EPR paradox, Bell inequality, etc.

Compatible and incompatible observables

$[A, B] = 0$, then compatible, can measure simultaneously, can diagonalize in one basis

commutator, $[A, B] \equiv AB - BA$

If we project a state onto an eigensubspace of A, and then project the result onto an eigensubspace of B, the resulting state is still in the same eigensubspace of A.

$[A, B] \neq 0$, then incompatible, cannot be measured simultaneously

Example: $[\sigma_x, \sigma_y] = 2i\sigma_z \neq 0$

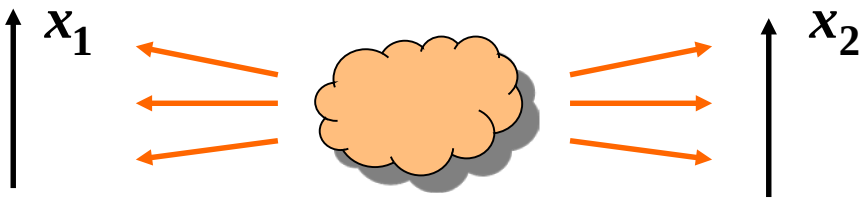
If we measure x-component of a spin ½, and then y-component, we destroy x-component

Another (usual) example in QM: $[\hat{p}, \hat{x}] = -i\hbar$, cannot simultaneously know position and momentum

Uncertainty principle: $\sigma_A^2 \sigma_B^2 \geq \left(\frac{1}{2i}\langle [A, B] \rangle\right)^2$

Not quite useful for σ_x and σ_y, but for $\hat{x}$ and $\hat{p}$ gives $\sigma_x^2 \sigma_p^2 \geq (\hbar/2)^2$
(Heisenberg uncertainty principle)

EPR paper (Einstein, Podolsky, Rosen, Phys. Rev., 1935)



$$\psi(x_1, x_2) = \int_{-\infty}^{\infty} \exp[(i/\hbar)(x_1 - x_2)\, p]\, dp = 2\pi\hbar\, \delta(x_1 - x_2)$$

Entangled state, $x_1 = x_2, p_1 = -p_2$ ($e^{ix_1 p/\hbar}$ means $p_1 = p$, $e^{-ix_2 p/\hbar}$ means $p_2 = -p$)

A person at the left can choose whether to measure x or p, which makes the second particle to have a well-defined x or a well-defined p. This seems impossible because of causality.

EPR: "spooky action at a distance" $\Rightarrow$ QM is an incomplete theory

A lot of philosophy

EPR In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system.

Bohr's reply (Phys. Rev., 1935)

It is shown that a certain "criterion of physical reality" formulated … by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena.

(crudely: do not try to understand QM, just use it)

Further developments of EPR paradox

Modified setup (David Bohm, 1950s)

Two separated spin-1/2 particles in spin-zero state (singlet, "Bell state")

$$|\psi\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Particles are far apart

If measure 0 for one qubit $\Rightarrow$ get 1 for the other qubit

Seems similar to classical correlation, but the key is that we can measure spin along any direction, so a person can choose a measurement direction, and this direction is passed to the second qubit faster than light. Compared to EPR (choice of either x or p), more freedom in the choice (continuous variable).

"Hidden variable" theory: some realistic parameters, not captured by QM

Using Bohm's setup, it is possible to distinguish QM predictions from predictions of *any* (local) hidden variable theory (find if something really propagates faster than light or not).

John Bell, 1964: Bell inequality, satisfied by any (local) hidden variable theory, but violated by quantum mechanics

CHSH, 1969 (Clauser, Horne, Shimony, Holt): similar inequality, suitable for experiments

Aspect, 1982: first convincing experiment, showing violation of CHSH inequality (nowadays a routing procedure for optical calibration in QC expts.)

