otimes \psi_1\rangle\, \psi_2 \otimes \psi_2 \\ \langle U(\psi_1 \otimes e)\rangle\, U(\psi_2 \otimes e) &= \langle \psi_1 \otimes e\rangle\, \psi_2 \otimes e \end{aligned} \tag{39}$$

Einfache Ersetzung führt dann zur folgenden Gleichung

$$\langle \psi_1 \otimes \psi_1\rangle\, \psi_2 \otimes \psi_2 = \langle \psi_1 \otimes e\rangle\, \psi_2 \otimes e \tag{40}$$

Da Tensor und Skalarprodukte kompatible sind[22] simplifiziert das weiter zu:

$$\langle \psi_1\rangle\, \psi_2\, \langle \psi_1\rangle\, \psi_2 = \langle \psi_1\rangle\, \psi_2\, \langle e\rangle\, e \tag{41}$$

Und schließlich, weil für jeden Zustand $|e\rangle$ die Gleichung $\langle e\rangle\, e = 1$ gilt, kommen wir zu dieser Gleichung:

$$\langle \psi_1\rangle\, {\psi_2}^2 = \langle \psi_1\rangle\, \psi_2 \tag{42}$$

Es sollte nun offensichtlich sein, dass diese Gleichung nur zwei Lösungen hat: $\langle \psi_1\rangle\, \psi_2 = 1$ or $\langle \psi_1\rangle\, \psi_2 = 0$. Die erste Lösung impliziert, dass $\psi_1 = \psi_2$, was für eine allgemeine Klon-Operation nicht hilfreich ist, erlaubt aber eine Operation, die Kopien eines bestimmten Zustands erzeugt. Das ist vor allem nützlich um Quantensysteme in einen bekannten Zustand zu initialisieren. Die zweite Lösung erlaubt zwar, dass sich ψ_1 und ψ_2 unterscheiden, und ist damit auf den ersten Blick vielversprechend, verlangt aber immer noch, dass die beiden Zustände orthogonal zueinander sind. Das ist zwar weniger restriktiv als die erste Lösung erlaubt aber immer noch nur eine Operation die eine bestimmte Klasse von Zuständen kopieren kann von der alle Mitglieder zueinander orthogonal sind. Somit ist auch mit dieser Lösung keine allgemeine Klon-Operation möglich.

3.3 Folgen

Das No-Cloning-Theorem hat weitreichende Auswirkungen auf eine Reihe von Gebieten der Quantenmechanik und Quanteninformatik.

3.3.1 Quantenkommunikation

In der klassischen Informationstheorie ist das Kopieren von Daten eine zentrale Technik, um Information zu vervielfältigen und zu übertragen. Bei klassischen Bits kann man exakt den gleichen Wert duplizieren, indem man eine Kopie eines Bits erstellt. Im Gegensatz dazu verhindert das No-Cloning-Theorem das Erstellen von exakten Kopien von Quantenbits (Qubits).

Das bedeutet, dass im Bereich der Quantenkommunikation, insbesondere bei der Quantenkryptographie, ein Angreifer, der versucht die Quanteninformation abzufangen oder zu kopieren, in der Regel Fehler einführen wird, die entdeckt werden können. Dieses Prinzip bildet die Grundlage für Sicherheitsprotokolle wie Quantum Key Distribution (QKD), bei denen ein Abhörversuch die Übertragung zerstören würde und somit leicht zu erkennen ist.

[21] Vgl: Postulates for general quantum mechanics, Segal, Irving E, 1947, S. 930–948.
[22] Siehe Fußnote 8

3.3.2 Schutz der Quanteninformation

Da das No-Cloning-Theorem das exakte Kopieren eines unbekannten Zustands verbietet, wird auch die Quanteninformation von Natur aus gegen bestimmte Arten von Angriffen geschützt. In klassischen Computersystemen kann ein Angreifer beliebig viele Kopien von Information erstellen, um sie zu analysieren und gegebenenfalls zu entschlüsseln. In einem quantenmechanischen System jedoch kann ein Datenexfiltrationsversuch oder das Kopieren eines Zustands nicht ohne weiteres erfolgen, ohne dass der Versuch des Kopierens den Zustand verändert und die Quanteninformation damit entwertet wird.

Ein gutes Beispiel für diese Art von Sicherheit ist das BB84-Protokoll für Quantenkryptographie. Bei der Quantenverschlüsselung wird eine Nachricht durch verschränkte Quantenbits übertragen. Jeder Versuch, die Nachricht zu kopieren oder abzufangen, verändert den Zustand der Qubits und wird vom Empfänger erkannt.

3.3.3 Design von Algorithmen

Das No-Cloning-Theorem hat auch tiefgehende Auswirkungen auf das Quantencomputing. In klassischen Computern ist das Kopieren von Informationen eine grundlegende Technik, die in vielen Algorithmen und Protokollen verwendet wird. Quantencomputer hingegen können keine exakten Kopien eines Zustands herstellen, was bedeutet, dass traditionelle Techniken wie fehlerkorrigierende Codes, die in klassischen Computern üblich sind, in der Quantenwelt nicht direkt anwendbar sind.

Allerdings existieren spezielle Quantenfehlerkorrekturcodes, die darauf ausgelegt sind, Fehler zu korrigieren, die durch das Fehlen einer exakten Kopierbarkeit von Quanteninformation entstehen. Diese Codes erfordern jedoch eine zusätzliche Anzahl von Qubits und eine komplexe Fehlerkorrekturstrategie, was das Quantencomputing technisch anspruchsvoll macht. Trotzdem sind Quantenfehlerkorrekturmethoden von entscheidender Bedeutung für die zukünftige Skalierbarkeit und Zuverlässigkeit von Quantencomputern und werden später in diesem Artikel genauer beschrieben[5.3].

Kommentar

Verschiedene Messmethoden Jeder Quantenalgorithmus ist auch grundsätzlich anders als ein klassischer Algorithmus, da Operationen anders implementiert werden müssen, auch wenn die Theorie des Algorithmus identisch zu einem klassischen Algorithmus ist. Dieser Aspekt wird hier allerdings nicht näher behandelt werden.

3.3.4 Speicherung von Quanteninformation

Das No-Cloning-Theorem hat weitreichende Konsequenzen für die Quanteninformationstheorie, insbesondere für die Konzepte der Informationsspeicherung und -übertragung. Die Unmöglichkeit des Klonens ist eng mit den grundlegenden Prinzipien der Quantenmechanik wie Überlagerung und Verschränkung

verknüpft. Sie hindert die Schaffung von perfekten Kopien von Quanteninformation und erfordert, dass Information auf neue, kreative Weise verarbeitet und gespeichert wird.

Ein interessantes Beispiel sind die Quantenlogikgatter, die in Quantencomputern verwendet werden. Diese Gatter müssen mit den Einschränkungen des No-Cloning-Theorems arbeiten und können keine klassischen, deterministischen Kopien erzeugen, sondern müssen die Quanteninformation in verschränkten oder überlagerten Zuständen manipulieren.

3.3.5 Messungen und Messgenauigkeit

In der Quantenmetrologie, die sich mit der präzisen Messung von quantenmechanischen Systemen beschäftigt, beeinflusst das No-Cloning-Theorem ebenfalls die Art und Weise, wie Messungen durchgeführt werden können. Da das exakte Kopieren von Zuständen nicht möglich ist, kann das Präzisionsmaß für Messungen nicht durch das Vervielfachen von Messinstrumenten oder durch das Erstellen von Kopien von Quantenobjekten verbessert werden. Stattdessen wird die Quantenmessung durch andere Techniken wie Quanteninterferometrie und den Einsatz von verschränkten Zuständen optimiert.

4 Quantenteleportation

4.1 Einführung

Quantenteleportation ist ein bahnbrechendes Phänomen, das die Übertragung von Quanteninformationen zwischen zwei entfernten Orten ermöglicht, ohne dass das Teilchen oder Objekt, das die Information trägt, physisch bewegt wird. Im Gegensatz zur theoretischen klassischen Teleportation, bei der es um den Transport von Materie oder Energie geht, konzentriert sich die Quantenteleportation auf die Übertragung von Quantenzuständen. Dieser Prozess nutzt die Prinzipien der Quantenmechanik, einschließlich Verschränkung, Superposition, und das No-Cloning-Theorem, um den Zustand eines Quantenobjekts (z.B. eines Photons oder eines Elektrons) von einem Ort zum anderen zu übertragen. Dabei spielt die Entfernung der Objekte keine Rolle.

