Quantenteleportation

Kurztext im Rahmen von „Quanten auf Reisen“

Physikdidaktik, Albert-Ludwigs-Universität Freiburg

Weitere Kurztexte hier: https://physikdidaktik.uni-freiburg.de/kurztexte/

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

universität freiburg

Inhaltsverzeichnis

1 Quantenteleportation **3**

1.1 No-Cloning-Theorem 4

1.2 Teleportation eines Qubits 5

1.2.1 Protokoll 5

1.2.2 Beispiel 6

1.2.3 Experimentelle Umsetzung 7

1.3 Anwendungen 8

Kapitel 1

Quantenteleportation

Autor: Anja Kuhnhold, Version vom: 23.11.2025
[1]

Den Zustand eines Quantensystems kann man weder beliebig genau bestimmen, noch kann man ihn exakt kopieren. Während klassische Informationen problemlos vervielfältigt werden können, sind Quantenzustände diesen Beschränkungen durch die Prinzipien der Quantenmechanik unterworfen. Man kann zwar Messungen durchführen, aber die möglichen (zufälligen) Messergebnisse hängen von der Wahl der gemessenen Observablen ab und der Zustand nach einer Messung entspricht immer dem Eigenzustand der gemessenen Observablen, der zu dem beobachteten Wert gehört (Projektionspostulat). Der Ausgangszustand wird daher im Allgmeinen durch eine Messung zerstört.

Es gibt jedoch die Möglichkeit, einen Quantenzustand zu übertragen, ohne dass dabei der Zustand unterwegs klassisch ausgelesen oder kopiert wird. Der Zustand muss dem Sender dabei nicht bekannt sein. Bei der Quantenteleportation wird ein Zustand mittels Messungen an maximal verschränkten Systemen (Qubits in einem Bell-Zustand) und Austausch von klassischen Informationen (2 Bits reichen) von einem Ort zu einem anderen übertragen, wobei der Ausgangszustand während des Vorgangs vernichtet wird (daher die Bezeichnung Teleportation). Es wird jedoch, im Gegensatz zum aus der Science Fiction bekannten Beamen, keine Materie transportiert, sondern nur der Quantenzustand des Systems übertragen.

Die Idee zur Quantenteleportation wurde 1993 von Forschern aus verschiedenen Institutionen gemeinsam veröffentlicht, u.a. Charles Bennett und Gilles Brassard, die auch für das BB84-Quantenkryptographieprotokoll verantwortlich sind, oder William Wootters, der viel zum Thema Quantenverschränkung beitrug [1].

[1] Bei der Überarbeitung und Gliederung dieses Textes wurde ChatGPT zu Rate gezogen (Zugang: HAWKI, https://hawki.uni-freiburg.de/interface, ChatGPT-4.1 (Provider: Firma OpenAI), bzw. Open WebUI, https://openwebui.uni-freiburg.de/ OpenAI: ChatGPT-5/5.2).

1.1 No-Cloning-Theorem

Die Unmöglichkeit des exakten Kopierens eines unbekannten quantenmechanischen Zustands bezeichnet man als No-Cloning-Theorem. Natürlich kann man Systeme immer im gleichen Zustand präparieren, also sozusagen Zustände kopieren; aber eben nur, wenn der Zustand vollständig bekannt ist (also klassisch beschrieben werden kann) und nicht, wenn es sich um einen beliebigen, möglicherweise unbekannten Quantenzustand handelt. Die Sicherheit von Quantenkryptographieprotokollen beruht u.a. auf dem No-Cloning-Prinzip. So kann ein Lauscher bei einem Schlüsselaustausch mit Hilfe von Quantenobjekten nicht einfach das Objekt abfangen, kopieren, das Original weitersenden und seine Kopie untersuchen. Jede Manipulation an dem übertragenen Quantenobjekt lässt sich leicht feststellen.