Rotational independence of spin-zero (Bell) state

$$|\psi\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Instead of rotating the measurement axis, let us rotate qubits

Theorem: $(U \otimes U)\,\dfrac{|01\rangle - |10\rangle}{\sqrt{2}} = \dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$ for any unitary U (up to a phase factor)

Proof (explicit)

$$U = e^{i\varphi}\begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} \qquad |a|^2 + |b|^2 = 1$$

Phase φ is not important, neglect

$$|0\rangle \xrightarrow{U} a|0\rangle + b|1\rangle$$
$$|1\rangle \xrightarrow{U} -b^*|0\rangle + a^*|1\rangle$$

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \xrightarrow{U \otimes U} \frac{(a|0\rangle + b|1\rangle)(-b^*|0\rangle + a^*|1\rangle) - (-b^*|0\rangle + a^*|1\rangle)(a|0\rangle + b|1\rangle)}{\sqrt{2}}$$

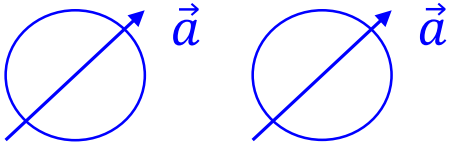
$$= \frac{|00\rangle(-ab^* + b^*a) + |01\rangle(aa^* + b^*b) + |10\rangle(-bb^* - a^*a) + |11\rangle(ba^* - a^*b)}{\sqrt{2}}$$

$$= \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

QED

Bell inequality

$$|\psi\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}$$



QM: if measure along <u>any</u> direction $\vec{a}$, then only result "$+\,-$" or "$-\,+$"

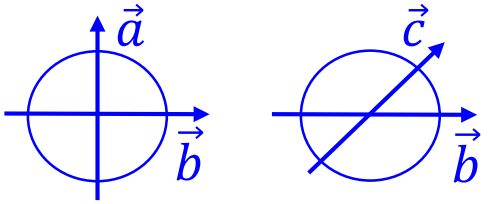
Theorem If $P_{\vec{a},\vec{a}}(+-) + P_{\vec{a},\vec{a}}(-+) = 1$ for any measurement direction $\vec{a}$, then in <u>*any*</u> (local) hidden variable theory (i.e., a realistic theory without faster-than-light interactions) the following inequality holds:

$$\left|E\left(\vec{a},\vec{b}\right) - E(\vec{a},\vec{c})\right| \le 1 + E\left(\vec{b},\vec{c}\right)$$

where $E\left(\vec{a},\vec{b}\right) \equiv P_{\vec{a},\vec{b}}(++) + P_{\vec{a},\vec{b}}(--) - P_{\vec{a},\vec{b}}(+-) - P_{\vec{a},\vec{b}}(-+)$ (correlator)

Rather simple proof (we will not discuss). General idea: if somebody (God) knows that results for $\vec{a},\vec{b}$ and $\vec{a},\vec{c}$ <u>would be</u> $\pm+$ and $\pm+$, then for $\vec{b},\vec{c}$ it must be $-+$; similar for other combinations.

However, QM predicts violation of this inequality, for example for the directions



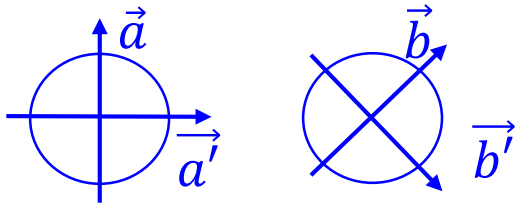
Easy to see: in QM, $E = -\cos\theta_{\vec{a},\vec{b}}$, so in this example it would be

$|-\cos 90^\circ + \cos 45^\circ| \le 1 - \cos 45^\circ$, which is $\sqrt{2}/2 \le 1 - \sqrt{2}/2$, which is wrong

Therefore, QM prediction contradicts <u>any</u> realistic theory, can distinguish (not a philosophy)

Caveat: Bell inequality needs assumption of <u>perfect</u> anticorrelation for the same $\vec{a}$ (not possible in an experiment)

CHSH inequality (often still called Bell inequality)