Der Begriff "Quantenteleportation" kann etwas irreführend sein, da bei diesem Prozess keine eigentliche Materie teleportiert wird. Was stattdessen "teleportiert" wird, ist die Information über den Quantenzustand eines Teilchens. Der Schlüssel zur Quantenteleportation ist die Quantenverschränkung, ein Phänomen, bei dem zwei oder mehr Teilchen so miteinander korrelieren, dass der Zustand des einen Teilchens den Zustand des anderen augenblicklich beeinflusst, unabhängig davon, wie weit sie voneinander entfernt sind. Diese "gespenstische Fernwirkung", wie Albert Einstein sie nannte, ermöglicht die Übertragung von Quanteninformation zwischen weit entfernten Parteien, ohne dass die oft fragilen Quantenzustände selbst transportiert werden müssen.

4.2 Aufbau

Es muss ein Quanten-Verschränkungspaar vorhanden sein. Dieses Paar muss sich im Bell-Zustand[23] befinden, um sicherzustellen, dass die Messung des einen den Zustand des anderen beeinflusst. Dieses Paar wird in der Regel durch einen Prozess wie Spontane parametrische Abwärtsumwandlung[24] erzeugt. Derzeit werden dafür in der Regel einfache Photonen oder Ionen verwendet.

Außerdem müssen sich an den Endpunkten der Teleportation zwei Parteien befinden, im Folgenden Alice und Bob genannt, die beide in der Lage sind, mit Quantensystemen zu interagieren und Messungen vorzunehmen, was normalerweise einen Quantencomputer mit begrenzter Funktionalität bedeutet. Schließlich muss ein klassischer Kommunikationskanal zwischen Alice und Bob bestehen. Der Schlüssel für die Quantenteleportation ist hier, dass dieser Kanal nicht in der Lage sein muss, Quantenzustände zu transportieren - dafür ist die Teleportation gedacht -, sondern nur herkömmliche Bits.

4.3 Vorgang

Nachdem der Aufbau abgeschlossen ist, stellt sich nun die Frage, was tatsächlich getan werden muss, um die Quantenteleportation durchzuführen. Dies kann in

[23] Vgl: Quantum computation and quantum information, Nielsen, Michael A.; Chuang, Isaac L., 2010

[24] Vgl: Spontaneous parametric down-conversion, Couteau, Christophe, 2018, S.291–304

mehrere Schritte aufgeteilt werden.

4.3.1 Alices Bell Zustand Messung

Der erste Schritt, den Alice durchführt, ist die Bell-State-Messung, die zwei wichtige Teilschritte umfasst.
Zunächst kombiniert Alice das Teilchen, das sie teleportieren möchte, mit ihrer Hälfte des verschränkten Paares. Dies geschieht in der Regel mithilfe eines Strahlenteilers oder eines Interferometers, um die beiden Teilchen in einen Superpositionszustand zu versetzen.
Zweitens misst Alice die beiden kombinierten Teilchen in der Bell-Basis, die die Teilchen aus ihren vier möglichen Zuständen in einen einzigen zusammenfallen lässt. Diese Messung ist entscheidend, denn sie bestimmt, wie Bob sein Teilchen anpassen muss, um den Zustand wiederherzustellen, den Alice teleportiert.

4.3.2 Klassische Kommunikation

Als Nächstes verwendet Alice ihren klassischen Kommunikationskanal, um ihre Messung an Bob zu senden. Dies erfordert die Übertragung von nur zwei Bits (den beobachteten Zustand des zu teleportierenden Qubits und den beobachteten Zustand des des verschränkten Paares), was für keinen Kommunikationskanal ein Problem darstellen sollte. Diese geringe Bandbreitenanforderung in der klassischen Kommunikation macht in der Tat mehrere Kommunikationskanäle verfügbar die normalerweise wegen ihrer geringen Bandbreite nicht infrage kämen, insbesondere wenn die Teleportation über große Entfernungen stattfinden soll. Diese Information reicht jedoch aus, um Bob zu instruieren, wie er sein eigenes System einstellen muss.

4.3.3 Bobs Quantenoperation

Nun, da Bob die klassische Messung erhalten hat, muss er eine oder beide (je nach Messung) der folgenden Methoden anwenden: Das Pauli-X-Gatter für einen Bit-Flip oder das Pauli-Z-Gatter für einen Phasen-Flip. Durch diese Operation wird sein Quantenzustand in denselben Zustand versetzt, den Alices Quantenteilchen hatten, bevor ihre Messung die Superposition kollabierte. Hier ist auch noch einmal darauf hinzuweisen, dass Bob den Zustand erst erstellt, nachdem Alice ihn mit der Messung bereits zerstört hat - wie das No-Cloning-Theorem besagt3 wird der Zustand nie kopiert, sondern nur übertragen.
Sobald Bob dies getan hat, ist die Quantenteleportation abgeschlossen.

4.4 Mathematik

4.4.1 Verschränkung und Bell-Zustände

Zu Beginn des Prozesses haben wir zwei Teilchen (Teilchen 2 und 3), die sich an den Orten A und B befinden. Diese Teilchen werden in einem verschränkten Zustand (Bell-Zustand) erzeugt. Ein Bell-Zustand ist eine der vier möglichen maximal verschränkten Zustände, die ein Paar von Quantenobjekten haben kann. Ein Beispiel für einen solchen Zustand ist:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \tag{43}$$

Dieser Zustand wird zwischen den beiden Teilchen 2 und 3 geteilt, wobei Teilchen 2 bei A und Teilchen 3 bei B ist.

4.4.2 Der zu teleportierende Zustand

Nun nehmen wir an, dass wir den Zustand eines dritten Teilchens (Teilchen 1) teleportieren möchten, das sich am Ort A befindet. Der Zustand des Teilchens 1 kann allgemein als:

$$|\psi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$$

ausgedrückt werden, wobei α und β komplexe Zahlen sind, die den Zustand beschreiben.

4.4.3 Verschränkung und Messung

Der gesamte Zustand des Systems (Teilchen 1, 2 und 3) kann als Produktzustand von Teilchen 1 und dem verschränkten Zustand von Teilchen 2 und 3 beschrieben werden:

$$|\Psi\rangle_{123} = |\psi\rangle_1 \otimes |\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}} (\alpha|0\rangle_1 + \beta|1\rangle_1) \otimes (|00\rangle_{23} + |11\rangle_{23})$$

Durch Anwenden der Distributivität ergibt sich:

$$|\Psi\rangle_{123} = \frac{1}{\sqrt{2}} (\alpha|0\rangle_1 \otimes (|00\rangle_{23} + |11\rangle_{23}) + \beta|1\rangle_1 \otimes (|00\rangle_{23} + |11\rangle_{23}))$$

$$|\Psi\rangle_{123} = \frac{1}{\sqrt{2}} (\alpha|000\rangle_{123} + \alpha|011\rangle_{123} + \beta|100\rangle_{123} + \beta|111\rangle_{123})$$

Nun wird eine Bell-Zustandsmessung auf den Teilchen 1 und 2 durchgeführt, die den Zustand des Systems in einen der vier Bell-Zustände projiziert. Die Messung ist zufällig, und die Ergebnisse können durch die folgenden Zustände beschrieben werden:

$$|\Phi^+\rangle_{12}, |\Phi^-\rangle_{12}, |\Psi^+\rangle_{12}, |\Psi^-\rangle_{12}$$

Klassische Kommunikation und Zustandserstellung

Nachdem die Messung durchgeführt wurde, sendet der Ort A das Messresultat an Ort B über einen klassischen Kanal. Anhand der Nachricht kann Ort B den Zustand des Teilchens 3 (das ursprünglich am Ort B war) in den gewünschten Zustand $|\psi\rangle_1$ transformieren. Dazu wird eine der folgenden Operationen durchgeführt, abhängig von der Messung, die an Ort A durchgeführt wurde:

$$
\begin{aligned}
|0\rangle_3 \quad & \text{(falls Messung das Ergebnis } |\Phi^+\rangle \text{ ergibt)} \\
X|0\rangle_3 \quad & \text{(falls Messung das Ergebnis } |\Phi^-\rangle \text{ ergibt)} \\
Z|0\rangle_3 \quad & \text{(falls Messung das Ergebnis } |\Psi^+\rangle \text{ ergibt)} \\
XZ|0\rangle_3 \quad & \text{(falls Messung das Ergebnis } |\Psi^-\rangle \text{ ergibt)}
\end{aligned}
$$

Durch diese Operationen wird der Zustand des Teilchens 3 in den ursprünglichen Zustand von Teilchen 1 ($\alpha|0\rangle + \beta|1\rangle$) überführt.

