

SKRIPT: Quantenverschränkung - Informationen nicht schneller als das Licht (?) (Klasse Q)

Mathecamp 2026

1 Gegebenheit

- "Spooky action at a distance"
- Experiment: Richtung des Polarisations-Filters (z.B. Sonnenbrille)
 - Elektrisches Feld
 - Polarisator
 - Winkel Polarisator zu Licht-Polarisationsebene $\leftrightarrow$ Wahrscheinlichkeit, dass es durch kommt oder abgeblockt wird
- Experiment 2:
 - "Verschränkte" Photonen generieren
 - in unterschiedliche Richtungen fliegen lassen
 - Polarisation an beiden der verschränkten Teilchen messen
 - Nach dem Vergleich der Ergebnisse stellen wir fest: Bei den verschränkten Teilchen messen wir immer den gleichen Wert
- Warum ist das ein Problem?
 - Man stelle sich vor, man lässt die Teilchen **WEIT** auseinander fliegen (je eine halbe Lichtsekunde)
 - Jetzt dauert eine klassische Kommunikation zwischen den Messtellen 1 Sekunde
 - Aber sobald das eine Teilchen gemessen wird, muss es dem anderen Teilchen ja **SOFORT** kommunizieren, was das Ergebnis war (sonst würden die Messergebnisse nicht immer übereinstimmen)
- Erste Lösung: Versteckte Variablen
 - Einfacher Ansatz: Was, wenn die Teilchen sich schon vorher (bei ihrer Entstehung direkt an der gleichen Stelle) darüber geeinigt haben, wie sie alle Messungen beantworten werden
 - Modellierung (wir ersetzen die obere Variante einfach durch die untere)
 - * Kommunikation: $A(a, b) \quad B(b, a)$ (also die Teilchen kennen den Zustand des anderen Teilchen "momentan" (Gleichzeitigkeit ist an sich auch problematisch wegen der Relativitätstheorie, aber das ist nicht Thema für diesen Zirkel))
 - * "Einigung": $A(a, \lambda) \quad B(b, \lambda)$ (also die Funktionen der beiden Teilchen enthalten eine – von uns in unserem Teilchenmodell bislang nicht modellierte – versteckte Variable, die auf den gleichen Wert gesetzt wurde als das verschränkte Paar entstanden ist)
- Dilemma:
 - Es lässt sich zeigen (siehe dieser Zirkel), dass sich die Lösung des Problems durch versteckte Variablen ausschließen lässt
 - Generell, d.h. auch nicht "wir müssen noch die korrekte Modellierung finden" sondern "EGAL wie man es modellieren würde, so eine Abhängigkeit kann nicht bestehen"
- "Lösung" (und Konsequenzen): siehe Abschnitt am Ende

2 Basics: Matrizen und Qubit Manipulation (Rechenregeln)

- Matrix-Rechenregeln: 2x2
 - Generelles Aufschreiben
 - "Ausklammern" von Zahlen aus der ganzen Matrix
 - Addieren von Matrizen und Vektoren Komponentenweise
- Matrix-Rechenregeln: Matrix-Vektor

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad v = \begin{pmatrix} x \\ y \end{pmatrix}$$

$$Av = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \cdot x + b \cdot y \\ c \cdot x + d \cdot y \end{pmatrix}$$

- Matrix-Rechenregeln: Transponieren
 - Vektoren und Matrizen
 - Skalarprodukt und der Zusammenhang zum Ko-vektoriellen
- Rechenregeln komplexe Zahlen
 - $i^2 = -1$ (Wow amazing)
 - Komplexe Zahlen sind wie reelle Zahlen was Distributivität, Kommutativität und Assoziativität angeht
 - Komplexe Zahlen können in Matrix-Einträgen stehen
 - Komplexe Konjugation

$$(a + i \cdot b)^* = a - i \cdot b$$

3 Quantenmechanische Zustände

- Quantenmechanische Zustände
 - Bra (Kovektor) und Ket (Vektor)
- $$|\Psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad \langle\Psi| = (a^* \quad b^*)$$
- Transformation mit $\dagger$ ("Dagger") = Komplex-Konjugieren und Transponieren
- $$|\Psi\rangle^\dagger = \langle\Psi|$$
- Up/down bzw. 1/0

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Was ist eigentlich eine Phase
 - Bei Messungen bleibt immer ein Faktor $e^{i\varphi}$ unbekannt
 - Global ist dieser egal
 - Relativ zwischen Qubits ist der relevant!