Any two-party system, with measurement results + or −, four pairs of meas. directions

As in the Bell inequality, define the correlator

$$E\left(\vec{a},\vec{b}\right) \equiv P_{\vec{a},\vec{b}}(++) + P_{\vec{a},\vec{b}}(--) - P_{\vec{a},\vec{b}}(+-) - P_{\vec{a},\vec{b}}(-+)$$

and then define the combination $S \equiv E\left(\vec{a},\vec{b}\right) - E\left(\vec{a},\vec{b'}\right) + E\left(\vec{a'},\vec{b}\right) + E\left(\vec{a'},\vec{b'}\right)$

Theorem: In a realistic hidden-variable theory $|S| \leq 2$

Proof Consider a deterministic theory, in which the measurement results for any measurement directions are fully determined by a single parameter λ (possibly multidimensional). (Classical probability can be included by averaging over λ.)

Table

sets	$\vec{a}$	$\vec{a'}$	$\vec{b}$	$\vec{b'}$
λ_1	+	+	+	+
λ_2	+	+	+	−
λ_3	+	+	−	+
…	…	…	…	…
λ_{16}	−	−	−	−

Idea that choice of directions $\vec{a}$ or $\vec{a'}$ cannot affect result for the second qubit (and vice versa)

Instead of averaging over measurements, let us calculate S for each row (set of λ), and then average over λ

$E = 1$ if the same signs in two columns, $E = -1$ if different

λ_1: $S = +1 - (+1) + 1 + 1 = 2$

λ_2: $S = +1 - (-1) + 1 + (-1) = 2$

CHSH inequality (cont.)

$$E\left(\vec{a},\vec{b}\right) \equiv P_{\vec{a},\vec{b}}(++) + P_{\vec{a},\vec{b}}(--) - P_{\vec{a},\vec{b}}(+-) - P_{\vec{a},\vec{b}}(-+)$$

$$S \equiv E\left(\vec{a},\vec{b}\right) - E\left(\vec{a},\overrightarrow{b'}\right) + E\left(\overrightarrow{a'},\vec{b}\right) + E\left(\overrightarrow{a'},\overrightarrow{b'}\right)$$

Need to show $|S| \leq 2$

Table

sets	$\vec{a}$	$\overrightarrow{a'}$	$\vec{b}$	$\overrightarrow{b'}$
λ_1	+	+	+	+
λ_2	+	+	+	−
λ_3	+	+	−	+
…	…	…	…	…
λ_{16}	−	−	−	−

$E = 1$ if the same signs in two columns, $E = -1$ if different

λ_1: $S = +1 - (+1) + 1 + 1 = 2$

λ_2: $S = +1 - (-1) + 1 + (-1) = 2$

λ_3: $S = -1 - (+1) + (-1) + 1 = -2$

Can check that $S = \pm 2$ in all 16 rows

Four E-numbers in S are ± 1, with the product of these 4 numbers equal to $+1$. Therefore even number of $+1$s and -1s. All $+1$, then $S = 2$, all -1, then $S = -2$, two $+1$ and two -1, then $S = \pm 2$.

Since $S = \pm 2$ in all rows, averaging over λ gives $|S| \leq 2$.

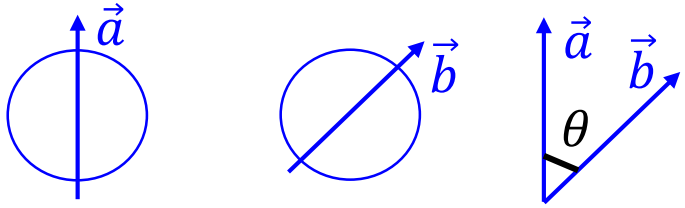
CHSH inequality (cont.)