4.5 Herausforderungen

Obwohl die Quantenteleportation ein vielversprechender Forschungszweig ist, gibt es noch einige Herausforderungen zu bewältigen

4.5.1 Verschränkung Erzeugen und Erhalten

Eine der größten Herausforderung ist die Erzeugung und Erhaltung eines verschränkten Systems zwischen dem Start- und Zielpunkt der Teleportation. Die Teleportation ist zwar theoretisch nicht durch Entfernung begrenzt, aber je größer die Entfernung zwischen den Orten des do schwieriger ist es die verschränkten Teilchen aufzuteilen, ohne die Verschränkung zu beschädigen.

Ein Lösungsansatz sind hier Quantenrepeater: Spezialisierte Geräte die die Entfernung zwischen direkt verschränkten Teilchen reduzieren, indem sie diese nur zwischen Repeater Stationen aufteilen müssen. In der Station werden dann mithilfe von Entanglement Swapping zwei Verbindungen des Repeaters verschränkt.

4.5.2 Klassische Kommunikation

Auch wenn die benötigte Bandbreite der klassischen Kommunikation minimal ist, muss trotzdem ein Kommunikationskanal existieren. Das hat zwei signifikante Nachteile: Zum einen ist die klassische Kommunikation auf die Lichtgeschwindigkeit begrenzt, was ein Geschwindigkeitslimit für die Teleportation erzeugt, auch wenn die "spukhafte Fernwirkung" der Quantenmechanik schneller passieren könnte[25]. Zum anderen sind klassische Kommunikationskanäle anfällig für Observation - ein Angreifer kann zwar ohne das verschränkte Teilchen den Quantenzustand nicht reproduzieren ist aber in der Lage festzustellen, dass die Kommunikation stattgefunden hat. Ebenfalls könnte der Angreifer auch die Kommunikation stören, was zwar bei geeigneten Protokollen den Teilnehmern offensichtlich ist aber trotzdem eine Schwachstelle darstellt. Die einzige bekannte Lösung ist hier ein robustes klassisches Kommunikationssystem, was für andere Kommunikationszwecke bereits aufgebaut ist oder wird, aber leider die Lichtgeschwindigkeitslimitation nicht umgehen kann.

[25]Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Hensen et. al., 2015, S. 682–686

4.5.3 Skalierbarkeit

Ein weiteres bedeutendes Problem der Quantenteleportation ist die Skalierbarkeit. Während die Quantenteleportation in kleinen, kontrollierten Systemen von einigen wenigen Qubits relativ einfach durchgeführt werden kann, stellt die Skalierung auf größere Netzwerke und damit nützliche Datenmengen und die Integration in reale Kommunikationssysteme eine enorme Herausforderung dar. Um Quantenteleportation praktisch nutzen zu können würde es ein großflächiges System von Kommunikationskomponenten benötigen. Die Erstellung dieser bräuchte Quantentechnologien in einer Menge in der diese momentan weder technisch möglich noch finanziell tragbar ist, wenn man bestehende Preise hochrechnet.

Hier ist allerdings die Erwartung, dass weitere Forschung dieses Problem beheben wird. Es wird sowohl an günstigeren Methoden zur Erstellung von verschränkten Systemen und der Stabilisierung dieser, als auch an der Erstellung von Quantenkomponenten rege geforscht. Auch an Forschungsbudget fehlt es hier nicht, da einige große Technologiefirmen wie Google und Microsoft an Quantentechnologie forschen.

4.5.4 Fehlerquellen und Messgenauigkeit

Die Messgenauigkeit ist entscheidend für die erfolgreiche Durchführung der Quantenteleportation. Eine fehlerhafte Messung der Bell-Zustände kann dazu führen, dass der teleportierte Zustand nicht korrekt wiederhergestellt werden kann. Fehlerquellen können in den Messinstrumenten, in der Kommunikation oder auch in der Quantenverschränkung selbst liegen.
Auch hier wird rege geforscht, da alle drei Aspekte nicht eigen zur Quantenteleportation sind, sondern nahezu alle Quantenoperationen betreffen.

5 Quantenhardware

Die Realisierung eines Quantencomputers ist durch hohe technische herausforderungen geprägt. Um die besonderen Eigenschaften der Qubits eines Quantencomputers, wie Superposition und Verschränkung, nutzen zu können, müssen sie durch externe Einflüsse geschützt werden und die Dekoheränz minimiert werden. Äußere Einflüsse wie Temperaturschwankungen, elektromagnetische Felder oder Strahlung aller Art können die Qubits beeinflussen. Aus diesem Grund werden Quantencomputer bei extrem niedrigen Temperaturen und in einem Vakuum betrieben.

Außerdem ist nicht nur die Herstellung der Qubits eine Herausforderung, sondern auch die Steuerung, Auslesung und Korrektheit von physikalischen Qubits.

5.1 Dekohärenz

Dekoheränz ist ein zentrales Konzept, welches wichtig in der Entwicklung von Quantencomputern ist. Der Prozess der Dekoheränz beschreibt den Verlust der koheränten Quanteneigentschaften eines Qubits durch Wechselwirkung mit der Umgebung. Diese Veränderung führt zu einem Übergang von quantenmechanischem Verhalten zu einem klassischem Verhalten von Bits.

In der Quantenmechanik können Systeme in Überlagerungszuständen existieren, wobei mehrere Zustände gleichzeitig eingenommen werden können. Diese Eigenschaft erklärt auch das Phänomen der Quanteninterferenz. Äußere Einflüsse durch die Umgebung kann eine Verschränkung von Qubits zerstören. Dies führt dazu, dass die Phasenbeziehungen zwischen den Qubits beeinflusst oder gar aufgehoben werden. Folgernd verliert das System die Interferenzeffekte und verhält sich zunehmend klassischer. Diese Zeit nennt man Dekoheränzzeit.

Die **Dekoheränzzeit** (T_2) eines Qubits misst die Länge der Zeit, in der er in der Lage bleibt kohärent zu bleiben, welcher danach von äußeren Einflüssen zerstört wird. Neben T_2 wird auch häufig die **Relaxationszeit** (T_1) gemessen, welche angibt, wie lange ein Qbit im angeregten Zustand bleibt, bevor es auf sein Grundzustand zurückfällt. In der Realität ist die Dekoheränzzeit jedoch in den meisten Fällen kürzer als die Relaxationszeit.

Berechnung der Dekoheränzzeit
Durch eine Messung der zeitlichen Abnahme der Koheränz eines beispielhaften Qubits kann die Dekoheränzzeit eines Systems festgelegt werden. Bei einem Quantencomputer, der auf dem Spin eines Teilchen beruht, kann dies durch die **Spin-Echo-Methode** gemessen werden. Quantencomputer, die auf anderen Qubits basieren, haben equivalente Methoden um die Kohärenz zu messen.

