11. Verschränkung, Nichtlokalität und Quantenkryptographie

11.1. Verschränkung

2-Teilchen-Hilbert-Raum (identische oder unterscheidbare Teilchen):

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$$

Entwicklung in Basiszustände:

$$|\psi\rangle = \sum_{n,m} c_{nm} |n\rangle_A \otimes |m\rangle_B$$

c_{nm}: Entwicklungskoeffizienten; $|n\rangle_A$: Basiszustände in A; $|m\rangle_B$: Basiszustände in B

Produktzustand:

Falls $c_{nm} = a_n b_m \Leftrightarrow |\psi\rangle = \left(\sum_n a_n |n\rangle_A\right) \otimes \left(\sum_m b_m |m\rangle_B\right) = |\phi\rangle_A \otimes |\chi\rangle_B$

$|\psi\rangle$ lässt sich als Produkt aus 1-Teilchen-Zuständen schreiben

Verschränkter Zustand:

$|\psi\rangle$ lässt sich <u>nicht</u> als Produkt aus 1-Teilchen-Zuständen schreiben

Beispiele (2 unterscheidbare Spin-$\frac{1}{2}$-Teilchen):

- Triplett-Zustände $|1,1\rangle = |\uparrow\rangle_A \otimes |\uparrow\rangle_B$ und $|1,-1\rangle = |\downarrow\rangle_A \otimes |\downarrow\rangle_B$ Produktzustände
- Triplett-Zustand $|1,0\rangle = |\uparrow\rangle_A \otimes |\downarrow\rangle_B + |\downarrow\rangle_A \otimes |\uparrow\rangle_B$ verschränkt
- Singulett-Zustand $|0,0\rangle = |\uparrow\rangle_A \otimes |\downarrow\rangle_B - |\downarrow\rangle_A \otimes |\uparrow\rangle_B$ verschränkt

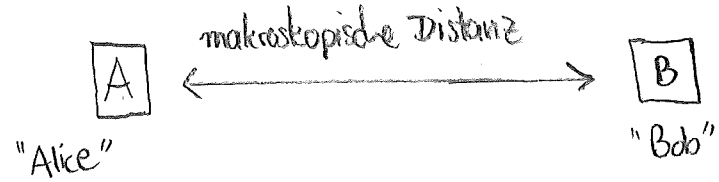
11.2. Nichtlokalität von Quantenkorrelationen – EPR

Gedankenexperiment von Einstein, Podolsky, Rosen ("EPR-Paradoxon", 1935):

Aufbau: 2 Spin-$\frac{1}{2}$-Teilchen im Singulett-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A \otimes |\downarrow\rangle_B - |\downarrow\rangle_A \otimes |\uparrow\rangle_B\right) \quad \text{(verschränkt!)}$$

Räumliche Trennung:



Erste Messung von $\hat{S}_{A,z}$ (Alice):

- Mögliche Messwerte: $+\frac{\hbar}{2}$, $-\frac{\hbar}{2}$
- Wahrscheinlichkeiten: $w(+\frac{\hbar}{2}) = w(-\frac{\hbar}{2}) = \frac{1}{2}$
- Annahme: Alice erhält $+\frac{\hbar}{2}$
- Kollaps der Wellenfunktion $|\psi\rangle \mapsto |\tilde{\psi}\rangle = |\uparrow\rangle_A \otimes |\downarrow\rangle_B$ (instantan!)

Direkte ausschließende Messung von $\hat{S}_{B,z}$ (Bob):

- Messwert $(-\frac{\hbar}{2})$ mit Wahrscheinlichkeit $w(-\frac{\hbar}{2}) = 1$ (!)

⇒ Verschränkung des Ausgangszustandes führt zu strikter Korrelation der Ergebnisse von nacheinander ausgeführten Messungen an weit entfernten Orten

Einstein: "spukhafte Fernwirkung ⇒ Unvollständigkeit der Quantenmechanik?"