$$E\left(\vec{a},\vec{b}\right) \equiv P_{\vec{a},\vec{b}}(++) + P_{\vec{a},\vec{b}}(--) - P_{\vec{a},\vec{b}}(+-) - P_{\vec{a},\vec{b}}(-+)$$

$$S \equiv E\left(\vec{a},\vec{b}\right) - E\left(\vec{a},\vec{b'}\right) + E\left(\vec{a'},\vec{b}\right) + E\left(\vec{a'},\vec{b'}\right)$$

We have proven that in any hidden-variable theory $|S| \leq 2$

Now QM prediction

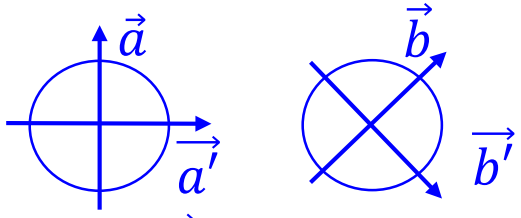


$$|\psi\rangle = \frac{|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle}{\sqrt{2}}$$

Then $E = -\cos\theta$

If result "+" for measurement along $\vec{a}$, then the second qubit becomes along $-\vec{a}$. Then its measurement along $\vec{b}$ gives "+" with probability $\sin^2(\theta/2)$ and "−" with probability $\cos^2(\theta/2)$, so correlator is $E = \sin^2(\theta/2) - \cos^2(\theta/2) = -\cos\theta$. Similarly, if result "−" along $\vec{a}$, then second result "−" with probability $\sin^2(\theta/2)$ and "+" with probability $\cos^2(\theta/2)$, so again $\boldsymbol{E = -\cos\theta}$.

Choose

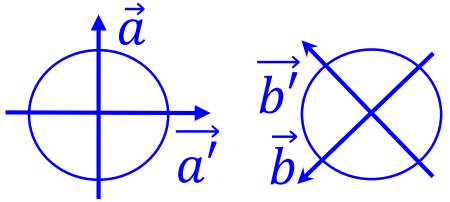


Then

$$S = -\left[\frac{\sqrt{2}}{2} - \left(-\frac{\sqrt{2}}{2}\right) + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\right] = -2\sqrt{2}$$

Violation: $2\sqrt{2}$ instead of 2

If choose



then

$$S = -\left[-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\right] = 2\sqrt{2}$$

Causality paradox

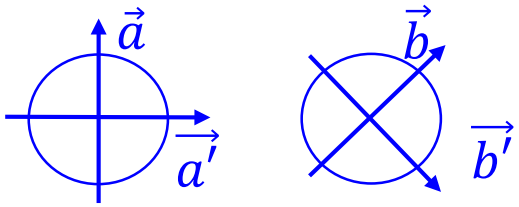
So, the CHSH (Bell) inequality is violated (repeatedly confirmed experimentally). What does this mean?

Yes, collapse propagates faster than light. Yes, spooky action at a distance.

> What about relativity? Can we pass information into the past (via a friend on a train moving away)?

No, we cannot transmit our own (classical) information into the past (only "useless" quantum information can be sent to the past).

Why? Randomness saves causality.



We can pass the chosen direction faster than light (therefore back in time), but we cannot control if the spin will be parallel or antiparallel.

Useless without cloning ($\rho = \hat{1}/2$) (with cloning, can learn about the direction with two measurements)

Experimental violations of Bell (CHSH) inequality: 1970s, 1980s (first convincing experiment with photons in 1982, Aspect et al.). Now a routine procedure to calibrate states in QC algorithms.

Bell states (EPR states, EPR pairs, etc.)

In QC the following four "Bell states" are most widely used:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Phi_+\rangle$$

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi_+\rangle$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\Phi_-\rangle$$

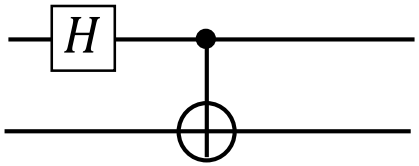
$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad |\Psi_-\rangle$$

All these states are similar to the singlet state.

Form orthonormal basis in 2-qubit Hilbert space (called "Bell basis")

The Bell states are maximum-entangled (measures of 2-qubit entanglement: concurrence, entanglement of formation, etc.)