Der Beweis des Theorems durch Widerspruch benötigt nur wenige Zeilen und beruht auf der Linearität der Quantenmechanik: Angenommen, es gäbe eine unitäre Abbildung U, die einen beliebigen Zustand $|\phi\rangle$ auf einen Zustand $|k\rangle$ kopiert, ohne $|\phi\rangle$ zu zerstören, d.h.:

$$U\left(|\phi\rangle \otimes |k\rangle\right) = |\phi\rangle \otimes |\phi\rangle \ . \tag{1.1}$$

Dies muss dann auch für einen anderen Zustand $|\psi\rangle$ funktionieren (denn U soll beliebige Zustände kopieren können):

$$U\left(|\psi\rangle \otimes |k\rangle\right) = |\psi\rangle \otimes |\psi\rangle \ . \tag{1.2}$$

Das Kopieren soll längen- und winkeltreu sein (daher unitär), was bedeutet, dass Skalarprodukte sich unter der Abbildung nicht ändern:

$$\langle \phi \otimes k | \psi \otimes k\rangle = \langle U\left(|\phi\rangle \otimes |k\rangle\right) | U\left(|\psi\rangle \otimes |k\rangle\right)\rangle = \langle \phi \otimes \phi | \psi \otimes \psi\rangle \tag{1.3}$$

$$\langle \phi | \psi\rangle \langle k | k\rangle = \langle \phi | \psi\rangle \langle \phi | \psi\rangle \ . \tag{1.4}$$

$|k\rangle$ kann so gewählt werden, dass $\langle k | k\rangle = 1$ ist, woraus folgt, dass, wegen $\langle \phi | \psi\rangle = \langle \phi | \psi\rangle^2$, $\langle \phi | \psi\rangle$ entweder 1 oder 0 sein kann. Falls man also eine Abbildung findet, die $|\phi\rangle$ kopieren kann, kann diese auch noch parallele und orthogonale Zustände zu $|\phi\rangle$ kopieren, nicht jedoch einen beliebigen unbekannten Zustand. Es kann keine allgemeine Kopierfunktion für beliebige Quantenzustände geben. Das No-Cloning-Theorem ist damit eine der zentralen Einschränkungen in der Quanteninformationstheorie und unterscheidet Quanteninformation grundlegend von klassischer Information.

1.2 Teleportation eines Qubits

1.2.1 Protokoll

Im Folgenden erläutern wir das Teleportationsprotokoll anhand eines einzelnen Qubits und mittels Manipulation der Qubits durch Quantengatter[2]. Wir nutzen die üblichen Bezeichnungen Alice als Sender und Bob als Empfänger. Das Protokoll läuft wie folgt ab:

1. **Verschränkung:** Alice und Bob besitzen je ein Qubit eines maximal verschränkten Zwei-Qubit-Zustands, z.B. $|\psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

2. **Zu teleportierendes Qubit:** Alice hat zusätzlich das Qubit $|\phi\rangle$, dessen Zustand sie übertragen möchte. Alice verknüpft ihre beiden Qubits mit einem CNOT-Gatter, wobei $|\phi\rangle$ das Kontroll-Qubit ist, und wendet auf $|\phi\rangle$ ein Hadamard-Gatter an.

3. **Messung und klassische Informationsübertragung:** Eine gemeinsame Messung ihrer beiden Qubits liefert ihr anschließend eine der vier Möglichkeiten $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ zu jeweils 25% Wahrscheinlichkeit. Diese zwei klassischen Bits teilt Alice Bob mit.

4. **Korrektur bei Bob:** Daraufhin weiß Bob, ob und welches weitere Gatter er auf sein Qubit anwenden muss, damit dieses dann im Zustand $|\phi\rangle$ endet. Bei $|00\rangle$ muss er nichts tun; bei $|01\rangle$ muss er eine X-Operation (NOT) durchführen; bei $|10\rangle$ muss er eine Z-Operation durchführen (Drehung um 90 Grad um die $|0\rangle$-Achse, d.h. $|1\rangle \to -|1\rangle$); und bei $|11\rangle$ muss er beides machen (erst X, dann Z).