3.1 Einige Notizen, Definitionen und Standards, (nicht alles besprochen oder notwendig)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Pauli-Matrix	Matrix	Linearkombination (Standard-Basisvektoren)	Linearkombination (Eigenvektoren)
$\sigma_1 = \sigma_x$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$ 0\rangle\langle 1 + 1\rangle\langle 0 $	$ +\rangle\langle + - -\rangle\langle - $
$\sigma_2 = \sigma_y$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$i(1\rangle\langle 0 - 0\rangle\langle 1)$	$ \phi^+\rangle\langle \phi^+ - \phi^-\rangle\langle \phi^- $
$\sigma_3 = \sigma_z$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$ 0\rangle\langle 0 - 1\rangle\langle 1 $	$ 0\rangle\langle 0 - 1\rangle\langle 1 $

(Die verwendeten Vektoren sind wie folgt definiert, wobei die verwendeten Kets durch Vektoren des $\mathbb{C}^2$ dargestellt werden)

$$\begin{aligned}
 |0\rangle &= |s_{z,+}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} & |1\rangle &= |s_{z,-}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
 |+\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} & |-\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
 |\phi^+\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} & |\phi^-\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}
 \end{aligned}$$

4 Tensorprodukt

- "Ineinander-Schreiben"
- Führt zu: einfach als Koeffizienten-Produkt schreiben
- Mögliche Zweiqubit-Basiszustände

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle$$

- Dann

$$|00\rangle = |0\rangle \otimes |0\rangle$$

- Und man kann das Tensorprodukt zunächst schlicht als Rechenregel einführen:

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$

- Daraus (macht Sinn, folgt aber auch, wenn komplett mit vorherigen Definitionen als Vektoren geschrieben und Regeln angewendet)

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

4.1 Die vier Bell-Zustände sind

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

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

5 Messung

- "Hinmultiplizieren" vom entsprechend ge-daggetem Zustand von links, quadriert
- Beispiel

– Dieser Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

– Messung in der 0/1-Basis

$$P(0) = \frac{1}{2}, \quad P(1) = \frac{1}{2}$$

– Rechne nach (mit den auch aus den vorherigen Regeln ableitbaren Zwischenergebnissen)

- * $\langle 0| \cdot |0\rangle = \langle 0|0\rangle = 1$
- * $\langle 1|1\rangle = 1$
- * $\langle 0|1\rangle = 0$
- * $\langle 1|0\rangle = 0$

- Also

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \text{und} \quad \langle\psi| = (\alpha^* \ \beta^*)$$

$\langle\phi|\psi\rangle$ = ist einfach das komplexe Skalarprodukt

- Zentrale Formel: die Wahrscheinlichkeit, bei einer Messung im Zustand $|\phi\rangle$ dieses Ergebnis (ϕ) zu bekommen

$$P(\phi) = |\langle\phi|\psi\rangle|^2$$

- (Funktioniert auch für die Zustände mit komplexen Zahlen – Dazu benötigt man die korrekte komplexe Konjugation)
- Verschränkung: Zustände sind NICHT separierbar
 - Als Beispiel für einen separierbaren Zustand (keine echte Verschränkung)

$$|\psi\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

– Aber ist das dann nicht klar, dass ein Zustand von zwei Teilchen immer aus den Zuständen der zwei Teilchen besteht???

– Dagegen:

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

– Kann man diesen Zustand "zerlegt" schreiben? (also so):

$$|\psi\rangle_A \otimes |\phi\rangle_B$$

– Versuche es!