Das einfachste Modell zur Beschreibung der Dekoheränzzeit ist die **Exponentielle Abnahme der Kohärenz**

$$C(t) = C(0) * e^{-t/T_2} \tag{44}$$

Dabei ist:
$C(t)$ Die Kohärenz des Qubits zum Zeitpunkt t

$C(0)$ Die initiale Koheränz
T_2 Die Dekoheränzzeit

Indem man den Kohärenzverlust experimentell misst und die Werte in eine exponentielle Abklingfunktion einpasst, erhält man T_2

Kommentar

Die **Dekoheränzzeit** kann auch durch genauere jedoch auch deutlich kompliziertere weise errechnet werden. Bekannte Methoden hierfür wären zum Beispiel die Spektrale Analyse, Dynamische Entkopplung, Hahn-Echo und Ramsey-Interferometrie. Außerdem wird duch das häufige messen der Dekoheränzzeit diese indirekt verlänger. Diesen Effekt nennt man Quanten-Zeno-Effekt.
Zuletzt muss auch die Lindblad-Gleichung genannt werden welche den Zeitverlauf der Dichtematrix in einem Offenen Quantensystem beschreibt.

$$\frac{dp}{dt} = -i[H, p] + \sum_i (L_i p L_i^\dagger - \frac{1}{2}\{L_i^\dagger L_i, p\}) \tag{45}$$

Diese Themen sprengen jedoch den Rahmen dieser Arbeit in Richtung Physik und werden deswegen nicht weiter behandelt.

5.2 Universelle Quantencomputer

Universelle Quantencomputer beruhen grundlegend auf einem Gatter Modell, wie bereits in diesem Artikel beschrieben. Folgend sind drei der meist erforschten Methoden, welche dieses Modell physikalisch umsetzen.

Ein prominentes Beispiel für die Umsetzung eines universellen Quantencomputers ist der **Sycamore Chip**, welcher auf supraleitenden Qubits basiert. Dieser Chip ist in einem Gatter angeordnet für die Kommunikation zwischen Qubits und die durchführung von Quantenoperationen.

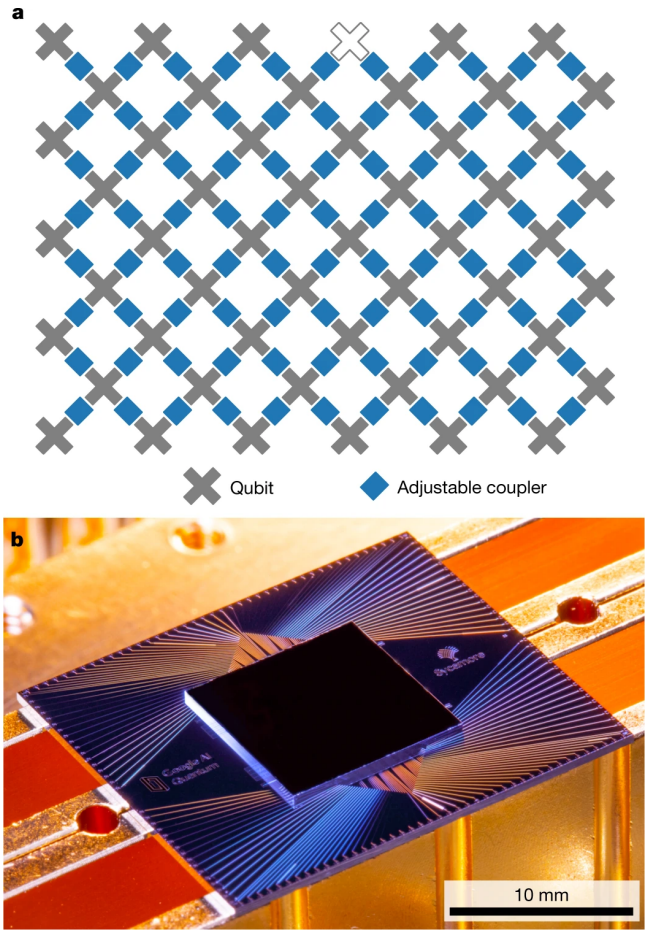

Abbildung 9: Sycamore Chip von Google

5.2.1 Supraleitende Qubits

Quantencomputer mit Supraleitern funktionieren mit elektrischen Schaltkreisen, die bei Temperaturen nahe dem absoluten Nullpunkt betrieben werden. Solche Temperaturen sind nötig, um die supraleitende Eigenschaft aufrecht zu erhalten.

Zwei häufig benutze Qubit-Typen dieser elektrischen Schaltkreise sind:
Transmon-Qubits, basieren auf der Ladung des Energieniveaus, welche durch eine Josephson-Junktion kontrolliert werden.
Flux-Qubits werden auch durch Josephson-Junktions kontrolliert, beruhen jedoch auf dem magnetischen Fluss in der Schleife.

Beide Ansätze basieren auf dem **Josephson-Effekt**, welcher auftritt, wenn ein supraleitender Strom durch eine dünne Isolierschicht zwischen zwei Supraleitern fließt.
Dieser Effekt hat zur Folge, dass eine nichtlineare Energie die für die Phasenunterscheidung der Qubits genutzt wird.

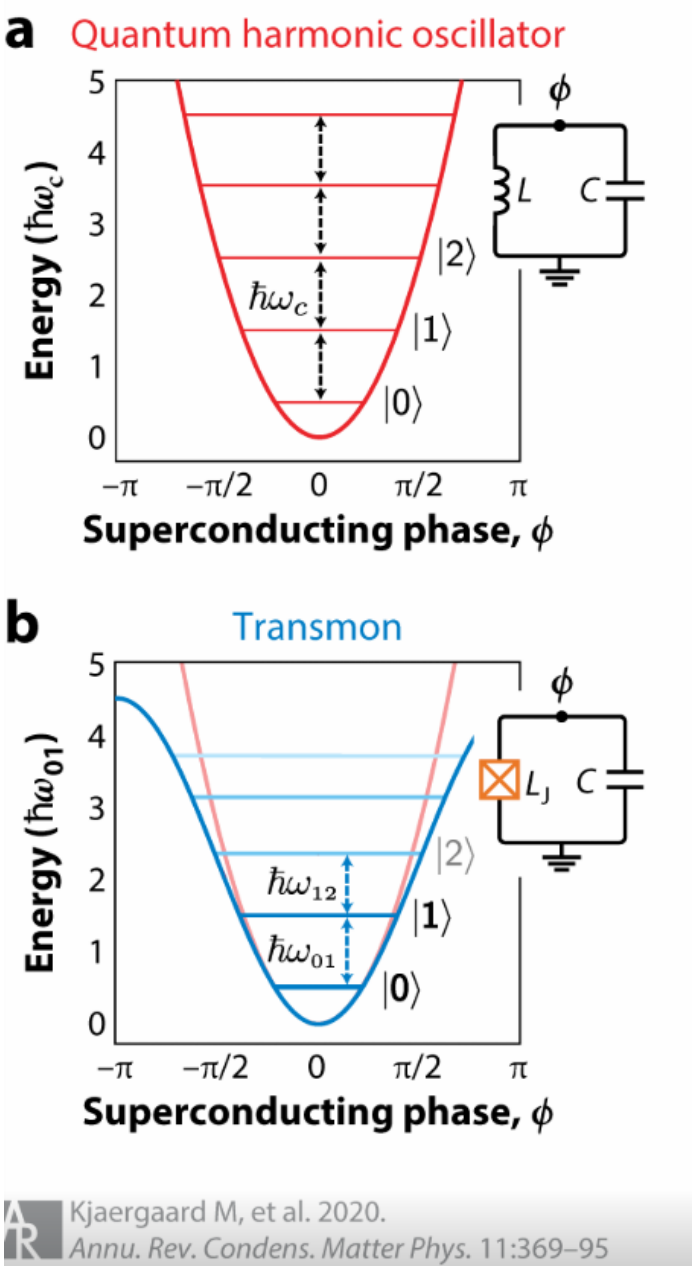

Abbildung 10: Josephson-Effekt mit einem Josephson Junktion

In der vorliegenden Abbildung wird der Unterschied zwischen einer harmonischen Quantenschwankung (a) und der nichtlinearen Schwankung des Energieniveau der Josephson Junktion (b) abgebildet.