Production of the Bell states



N-C book

$$|00\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{\text{CNOT}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Phi_+\rangle \qquad |\beta_{00}\rangle$$

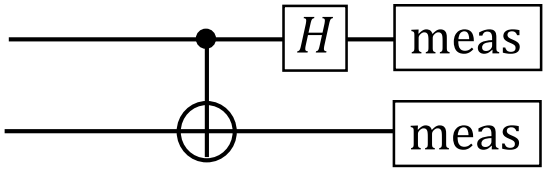
$$|01\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{\text{CNOT}} \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi_+\rangle \qquad |\beta_{01}\rangle$$

$$|10\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{\text{CNOT}} \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\Phi_-\rangle \qquad |\beta_{10}\rangle$$

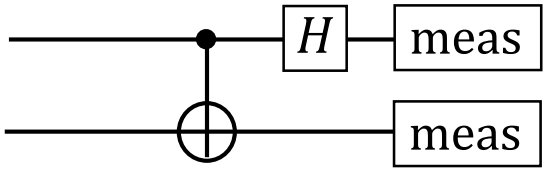
$$|11\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{\text{CNOT}} \frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad |\Psi_-\rangle \qquad |\beta_{11}\rangle$$

Unitary transformation from computational basis to Bell basis

Measurement in the Bell basis:
just the reverse



Measurement in the Bell basis



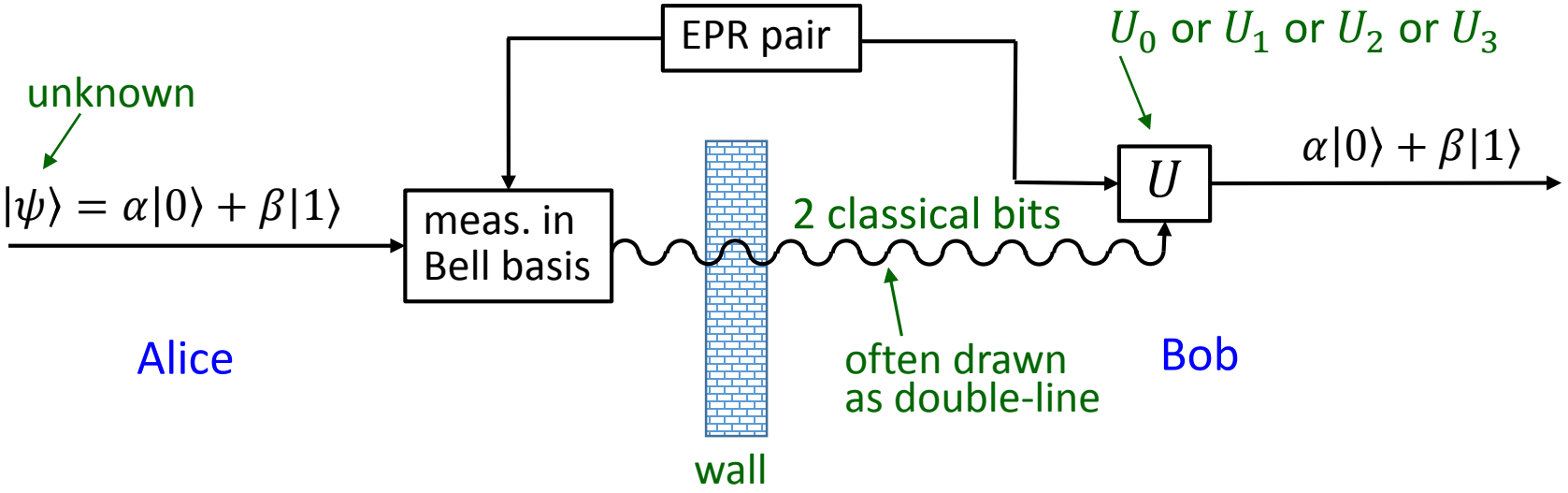
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{H} |00\rangle$$

$$\frac{|01\rangle + |10\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|01\rangle + |11\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{H} |01\rangle$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle - |10\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{H} |10\rangle$$