- Beweis, dass dies unmöglich ist:

– Setze

$$|\psi\rangle_A = a|0\rangle + b|1\rangle$$

$$|\phi\rangle_B = c|0\rangle + d|1\rangle$$

– Dann wäre

$$|\psi\rangle_A \otimes |\phi\rangle_B = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

– Wir benötigen aber

$$ac = \frac{1}{\sqrt{2}}, \quad ad = 0, \quad bc = 0, \quad bd = \frac{1}{\sqrt{2}}$$

– Und daraus folgt sofort ein Widerspruch

* $ac \neq 0$, also $a, c \neq 0$

* $ad = 0$, also $d = 0$

* aber dann $bd = 0$, obwohl $bd = 1/\sqrt{2}$ sein müsste

- Welche Zustände haben diese Eigenschaften

– Bell Zustände (Bell-States)

– Waren vorher schon zu sehen

– Messen am Bell state: Korrelation

- Jetzt ein konkretes Beispiel für die verteilte Messung

– Zustand:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

– Wenn Alice misst

* Alice bekommt 0 $\rightarrow$ Bob bekommt sicher 0

* Alice bekommt 1 $\rightarrow$ Bob bekommt sicher 1

– Aber Alice bekommt zufällig 0 oder 1 (Und genauso für Bob)

$$P(A = 0) = P(A = 1) = \frac{1}{2}.$$

- Die einzelnen Ergebnisse sind zufällig.

Die gemeinsamen Ergebnisse sind hochgradig korreliert.

6 Erste Intuition: Hidden Variables

- Was, wenn nicht einfach jedes Paar bei der Verschränkung schon Regeln hat / zugewiesen bekommt wie sich das andere verhalten wird
- "Du bist das vertikal polarisierte Teilchen bei 45°" etc.

6.1 Wir widerlegen WAS wenn wir Hidden Variables widerlegen?

- die Kombination aus
 - Realismus / vorgegebenen Ergebnissen
 - Lokalität
- "Das Teilchen von Alice darf nicht davon abhängen, welche Messung Bob in diesem Moment auswählt"

- Es gibt eine verborgene Variable

$$\lambda$$

- Alice wählt Messrichtung a , Bob b . Dann liefern die Teilchen:

$$A(a, \lambda) \in \{-1, +1\}, \quad B(b, \lambda) \in \{-1, +1\}.$$

- Lokalität bedeutet

$$A = A(a, \lambda)$$

- und NICHT

$$A = A(a, b, \lambda').$$

7 CHSH Ungleichung (Clauser-Horne-Shimony-Holt)

- Angenommen, wir fixieren das System auf ein bestimmtes λ
- dann machen wir viele Experimente mit verschiedenen Messkombinationen a oder a' und b oder b'
- z.B. (vergleiche mit später)

$$\begin{aligned} a : \quad \theta_a &= 0^\circ, & a' : \theta_{a'} &= 45^\circ \\ b : \quad \theta_b &= 22.5^\circ, & b' : \theta_{b'} &= -22.5^\circ \end{aligned}$$

- Alice hat zwei mögliche Einstellungen

$$a, \quad a'$$

- Bob ebenfalls (Jedes Ergebnis ist ± 1)

$$b, \quad b'$$

- Betrachte für ein bestimmtes (beliebiges aber unbekanntes) λ

- Folgende "Zufallsvariable" (Zufallsvariablen und deren Erwartungswert wie in der Schule. Beispiel über das zuweisen von Würfel-Ergebnissen zu "gewünschten" und "ungewünschten" Fällen. Hier nicht im Detail ausgeführt.)