Die folgende Tabelle gibt eine Übersicht der möglichen Messresultate und der jeweils nötigen Korrekturoperation bei Bob:

Alices Messergebnis	**Korrekturoperation bei Bob**	**Symbolisch**
$\|00\rangle$	Identität (nichts tun)	I
$\|01\rangle$	X (NOT-Gatter)	X
$\|10\rangle$	Z (Phasengatter)	Z
$\|11\rangle$	X gefolgt von Z	XZ

Die verschiedenen Korrekturen, die Bob je nach Messwert durchführt, kann man auch mittels der CNOT- und CZ-Operationen darstellen, wie im folgenden Beispiel zu sehen ist.

[2] Es wird vorausgesetzt, dass der Leser sich ein wenig mit Quantengattern auskennt.

1.2.2 Beispiel

Wir verdeutlichen dies noch am Beispiel des $|+\rangle$-Zustands. Wir notieren an erster Stelle das zu übertragende Qubit, an zweiter Stelle Alices Qubit des verschränkten Paares und an dritter Stelle Bobs Qubit des verschränkten Paares. Weitere Hinweise zur Notation: CNOT(x→y) sorgt für das Invertieren des Qubits y, falls Qubit x im Zustand $|1\rangle$ ist. Hadamard(x) wandelt das Qubit x in $(|0\rangle + |1\rangle)/\sqrt{2}$, falls es im Zustand $|0\rangle$ ist, und in $(|0\rangle - |1\rangle)/\sqrt{2}$, falls es im Zustand $|1\rangle$ ist. CZ(x→y) dreht das Qubit y 90 Grad um die $|0\rangle$-Achse, falls Qubit x im Zustand $|1\rangle$ ist.

$$\text{Ausgangszustand: } |\omega\rangle = |+\rangle \otimes |\psi^+\rangle \tag{1.5}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.6}$$

$$= \frac{1}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \tag{1.7}$$

$$\text{CNOT}(1 \to 2)\text{: } |\omega\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle) \tag{1.8}$$

$$\text{Hadamard}(1)\text{: } |\omega\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |100\rangle + |011\rangle + |111\rangle + |010\rangle - |110\rangle + |001\rangle - |101\rangle) \tag{1.9}$$

$$\text{Messung(1,2): } |\omega(00)\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle) \tag{1.10}$$

$$|\omega(01)\rangle = \frac{1}{2\sqrt{2}}(|011\rangle + |010\rangle) \tag{1.11}$$

$$|\omega(10)\rangle = \frac{1}{2\sqrt{2}}(|100\rangle - |101\rangle) \tag{1.12}$$

$$|\omega(11)\rangle = \frac{1}{2\sqrt{2}}(|111\rangle - |110\rangle) \tag{1.13}$$

Korrektur bei Bob:

$$\text{CNOT}(2 \to 3)\text{: } |\omega(00)\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle) \tag{1.14}$$

$$(*)\, |\omega(01)\rangle = \frac{1}{2\sqrt{2}}(|010\rangle + |011\rangle) \tag{1.15}$$

$$|\omega(10)\rangle = \frac{1}{2\sqrt{2}}(|100\rangle - |101\rangle) \tag{1.16}$$

$$(*)\, |\omega(11)\rangle = \frac{1}{2\sqrt{2}}(|110\rangle - |111\rangle) \tag{1.17}$$

$$\text{CZ}(1 \to 3)\text{: } |\omega(00)\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle) = \frac{1}{2}|00\rangle \otimes |+\rangle \tag{1.18}$$

$$|\omega(01)\rangle = \frac{1}{2\sqrt{2}}(|010\rangle + |011\rangle) = \frac{1}{2}|01\rangle \otimes |+\rangle \tag{1.19}$$

$$(*)\, |\omega(10)\rangle = \frac{1}{2\sqrt{2}}(|100\rangle + |101\rangle) = \frac{1}{2}|10\rangle \otimes |+\rangle \tag{1.20}$$

$$(*)\, |\omega(11)\rangle = \frac{1}{2\sqrt{2}}(|110\rangle + |111\rangle) = \frac{1}{2}|11\rangle \otimes |+\rangle \tag{1.21}$$

Die verschiedenen Korrekturen, die Bob je nach Messwert durchführt, sind hierbei als CNOT und CZ interpretiert, da sie eben vom Ergebnis der vorhergehenden Messung abhängen. In jedem Fall endet Bobs Qubit im $|+\rangle$-Zustand und Qubit 1 trägt keine Information über seinen Ausgangszustand mehr. Das No-Cloning-Theorem wird also nicht verletzt.