Der Phasenunterschied bei der harmonischen Oscellation, gekennzeichnet als $\hbar\omega_c$, ist identisch. Auf der Abbildung ist zu sehen, dass das Energieniveau der Phasen zwischen $|0\rangle \leftrightarrow |1\rangle$ und $|1\rangle \leftrightarrow |2\rangle$ identisch ist und dadurch nicht unter-

schieden werden kann zwischen welcher Phase gewechselt wurde.

Mit einer Josephson Junktion kann jedoch eine nichtlineare Schwankung des Energieniveaus erreicht werden, die auf der Abbildung als orangenes ⊠ gekennzeichnet ist (b). Durch diese nichtlineare Schwankung ist das Energieniveau zwischen den Phasen $|0\rangle \leftrightarrow |1\rangle$ und $|1\rangle \leftrightarrow |2\rangle$ unterschiedlich groß und kann somit unterschieden werden. Der als $\hbar\omega_{01}$ gekennzeichnete Energieunterschied ist unser Qubit

Steuerung und Auslesung
Die Steuerung der Josephson-Junktion erfolgt durch Mikrowellenpulse, welche die Energie des Qubits verändern. Die Auslesung erfolgt durch eine Mikrowellenresonanz um die Energie des Qubits zu messen.

5.2.2 Quantenpunkte

Quantencomputer basierend auf Quantenpunkten, auch Quantum-Dot genannt, nutzen winzige Halbleiterstrukturen um Qubits zu realisieren. Quantum-Dots sind künstlich erzeugte Nano-Partikel, in denen Elektronen in drei Dimensionen eingeschlossen sind, was zu quantisierten Einergiezuständen führt.

Die Größe eines Quantum-Dots ist typischerweise 2-10 Nanometer und es schließt eine kleine Anzahl oder ein einzelnes Elektron ein. Für die Fertigung werden oftmals Galliumarsenid (GaAs) oder Silizium (Si) verwendet. Der physikalische Einschluss der Elektronen schränkt ihre Bewegung stark ein, wodurch ein quantisiertes Energieniveau entsteht. Dies ähnelt dem Energieniveaus eines Atoms, weswegen Quantum-Dots auch als künstliche Atome bezeichnet werden.

Die Zustände der Qubits werden durch die Eigenschaften einzelner Elektronen in den Quantum Dots definiert. Es gibt zwei Hauptansätze zur Realisierung von Qubits mit Quantum Dots.

Ladungs-Qubits
Der Ladungszustand eine Quantum Dots kann als Qubit verwendet werden. Die Ladung eines Elektrons kann entweder 0 oder 1 sein, was als $|0\rangle$ und $|1\rangle$ interpretiert wird. Für eine Messung wird der Ladungszustand mit einer Kapazitätsmessung der Tunnelströme ermittelt. Für die Manipulation des Qubits werden elektrische Felder verwendet, um die Elektronen in den Quantum Dots zu bewegen.

Diese Methode ist durch die Ladungsquantisierung sehr genau, jedoch auch sehr empfindlich gegenüber Störungen durch die Umgebung.

Spin-Qubits
Die Spin-Eigenschaften von Elektronen in Quantum Dots können auch als Qubit verwendet werden. Hierbei sind die beiden Spinrichtungen($\uparrow$ für Spin-Up und $\downarrow$ für Spin-Down). Dieser beiden Spinrichtungen entsprechen den Zuständen $|0\rangle$ und $|1\rangle$ und die Kombination aus beiden Zuständen ergibt eine Superposition.

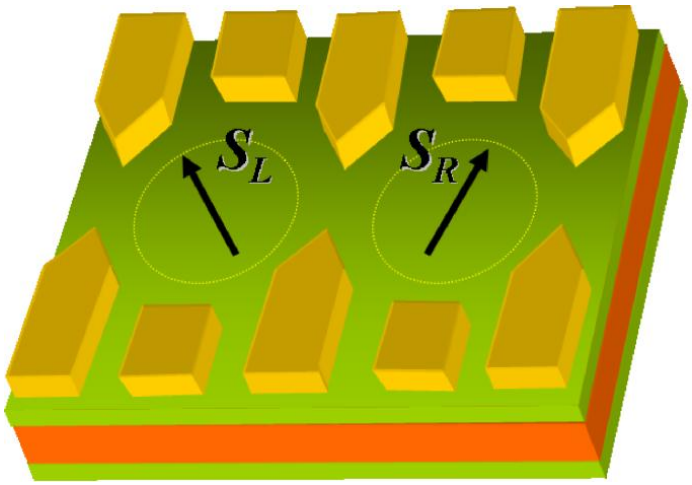

Abbildung 11: Ein doppel Quantum-Dot Qubit

In der Abbildung ist ein Doppel Quantum-Dot Qubit dargestellt. Sowohl in S_L als auch S_R befinden sich Elektornen. Beide können separat voneinander, sowohl im Spin als auch in der Ladung, manipuliert werden. Durch die physikalische Nähe der beiden Quantum-Dots können durch Tunnelkopplung und Austauschwechselwirkung die beiden Qubits miteinander verschränkt werden.

Die Umsetzung dieser Methode beschränkt sich hauptsächlich auf die Spin-Variante. Der Grund dafür ist, dass durch die hohe Ladungsanforderung der Ladungsvariante die Qubits sehr empfindlich gegenüber Störungen sind. Außerdem sind die Nachteile der Spin-Variante gegenüber der Ladungsvariante nicht so gravierend.
Jedoch sind die größten Herausforderungen die Herstellung der Halbleiterstrukturen und die Kontrolle der Elektronen in den Quantum-Dots. Damit ist der größte Vorteil, die hohe Skalierbarkeit, auch der größte Nachteil, da die Herstellung und Kontrolle von vielen Quantum-Dots sehr aufwendig und schwierig ist.

5.2.3 Topologische Quantencomputer

Der Ansatz von topologischen Quantencomputern ist völlig anders als die bisher genannten. Im Gegensatz zu vorher erläuterten Quantencomputern, welche auf Eigenschaften einzelner Elektronen oder Energieniveaus basieren, basieren topologische Quantencomputer auf topologischen Eigenschaften von Materie.
Diese Methode soll das Problem der Dekoheränz minimieren, indem sie Qubits aus Majorana-Partikeln aufbauen.

Topologie in der Physik
In einem physikalischem System beschreibt die Topologie die Eigenschaften, welche sich nicht durch Deformation verändern lassen. Ein Beispiel hierfür ist ein Kaffeebecher, der sich durch Verformung in eine Donutform umwandeln lässt. Beide haben die topologische Eigenschaft eines Loches. Daraus folgernd ist es nicht möglich, einen Kaffeebecher oder ein Donut in eine Kugel zu verformen

ohne die topologische Eigenschaft zu verändern.

Funktionsweise
Die physikalische Grundlage für topologische Quantencomputer liegt in speziellen Materialien und Systemen, die topologische Materiephasen unterstützen. Ein prominentes Beispiel ist die Verwendung von Majorana-Quasiteilchen, die in bestimmten Supraleitern auftreten können.

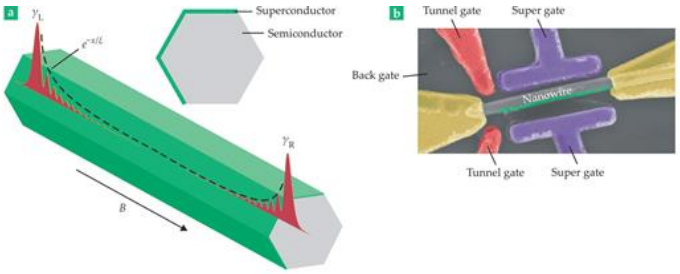

Abbildung 12: Nanowire mit Majorana-Quasiteilchen

In der Abbildung ist ein Nanowire dargestellt, der durch ein Supraleiter und ein Magnetfeld in eine topologische Phase gebracht wird. Diese Art von Partikel treten immer als Paar auf und bilden eine Art Brücke zwischen den Enden des Nanowire und besteht auf einer Vielzahl von Elektronen. Diese Brücke wird durch die topologischen Eigenschaften der Majorana-Partikel stabilisiert und ist somit weniger anfällig gegenüber Störungen.