$$S = A(a)B(b) + A(a)B(b') + A(a')B(b) - A(a')B(b')$$

- Jetzt gruppieren

$$S = A(a) [B(b) + B(b')] + A(a') [B(b) - B(b')]$$

- Beobachte:

$$B(b), B(b') \in \{-1, +1\}$$

- * Entweder:

$$B(b) + B(b') = \pm 2 \quad \text{und} \quad B(b) - B(b') = 0$$

- * Oder umgekehrt

$$B(b) + B(b') = 0 \quad \text{und} \quad B(b) - B(b') = \pm 2$$

- Und weil $|A| = 1$, gilt für *jede* einzelne verborgene Variable

$$|S| = 2$$

- Beim Mitteln (Erwartungswert bilden) über viele Versuche (unterschiedliche λ) folgt (Erwartungswert ist eine lineare Funktion, daher ist diese Notation möglich):

$$\boxed{|E(a, b) + E(a, b') + E(a', b) - E(a', b')| \leq 2}$$

Das ist die **CHSH-Ungleichung**

8 Contra Argument: Was sagt die Quantenmechanik

- Jetzt machen wir für einen bestimmten eingesetzten Wert/eine Beobachtung eine Rechnung die das ganze widerlegt
- Wir nehmen den Bell-Zustand (Das ist der sogenannte Singulettzustand)

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Für Messungen entlang zweier Richtungen a, b sagt die Quantenmechanik für geeignete Polarisations-/Spin-Messungen:

$$E(a, b) = -\cos(\theta_a - \theta_b)$$

- Mache eine konkrete Rechnung. Wähle:

$$\begin{aligned} a : \quad \theta_a &= 0^\circ, & a' : \theta_{a'} &= 45^\circ \\ b : \quad \theta_b &= 22.5^\circ, & b' : \theta_{b'} &= -22.5^\circ \end{aligned}$$

- Dann

$$E(a, b) = -\cos(22.5^\circ)$$

$$E(a, b') = -\cos(22.5^\circ)$$

$$E(a', b) = -\cos(22.5^\circ)$$

$$E(a', b') = -\cos(67.5^\circ)$$

- Einsetzen ($S = E(a, b) + E(a, b') + E(a', b) - E(a', b')$)

$$S = -3\cos(22.5^\circ) + \cos(67.5^\circ)$$

$$|S| = 2\sqrt{2} > 2$$

- Das widerspricht allerdings der **CHSH-Ungleichung**

$$|S| = |E(a, b) + E(a, b') + E(a', b) - E(a', b')| = \begin{cases} \text{CHSH:} & \leq 2 \\ \text{QM-Beispiel:} & > 2 \end{cases}$$

- Das Ergebnis aus der Quantenmechanik lässt sich auch experimentell bestätigen. Also ist dies unumstößlich. Also haben wir hier einen Fehler in unserer Modellierung.
Wenn man jetzt genau überlegt, dann waren die Argumente alle Rechnungen mit dem Erwartungswert. Die Statistik ist hier im Prinzip als sicher anzusehen.
Wir haben allerdings für die Umformungen eine Annahme gemacht: Dass die Ereignisse in unabhängige A und B Teile zerfallen – Weil wir die zusammenhängende Formulierung dank der versteckten Variable auftrennen konnten – Dies MUSS also eine falsche Annahme gewesen sein.
(Die komplette Tatsache mit einer beliebigen Formulierung. Also auch nicht, dass wir die Formulierung vielleicht noch nicht entdeckt haben)
- "Das Problem kann NICHT durch irgendeine Theorie mit versteckten Variablen gelöst werden"

9 Extra: Warum cosinus aus der Quantenmechanik

- Woher bekommt man cosinus? (Tatsache dass $\cos^2 + \sin^2 = 1$ passt zu schon gesehenen Normierungsbedingungen)
- Für einen einzelnen Qubit-Zustand und einen Messzustand (die Komponenten des elektrischen Feldes haben "einen Winkel am Einheitskreis") – Das gibt uns eine Intuition, aber nicht genau den cosinus

$$\begin{aligned} &|0\rangle \\ |\theta\rangle &= \cos\theta |0\rangle + \sin\theta |1\rangle \\ \langle\theta|0\rangle &= \cos\theta \\ P(\theta) &= |\langle\theta|0\rangle|^2 = \cos^2\theta \end{aligned}$$