Vorschlag zur experimentellen Überprüfung des Paradoxons (Bell, 1964):

Lokal-realistische Theorie wie von Einstein gefordert muss Bell'sche Ungleichungen erfüllen

Experimentelle Realisierung: z.B. Hensen et al., Nature 526, 682 (2015)

- Verschränktes Elektronenpaar in 1,3 km Entfernung
- Strikte Korrelation der Messergebnisse
- Verletzung der Bell'schen Ungleichungen
- Bestätigung der Vorhersagen der Quantentheorie

Schlussfolgerung:

Eine lokal-realistische "Vervollständigung" der Quantentheorie ist nicht möglich

Bemerkung:

Nichtlokalität der Quantenkorrelationen erlaubt keine (Überlichtschnelle) Informationsübertragung

11.3 Quantenkryptographie

Aufbau: Teilen von n ($n \gg 1$) Singulett-Paaren zwischen Alice und Bob

Singulett-Zustand:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A \otimes |\downarrow\rangle_B - |\downarrow\rangle_A \otimes |\uparrow\rangle_B \right)$$

$$= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle_A \otimes |\leftarrow\rangle_B - |\leftarrow\rangle_A \otimes |\rightarrow\rangle_B \right)$$

mit

$$\hat{S}_z|\uparrow\rangle = +\frac{\hbar}{2}|\uparrow\rangle \quad , \qquad \hat{S}_x|\rightarrow\rangle = +\frac{\hbar}{2}|\rightarrow\rangle$$
$$\hat{S}_z|\downarrow\rangle = -\frac{\hbar}{2}|\downarrow\rangle \quad , \qquad \hat{S}_x|\leftarrow\rangle = -\frac{\hbar}{2}|\leftarrow\rangle$$

Kryptographisches Protokoll:

1) Messung von $\hat{S}_{A,z}$ oder $\hat{S}_{A,x}$ (zufällig ausgewählt) an jedem Singulett, z.B.:

A: $+z, -x, +x, -z, -z, +x, \dots$

2) Anschließende Messung von $\hat{S}_{B,z}$ oder $\hat{S}_{B,x}$ (zufällig ausgewählt), z.B.:

B: $-z, +z, -x, +z, -x, +z, \dots$

3) Kommunikation über gewählte Messoperatoren über klassischen Kanal und Verwerfung von Einträgen, bei denen unterschiedliche Operatoren gemessen wurde, z.B.:

A: $\hat{S}_z, \cancel{\hat{S}_x}, \hat{S}_x, \hat{S}_z, \cancel{\hat{S}_z}, \cancel{\hat{S}_x}, \dots$

B: $\hat{S}_z, \cancel{\hat{S}_z}, \hat{S}_x, \hat{S}_z, \cancel{\hat{S}_x}, \cancel{\hat{S}_z}, \dots$

(4) Sicherheitskontrolle (Ausschluss eines Lauschangriffs): Kommunikation über einen (zufällig ausgewählten) Teil der Messergebnisse für gleiche Operatoren, um strikte Korrelation zu überprüfen, z.B.:

A: $+z, -x, +x, -z, -z, +x, \dots$

E: $-z, +x, -x, +x, +z, -x, \dots$ ("eavesdropper")

B: $-z, +z, -x, -z, -x, +z, \dots$

✓ ✓ ✗

(5) Verwendung des verbleibenden Teils der Messergebnisse für gleiche Operatoren als One-Time-Pad

Fazit: Mithilfe verschränkter Quantenzustände lassen sich geheime Schlüssel austauschen, bei denen durch Erhöhung der Anzahl von Kontrollsequenzen die Wahrscheinlichkeit, einen erfolgten Lauschangriff zu entdecken, beliebig gesteigert werden kann

Experimentelle Realisierung: z.B. Liao et al., Nature 549, 43 (2017)
Austausch von Quantenschlüssel über Distanz von 1200 km zwischen terrestrischem Observatorium bei Peking und Micius-Satellit in der Erdumlaufbahn