Kommentar

Die Vertiefung der durch den Quanten-Hall Effekt entsteht wird nur oberflächlich behandelt. Ist jedoch essentiell für die Funktionsweise von Topologischen Quantencomputern.

Verpflechtung
Braiding ist der Prozess, bei dem die Majorana-Partikel miteinander verflochten werden, um die Quantenbits zu manipulieren. Dies passiert auf einer zweidimensionalen Oberfläche, auf der die Majorana-Partikel miteinander verflochten werden.

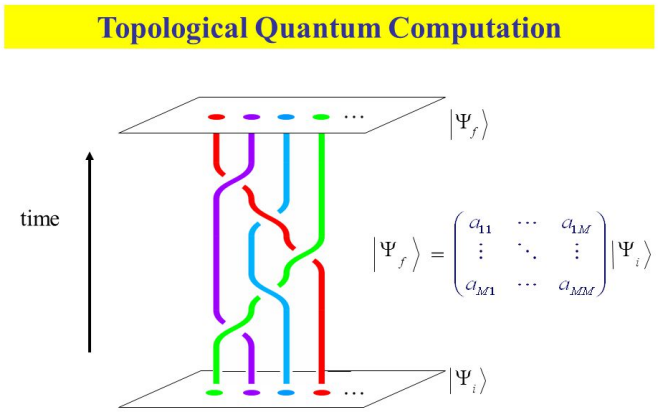

Abbildung 13: Braiding von Majorana-Quasiteilchen

Hierbei ist die Reihenfolge sehr wichtig, da durch diese Reihenfolge Quantenoperationen realisiert werden. Jede Verpflechtung entspricht einer Quantenoperation und durch die Kombination von mehreren Verpflechtungen können beliebige Quantenoperationen realisiert werden.

Da die Informationen und Quantenoperationen in der Topologie steckt, sind sie gegenüber kleinen Fehlern in der Bewegung/Störungen unempfindlich.

Kommentar

Die Technische Umsetzung von topologischen Quantencomputern ist deutlich komplizierter als es in diesem Abschnitt oberflächlich beschrieben ist.
Bisher hat nur Google einen topologischen Quantencomputer vorgestellt, der jedoch noch nicht in der Lage ist, Quantenoperationen durchzuführen.

5.3 Quantum Error Correction

Quantum Error Correction, oder auch QEC genannt, ist grundlegend wichtig für die funktionellen Betrieb eines Quantencomputers. Wie bereits in den vorherigen Abschnitten beschrieben, sind Qubits sehr anfällig gegenüber Dekoheränz und Quantenrauschen.

Warum ist Fehlerkorrektur notwendig
Es ist unabdingbar, dass eine Fehlerkorrektur in Quantencomputern implementiert wird, da die Fehleranfälligkeit von physischen Qubits durch bessere Herstellung nur einen gewissen Grad an Fehlertoleranz aufbringen kann, welche nicht genug ist.

Fehler treten in Quantencomputer durch drei Hauptquellen auf.
1. **Dekoheränz:** Äußere Einflüsse wie Temperaturschwankungen oder elektromagnetische Felder zerstören die koheränten Eigenschaften der Qubits.
2. **Phasen-Flip-Fehler:** Die Phasenwinkel zwischen den Quantenzuständen werden verändert($|0\rangle \rightarrow |0\rangle, |1\rangle \rightarrow -|1\rangle$).
3. **Bit-Flip-Fehler:** Die Zustände der Qubits werden verändert ($|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$).

Bei der Fehlerkorrektur von Quantencomputern ist jedoch zu beachten, dass diese nicht wie bei herkömmlichen Computern implementierbar ist, da durch das No-Cloning-Theorem keine Quanteninformationen kopiert werden können.

Grundprinzip
Quanten-Fehlerkorrektur verwendet **Redundanz** um Fehler zu detektieren und zu korrigieren, ohne dass die eigentliche Quanteninformationen direkt ausgelesen werden müssen.

Eine Art der Redundanz ist der Steane-Code, welcher auf 7 Qubits basiert. Dieser Zusammenschluss aus 7 Physischen Qubits bildet ein logisches Qubit, welches maximal einen Fehler auf einem der 7 Qubits korrigieren kann. Treten jedoch mehrere Fehler auf, kann der Steane-Code diese nicht mehr korrigieren.

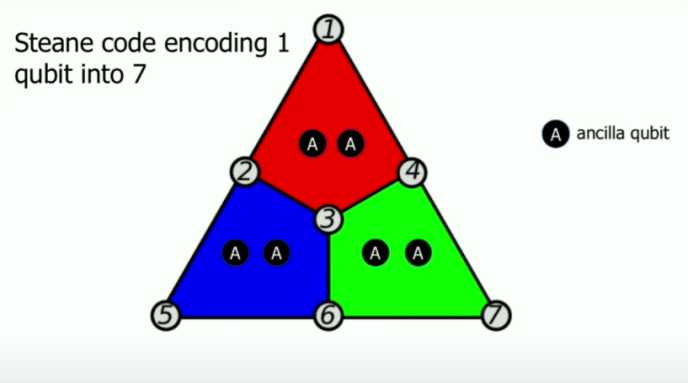

Abbildung 14: Steane-Code

Um die Qubits zu überwachen werden zusätzliche Qubits benötigt. Der Grund hierfür ist die Daten-Qubits, in der Abbildung mit 1-7 gekennzeichnet, nicht direkt zu messen und den Quantenzustand zu bewahren. Diese zusätzlichen Qubits werden als **Ancilla Qubit** bezeichnet und mit den eigentlichen Qubits verschränkt.

Fehlertoleranz
Diese Herangehensweise ist jedoch auch nicht perfekt. Die Ancilla Qubits sind gleichermaßen anfällig gegenüber Fehlern wie die eigentlichen Qubits.

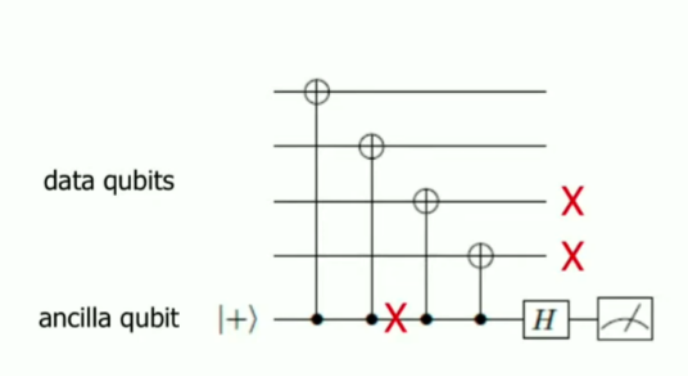

Abbildung 15: Fehlertoleranz von Ancilla Qubits

Dieses Abbildung zeigt, wie ein einzelner Fehler in einem CNOT Gatter auf dem Ancilla Qubit Messung ein Daten-Qubits als fehlerhaft kennzeichnet und eigentlich richtige Daten-Qubits korrigiert.
Die Folge hieraus ist, dass die Fehlerkorrektur mit wenigen Qubits nicht ausreicht um diesen logischen Qubit vollkommen fehlerfrei zu halten.

Hierbei werden zwischen zwei Paritätchecks unterschieden. Eine Z und X Parität, welche festlegen, ob der Fehler im CNOT Gatter des Ancilla Qubits oder den Daten Qubits aufgetreten ist.

Suface Code
Eine weitere Methode zur Fehlerkorrektur ist der Surface Code, welcher auf einem 2D Gitter von Qubits basiert. Dieser Code ist in der Lage Fehler zu detektieren und zu korrigieren, solange die Fehlerdichte unter einem bestimmten Wert bleibt.

Die Größe des Surface Codes ist variabel und kann skaliert werden, um die Fehlerkorrektur zu verbessern. Es gibt jedoch ein Threshold, an der die Vergößerung des Codes keine Verbesserung mehr bringt. Durch die vorher besprochene Fehlertoleranz der Ancilla Qubits wird die Effektivität des Surface Codes gedeckelt. Die Fehler in der Korrektur werden hierbei mehr, als wenn keine Korrektur vorgenommen wird und es würde keinen Sinn ergeben, den Surface Code weiter zu vergößern.