- Wir haben zunächst

$$|0\rangle, \quad |1\rangle$$

Eine Messrichtung mit Winkel θ definieren wir durch die beiden orthogonalen Zustände

$$\begin{aligned} |+\theta\rangle &= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \\ |-\theta\rangle &= -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \end{aligned}$$

(Das $\theta/2$ ist spezifisch für das Spin- $\frac{1}{2}$ -Modell)

- Die beiden Ergebnisse nennen wir

$$+1, \quad -1$$

- Wir haben die den Bell-Zustand

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Alice misst in Richtung a , Bob in Richtung b .
Wir wollen wissen: Wie wahrscheinlich sind die verschiedenen Kombinationen von Ergebnissen?

$$(+, +), \quad (+, -), \quad (-, +), \quad (-, -)$$

- Betrachte zunächst die Wahrscheinlichkeit, dass beide $+$ bekommen:

$$P(++ | \theta_a, \theta_b)$$

- Die Amplitude dafür ist einfach das Skalarprodukt

$$\langle +a, +b | \Psi^- \rangle$$

- Jetzt setzen wir den Bell-Zustand ein:

$$= \frac{1}{\sqrt{2}} (\langle +a|0\rangle \langle +b|1\rangle - \langle +a|1\rangle \langle +b|0\rangle)$$

- Aus unseren Definitionen

$$\begin{aligned} \langle +a|0\rangle &= \cos\frac{a}{2} \\ \langle +a|1\rangle &= \sin\frac{a}{2} \end{aligned}$$

- Also

$$\begin{aligned} \langle +a, +b | \Psi^- \rangle &= \frac{1}{\sqrt{2}} \left(\cos\frac{a}{2} \sin\frac{b}{2} - \sin\frac{a}{2} \cos\frac{b}{2} \right) \\ &= \frac{1}{\sqrt{2}} \sin\left(\frac{b}{2} - \frac{a}{2}\right) \\ &= -\frac{1}{\sqrt{2}} \sin\frac{a-b}{2} \end{aligned}$$

- Jetzt quadrieren wir den Betrag

$$P(++ | a, b) = \frac{1}{2} \sin^2 \frac{a-b}{2}$$

- Es lässt sich nachrechnen, dass

$$P(++) = P(--) = \frac{1}{2} \sin^2 \frac{a-b}{2}$$

$$P(+ -) = P(- +) = \frac{1}{2} \cos^2 \frac{a-b}{2}$$

- Der Erwartungswert ist nur oben zu unabhängigen A und B zerfallen, da wir die versteckten Variablen (fälschlicherweise) angenommen hatten.

- Hier bleibt es ein Term (wir können das Produkt nicht aus dem Erwartungswert ziehen).

$$E(a, b) = \langle AB \rangle$$

- Da $A, B = \pm 1$ gilt

* gleiche Ergebnisse $\rightarrow AB = +1$

* verschiedene Ergebnisse $\rightarrow AB = -1$

- Also sortiert:

$$E = P(\text{gleich}) - P(\text{verschieden})$$

$$E = 2 \cdot \frac{1}{2} \sin^2 \frac{a-b}{2} - 2 \cdot \frac{1}{2} \cos^2 \frac{a-b}{2}$$

- das sich offensichtlich kürzen lässt:

$$E = \sin^2 \frac{a-b}{2} - \cos^2 \frac{a-b}{2}$$

- Und jetzt benutzen wir diese trigonometrische Identität

$$\cos \Delta = \cos^2 \frac{\Delta}{2} - \sin^2 \frac{\Delta}{2}$$

- Und erhalten damit für das Spin- $\frac{1}{2}$ -Modell

$$E(a, b) = -\cos(a-b)$$

10 Interpretation

- Man könnte nach Bell zunächst denken

Wenn Alice ihre Messrichtung ändert, ändert sie doch sofort Bobs Ergebnis!