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|01\rangle - |11\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{H} |11\rangle$$

Quantum teleportation



Goal: transfer a qubit through a "wall" by sending only 2 classical bits over phone/radio (also need a Bell pair, shared by Alice and Bob)

Surprise! We can transfer continuous numbers α and β (infinite amount of classical information) by using only 2 classical bits (and shared EPR pair)

1 qubit $\leq$ 1 ebit +2 bits (ebit is a shared EPR pair)

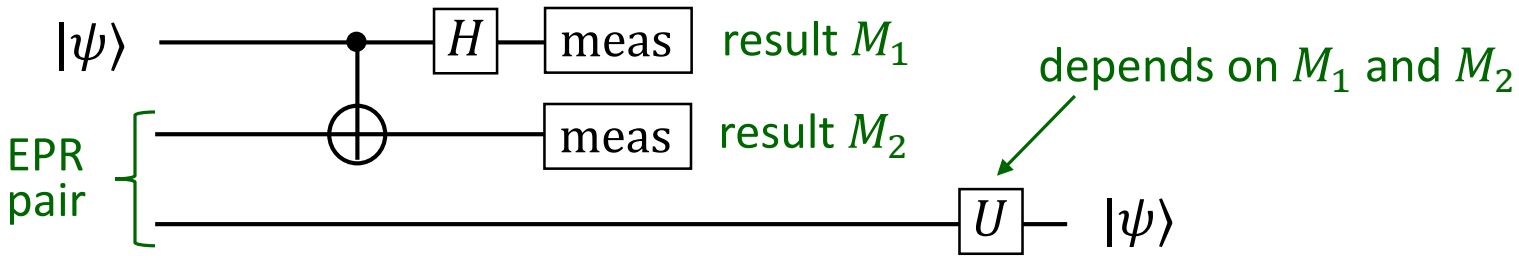
Not a cloning, we destroy initial state and recreate it in a different place (teleportation)

Slower than light (needs a phone call)

Possible interpretation: EPR pair travels back in time

First realized in 1997 (143 km in 2012).

Quantum teleportation: quantum circuit diagram



Let us use $|\Phi_+\rangle$ for the EPR pair. Let us see what happens after measurement.

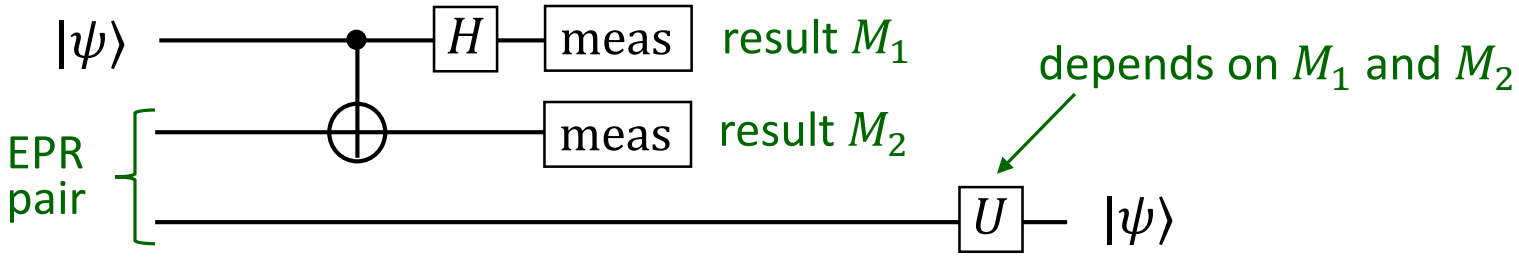
$$(\alpha|0\rangle + \beta|1\rangle)\ \frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}} \xrightarrow{H}$$