Die Nachfolgende Abbildung eines Surface Codes des Grades $d = 3$ zeigt wie die Qubits in einem 2D Gitter angeordnet sind und wie die Fehlerkorrektur durchgeführt wird. Jede Überschneidung des Gatters stellt ein physisches Qubit dar. Die Kreise in den Quadraten sind die Ancilla Qubits, welche die Fehlerkorrektur durchführen.

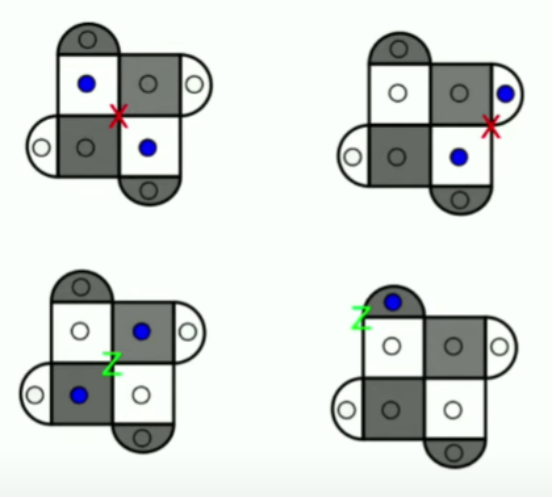

Abbildung 16: Fehlerkorrektur durch Surface Code des Grades $d = 3$

Ancilla Qubits in einem weißen Feld prüfen die Qubits auf ein logisches X und Ancilla Qubits in einem Schwarzen Feld prüfen die Qubits auf ein logisches Z.

Ancilla Qubits, die einen Fehler erkennen, werden als Blau markiert. Durch die Position dieser und für welche Daten Qubits diese zuständig sind, wissen wir welche Qubits fehlerhaft sind.

Praktische Umsetzung
Am 09.12.2024 hat Google den ersten selbst korrigierenden Quantencomputer vorgestellt, der auf dem Surface Code basiert. Der Chip namens **Willow** basiert auf 105 physischen Qubits, wobei diese auf der 7x7 Surface Code Architektur aufbaut. Dies resultiert in 49 Qubits, die deutlich weniger anfällig gegen Fehler sind als phyische Qubits. Die restlichen Qubits werden für Parität und error Korrektur gebraucht.

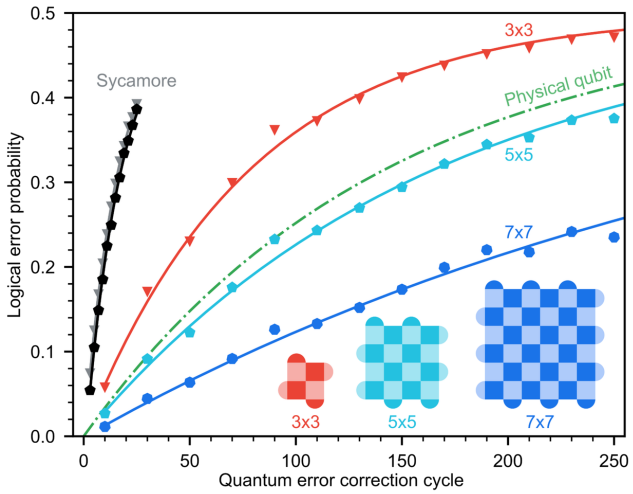

Abbildung 17: Error Korrektur des 7x7 Surface Code

Außerdem wurde durch die Anwendung des Surface Codes die T_1 Zeit von $20\mu s$ auf $68\mu s \pm 13\mu s$ erhöht und ermöglich hierdurch mehr Operationen pro Qubit.

6 CHSH-Ungleichung

6.1 Geschichte

6.2 Bell‘s Inequalität

Bell‘s Inequalität bezieht sich auf die statistische korrelation zwischen Messungen von verschränkten Teilchen. Die Ungleichung wurde von John Bell 1964 formuliert und besagt, dass die Wahrscheinlichkeit der Messergebnisse von verschränkten Teilchen durch eine lokale versteckte Variable erklärt werden können, und hierdurch begrenzt ist. Wenn die korrelation jedoch über die Grenze der Ungleichung hinausgeht, kann dies nur durch Quantenmechanik erklärt werden.

Bell setzte für seine Idee voraus mehrere kopien von verschränkten Teilchen zu haben, dise Partikel können heutzutage druch ein Zerfallsprozess erreicht werden in dem ein Partikel in zwei verschränkte Teilchen zerfällt.

Durch den Zeraffl eines Teilchen, und dem Stern-Gerlach-Experiment, wissen wir das ein Teilchen mit einem Spin von 0 in zwei Teilchen mit einem Spin von $1/2$ zerfällt.

$$S = 0 \rightarrow S_1 = S_2 = \pm\frac{1}{2} \tag{46}$$

Beide Teilchen haben den Spin von $\pm\frac{1}{2}$ müssen jedoch sich gegenseitig aufheben, sodass die Summe der Spins 0 ergibt. Dies nennt man auch spin up und spin down. Wenn das eine Teilchen spin up ist muss das andere spin down sein und anders herum.
Dadurch sind die beide Teilchen miteinander verschränkt und kann wie folgt beschrieben werden:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\,|\downarrow\rangle - |\downarrow\rangle\,|\uparrow\rangle) \tag{47}$$

Gehen wir davon aus das wir zwei Messungen durchführen, die Messung von Alice und die Messung von Bob. Beide dürfen den Spin des Partikels in jede beliebige Richtung messen, wie sind die beiden Messungen korreliert?
Laut Einstein ist jedes einzelne Teilchen deterministisch, das bedeutet das die Messung vom Spin des Teilchens nicht zufällig ist, sondern durch eine versteckte Variable bestimmt wird und dadurch der Spin beider Teilchen nicht korreliert sind.
Daraus folgernd muss die Messergebnisse deterministisch sein. Wenn Bob $(+a, +b, -c)$ misst, dann muss Alice $(-a, -b, +c)$ sein welches durch die versteckte Variable vorherbestimmt ist und zusammen ein 0 spin ergibt. Durch die voraussetzung des aufheben des spins kann eine Tabelle an alle deterministischen messergebnissen erstellt werden.

Population	Particle 1	Particle 2
N_1	$(+\hat{a}, +\hat{b}, +\hat{c})$	$(-\hat{a}, -\hat{b}, -\hat{c})$
N_2	$(+\hat{a}, +\hat{b}, -\hat{c})$	$(-\hat{a}, -\hat{b}, +\hat{c})$
N_3	$(+\hat{a}, -\hat{b}, +\hat{c})$	$(-\hat{a}, +\hat{b}, -\hat{c})$
N_4	$(+\hat{a}, -\hat{b}, -\hat{c})$	$(-\hat{a}, +\hat{b}, +\hat{c})$
N_5	$(-\hat{a}, +\hat{b}, +\hat{c})$	$(+\hat{a}, -\hat{b}, -\hat{c})$
N_6	$(-\hat{a}, +\hat{b}, -\hat{c})$	$(+\hat{a}, -\hat{b}, +\hat{c})$
N_7	$(-\hat{a}, -\hat{b}, +\hat{c})$	$(+\hat{a}, +\hat{b}, -\hat{c})$
N_8	$(-\hat{a}, -\hat{b}, -\hat{c})$	$(+\hat{a}, +\hat{b}, +\hat{c})$

Abbildung 18: Bell zuständen nach der versteckten Variable

Jetzt errechnen wir die Wahrscheinlichkeit das Alice und Bob, bei unabhängigen Messungen, das selbe vorzeichen messen. Die Wahrscheinlichkeit in Zeile 1 und 8 sind 0%und in Zeile 2 bis 7 sind es $P = \frac{4}{9}$. Das bedeutet das nach Einstein die Wahrscheinlichkeit das Alice und Bob das selbe messen $P \leq \frac{4}{9}$ ist. Dies ist Bell‘s Inequalität.
Vorliegendes beispiel ist generalisiert und kann auf beliebige Winkel angewendet werden, wobei die Wahrscheinlichkeit wie folgt für alle möglichen Winkel berechnet wird.