- Aber: Nein. Also ja, aber nicht dass Bob das so sehen würde – Nur Alice
- Für Bob ist das Ergebnis immer zufällig – Egal, was Alice tut

$$|\Psi^-\rangle : \quad P(B = +1) = P(B = -1) = \frac{1}{2}$$

- Alice kann also nicht entscheiden

Ich möchte Bob eine 1 schicken, also erzwinge ich bei mir Ergebnis +1.

Das kann sie nicht – Für sie ist das Ergebnis AUCH zufällig

- Bob sieht lokal immer eine zufällige Folge

+ - + + - - + ...

- Erst wenn Alice und Bob ihre Daten später klassisch vergleichen, erkennen sie

"Wow – unsere Zufallszahlen sind auf eine Weise korreliert, die keine lokale Hidden-Variable-Theorie erklären kann."

11 Warum können wir jetzt damit keine überlicht-schnelle Kommunikation erlangen?

- Zentraler Unterschied

Nichtlokale Korrelationen $\neq$ überlichtschnelle Kommunikation
--

- Socken-Analogie

- Stellt euch vor, ihr habt zwei identische Socken. Eine gebt ihr eurem Freund.
- Dann geht ihr beide nach Hause.
- Irgendwann zwischen 10:00 und 10:30 zieht ihr eine Socke auf den linken Fuß. Dadurch wird die Socke in den Händen eures Freundes sofort zur rechten Socke.
- Allerdings weiß das euer Freund nicht. Und er weiß auch nicht wann im Intervall das passiert ist.
- Er kann sich um 10:30 die Socke auf den rechten oder den linken Fuß ziehen. Aber ob er korrekt oder inkorrekt angezogen hat, das wird er erst merken, wenn ihr euch klassisch das nächste Mal trifft und er tatsächlich sieht was ihr gemacht habt. Euer Freund bekommt die Information also genauso schnell, ob er jetzt eine der Socken hat, oder aber nicht.

- (Das Beispiel erhält die Eigenschaft nicht, dass man sich sicher sein kann, dass die Ergebnisse identisch sind – das ist dann doch den Zaubern der Quantenwelt vorbehalten – aber es macht hoffentlich klar, warum keine nutzbare Information über z.B. den Messzeitpunkt ausgetauscht wird)

- Könnte man das zufällige Ergebnis nicht beeinflussen, aber herausfinden wann die Messung der anderen Partei passierte, könnte man auch Information übertragen
- Man könnte einfach vereinbaren "wenn ich dir eine 1 schicken will, Messe ich zu einer Geraden Sekunde, wenn ich eine 0 schicken will, messe ich zu einer ungeraden Sekunde"

- Und warum kann man keine Information aus der Gleichheit der Messung ziehen?

- Weil die Messungen im Bereich in dem die Ergebnisse nicht vorhersagbar sind **zufällig** sind
- Ich kann etwas tun, um den Zustand des Teilchens zu verändern – Aber ich kann es *nicht beeinflussen* ob es sich zu 1 oder 0 verändert – das ist zufällig
- Und damit scheint es auch für den anderen immer zufällig – er kann nicht unterscheiden, ob es 1 wird, weil "der Partner auch 1 gemessen hat" oder "ich der Partner bin der den Zufall aufgelöst hat"

- Nützlich oder kompletter unnötig?

- Man kann damit erreichen, dass wenn man zwei Parteien ein paar verschränkte Teilchen gibt (diese kann man maximal mit Lichtgeschwindigkeit transportieren – also gleiche Geschwindigkeit wie klassische Kommunikation), dann haben sie bei Messung sicher die **gleichen zufälligen Zahlen**
- Das ist genau das, was man für einen geteilten geheimen Schlüssel für symmetrische Verschlüsselung benötigt
- Hat angenehme Nebeneffekte wie Manipulations- und Abhörsicherheit (Man in the Middle) ein Stück weit eingebaut, da man einen Quantenzustand nicht kopieren kann und ihn nicht lesen, ohne ihn zu kollabieren – also kann nicht noch eine dritte Partei die gleiche Zufallszahl erlangen