$$\xrightarrow{H} \alpha\ \frac{|0\rangle + |1\rangle}{\sqrt{2}}\ \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta\ \frac{|0\rangle - |1\rangle}{\sqrt{2}}\ \frac{|10\rangle + |01\rangle}{\sqrt{2}} =$$

$$= \frac{|00\rangle\ (\alpha|0\rangle + \beta|1\rangle)}{2} + \frac{|01\rangle\ (\alpha|1\rangle + \beta|0\rangle)}{2} + \frac{|10\rangle\ (\alpha|0\rangle - \beta|1\rangle)}{2} + \frac{|11\rangle\ (\alpha|1\rangle - \beta|0\rangle)}{2}$$

Measure first two qubits, get $00, 01, 10, 11$ with probability $1/4$ each,
in each case the third qubit state is very similar to the original state,
use unitary operation U to make it exactly the original state

Quantum teleportation (cont.)



$$(\alpha|0\rangle + \beta|1\rangle)\ \frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}} \xrightarrow{H}$$

$$\xrightarrow{H} \frac{|00\rangle\,(\alpha|0\rangle + \beta|1\rangle)}{2} + \frac{|01\rangle\,(\alpha|1\rangle + \beta|0\rangle)}{2} + \frac{|10\rangle\,(\alpha|0\rangle - \beta|1\rangle)}{2} + \frac{|11\rangle\,(\alpha|1\rangle - \beta|0\rangle)}{2}$$

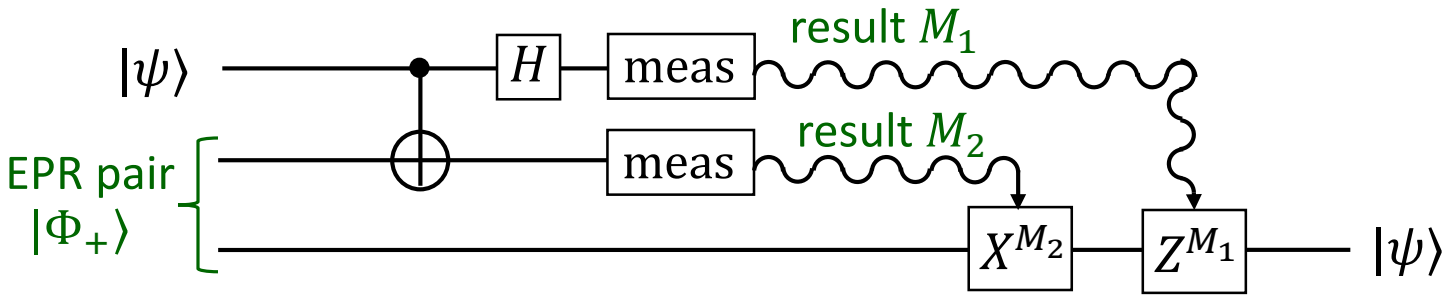
result 00: $\alpha|0\rangle + \beta|1\rangle$ good by itself, no need to do anything, $U = \hat{1}$

result 01: $\alpha|1\rangle + \beta|0\rangle$ apply $U = X$, corrects to $\alpha|0\rangle + \beta|1\rangle$

result 10: $\alpha|0\rangle - \beta|1\rangle$ apply $U = Z$

result 11: $\alpha|1\rangle - \beta|0\rangle$ apply $U = ZX$ ($\xrightarrow{X}\ \alpha|0\rangle - \beta|1\rangle\ \xrightarrow{Z}\ \alpha|0\rangle + \beta|1\rangle$)

Quantum teleportation (cont.)