$$E(\overrightarrow{a}, \overrightarrow{b}) = \int d\lambda \rho(\lambda) A(\overrightarrow{a}, \lambda) B(\overrightarrow{b}, \lambda) \tag{48}$$

Nun zu der Wahrscheinlichkeit nach der Quantenmechanik. Wir gehen davon aus das Bob den spin in a richtung misst beispielsweise spin up, daraus folgernd muss wenn Alice in a richtung misst das Ergebniss spin down sein.
Dadurch das wir das Ergebniss einer der achsen kennen, können wir die Wahrscheinlichkeit für die anderen Achsen mit folgender Gleichung berechnen.

$$P(b) = \cos^2(\frac{\theta}{2}) \tag{49}$$

Hierbei ist θ der Winkel zwischen den Achsen. Wenden wir dies auf das beispiel auf die Achse b an so setzen wir $\theta = 60°$

$$P(b) = \cos^2(\frac{60°}{2}) = \frac{3}{4} \tag{50}$$

Machen wir dies auch für die andere Achse c wo $\theta = 120°$ ist erhalten wir

$$P(c) = \cos^2(\frac{120°}{2}) = \frac{1}{4} \tag{51}$$

Von diesen beiden Wahrscheinlichkeit errechnen wir den durchschnitt von $P = \frac{1}{2}$, was bedeutet das Bell‘s Inequalität mit $P = \frac{1}{2} \geq \frac{4}{9}$ verletzt ist.

6.2.1 Bell im Quantumcomputer

Wir haben das Beispiel von Bell's Inequalität in der Quantenmechanik gezeigt, jedoch ist es auch möglich dies in einem Quantumcomputer zu zeigen. Hierbei haben wir das Bells Theorem folgendermaßen umgesetzt.

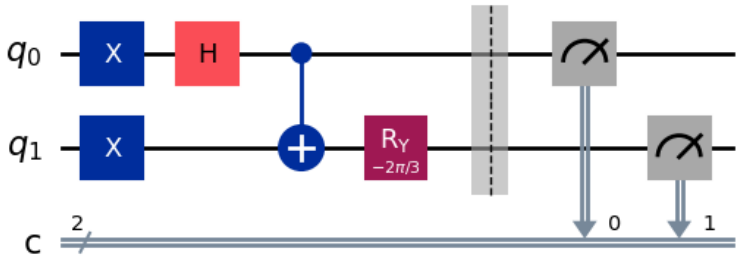

Abbildung 19: Bell's Theorem im Quantumcomputer

Die beiden linien q_0 und q_1 sind die beiden verschränkten Teilchen, die durch den zerfall eines Teilchens entstanden sind. Den verschänkten zustand erreichen wir durch die beiden X gates, dass H gate und das CNOT gate. Nachdem wir den verschränkten Zustand erreicht haben, messen wir q_0 in der a Achse und q_1 an der b Achse. Dies ist mit dem R_y gate realisiert der die messung um 120° dreht.

Um eine genaueres Ergebniss zu erhalten, führen wir diese Messungen 30000 mal durch

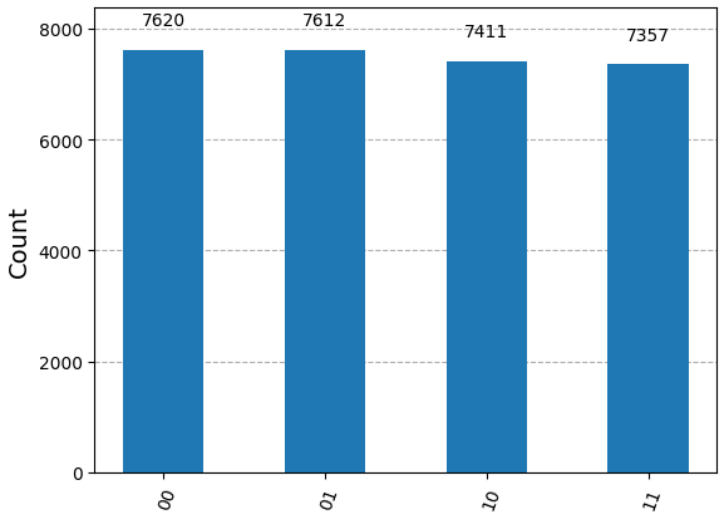

Abbildung 20: Ergebniss von Bell's Theorem im Quantumcomputer

Die Ergebnisse zeigen das die Wahrscheinlichkeit das selbe vorzeichen zu mes-

sen bei $P = (7620 + 7357)/30000 = 0.49923$ oder auch 49,923% liegt, was Bell's Inequalität verletzt.

6.3 CHSH experimentell

6.4 local hidden variable theory

7 Schluss

Zusammenfassend lässt sich festhalten, dass die Quanteninformatik ein vielversprechendes Feld darstellt, dass das Potenzial hat, klassische Computer in zahlreichen Bereichen zu übertreffen. So haben wir in den Grundlagen die fundamentalen Prinzipien und Funktionsweisen für Quantencomputer herausgestellt. Mit Quantenbits ist es möglich, mehrere Zustände gleichzeitig zu repräsentieren was zusammen mit der Zerstörung der Superposition durch Messungen einen entscheidenden Vorteil in der Kryptografie bietet. Die Verschränkung ermöglicht es, dass zwei Quantenbits in einem Zustand sind, sodass die Messung eines Bits den Zustand des anderen beeinflusst, was die Grundlage für Quantenteleportation bildet.

Mit dem No Cloning Theorem haben wir eine der grundlegendsten Einschränkungen und gleichzeitig auch Möglichkeit in der Quanteninformatik kennengelernt. Es besagt, dass ein unbekannter Quantenzustand nicht kopiert werden kann. Zum einen erfordert dies eine neue Denkweise bei der Entwicklung von Algorithmen, zum anderen bietet es die Möglichkeit, Quantenkommunikation abhörsicher zu gestalten.

Die Quantenteleportation ist eines der faszinierendsten Konzepte der Quanteninformatik, welches die Übertragung von Informationen ohne physische Bewegung ermöglicht. Hier liegt die Herausforderung in der Erzeugung und Aufrechterhaltung der Quantenverschränkung, sowie der Notwendigkeit der klassischen Kommunikation.

Eine der größten technischen Hürden bildet die Dekohärenz, die durch die Wechselwirkung der Quantenbits mit ihrer Umgebung entsteht. Es wurde beleuchtet, wie sie entsteht und berechnet wird, sowie wie sie durch Fehlerkorrekturverfahren minimiert werden kann. Außerdem wurden unterschiedliche Modelle für universelle Quantencomputer vorgestellt, die auf verschiedenen Technologien basieren.

Zusammenfassend lässt sich sagen, dass die Quanteninformatik sowohl ein enormes Potenzial als auch einige fundamentale Herausforderungen birgt. Die Entwicklung von Quantencomputern und -algorithmen ist ein aktives Forschungsfeld, das in den nächsten Jahren weiter an Bedeutung gewinnen wird. Wir sind sehr gespannt, wie sich die Technologie entwickeln wird und in welchen Bereichen wir selbst damit auch in Berührung kommen werden.

8 Quellenverzeichnis

Homeister, Matthias. *Quanten Computing verstehen.* Springer Verlag, 2022, 6.Auflage.

Fraunhofer Cluster of Excellence Cognitive Internet Technologies. *Quantencomputing – Forschungsthemen.* cit.fraunhofer.de., (abgerufen am 02. März 2025)

Technische Universität Wien. *Grenzen für Quantencomputer: Perfekte Uhren sind unmöglich.* tuwien.at., (abgerufen am 02. März 2025)

Bundesamt für Sicherheit in der Informationstechnik. *Quantenmechanische Sicherheitslücken (QML) - Studien.* bsi.bund.de., (abgerufen am 02. März 2025)

Fraunhofer-Institut für Werkstoffmechanik IWM. *Quantencomputer für innovative Materialsimulation nutzen.* iwm.fraunhofer.de., (abgerufen am 02. März 2025)