Bemerkung: Da für das Teleportieren des Qubits das Übermitteln klassischer Bits nötig ist, findet hier kein überlichtschneller Austausch von Informationen statt.

Man könnte sich noch fragen, warum man nicht direkt das Quantenobjekt verschickt, sondern nur dessen Zustand übertragen möchte. Ein Grund ist, dass jede Art von Wechselwirkung die Gefahr mit sich bringt, den Zustand des Objekts zu verändern. Der ungestörte Transport des Objekts ist also nur sehr aufwendig möglich. Zum anderen kann man mit der Teleportation beliebige Orte erreichen, solange Sender und Empfänger im Besitz eines Teiles eines verschränkten Paares des Quantenobjekts sind. Der Sender muss nicht einmal wissen, wo sich der Empfänger befindet.

Der zu übertragende Zustand muss kein Einteilchenzustand sein. Es könnte sich alternativ um einen Teil eines mit anderen Teilchen verschränkten Zustands handeln bzw. können auch Mehrteilchenzustände übertragen werden.

1.2.3 Experimentelle Umsetzung

Die experimentelle Realisierung wurde beispielsweise von Bouwmeester et al. mit Hilfe von Photonen gezeigt [2]. Verschränkte Photonen können durch parametrische Fluoreszenz (*Spontaneous parameteric down-conversion*, SPDC) erzeugt werden. Die Verschänkung bezieht sich dabei auf den Polarisationszustand der Photonen. Die Verschränkung mit dem unbekannten Zustand erfolgt durch Überlagerung an einem Strahlteiler. Sobald das unbekannte Photon und Alices Photon exakt gleichzeitig auf einen Strahlteiler treffen, befinden sie sich danach in einem gemeinsamen Zustand. Dessen Messung liefert die klassischen Bits, die an Bob übertragen werden. Messungen bei Bob werden dann mit polarisierenden Strahlteilern durchgeführt. Neben Photonen sind als physikalische Plattformen auch Ionenfallen und supraleitende Qubits im Einsatz, um über verschiedene Distanzen hinaus Quantenteleportation zu zeigen.

1.3 Anwendungen

- **Quanteninternet und Quantenkommunikation:** Für ein globales Netzwerk—das Quanteninternet—ist es nötig, Quanteninformation verlustarm über große Distanzen zu übertragen. Herkömmliche Signalverstärker sind für Quantenzustände nicht einsetzbar, da sie das No-Cloning-Theorem verletzen würden. Stattdessen kommen sogenannte *Quantenrepeater* zum Einsatz. Sie basieren auf der Quantenteleportation und erlauben die schrittweise Übertragung verschränkter Zustände über große Entfernungen, indem sie Verschränkung „recyceln“/verlängern (Verschränkungsverstärkung).

- **Quantencomputer-Netzwerke:** Für die Vernetzung mehrerer Quantencomputer (z.B. zur Bildung von verteilten Quantenprozessoren) muss Quanteninformation zwischen entfernten Knoten ausgetauscht werden. Quantenteleportation ermöglicht diesen Transfer, ohne dass der ursprüngliche Zustand entlang des Übertragungsweges offengelegt oder zerstört wird.

- **Quantenkryptographie:** Auch für bestimmte kryptographische Protokolle kann Teleportation genutzt werden, um Kommunikation abhörsicher zu gestalten oder Schlüsselverteilung zu realisieren. Ein Beispiel ist die sogenannte *device-independent quantum key distribution* (DIQKD), bei der die Sicherheit auf dem Vorhandensein von Verschränkung und Teleportation beruht.

Literaturverzeichnis

[1] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical review letters, 70(13), 1895.

[2] Bouwmeester, D., Pan, J. W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A. (1997). Experimental quantum teleportation. Nature, 390(6660), 575-579.