Generalization: an entangled qubit can be teleported in the same way

$$|\psi_{in}\rangle = \alpha\,|0\rangle\,|\text{other}_0\rangle + \beta\,|1\rangle\,|\text{other}_1\rangle$$

(can always represent in this way with $|\alpha|^2 + |\beta|^2 = 1$
and normalized states $|\text{other}_0\rangle$ and $|\text{other}_1\rangle$)

The same analysis, just $\alpha \to \alpha|\text{other}_0\rangle,\ \beta \to \beta|\text{other}_1\rangle$

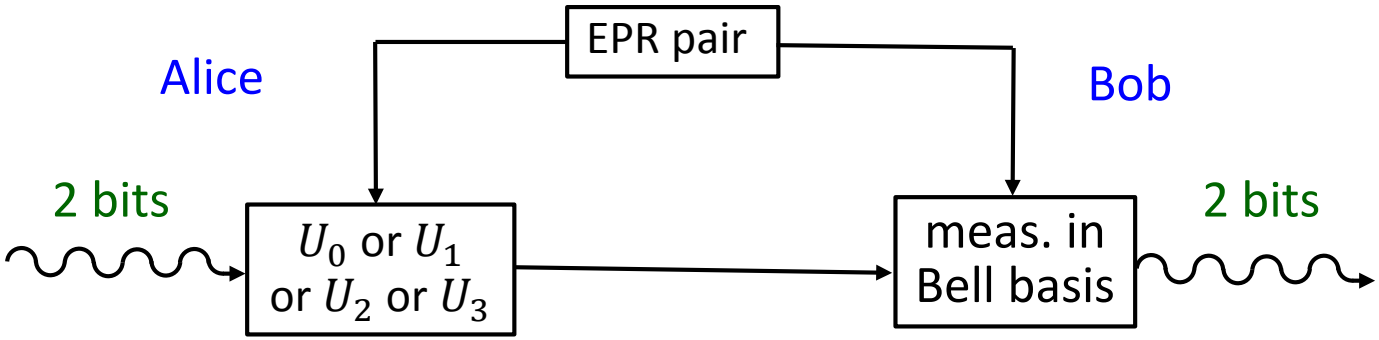
Therefore, any n-qubit entangled state can be teleported bit-by-bit (needs n EPR pairs)

Dense coding

Mermin: dense coding, usual terminology: superdense coding

Usually 1 qubit cannot carry more than 1 bit of classical information. However, with using a shared EPR pair, 1 qubit can carry 2 bits of classical information.

Procedure: reverse of teleportation



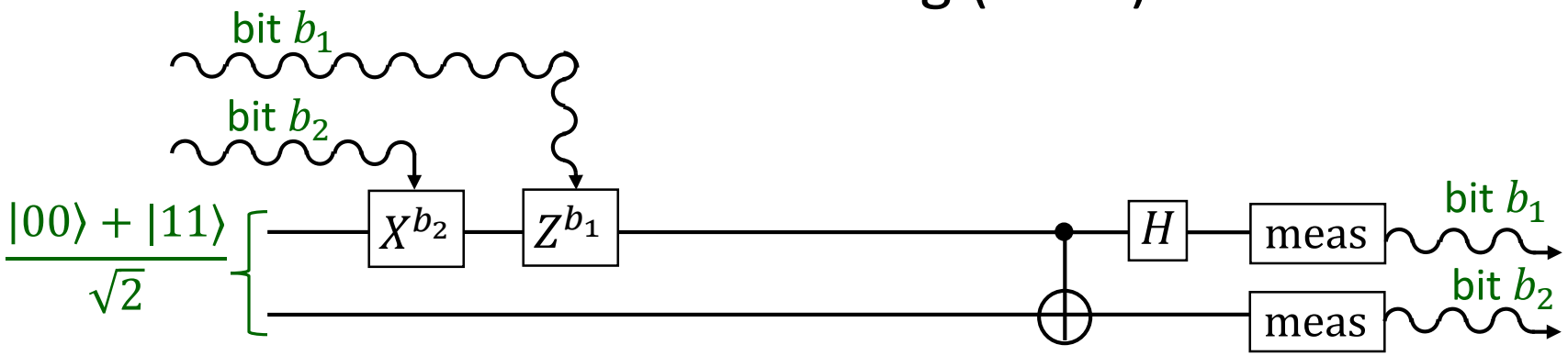
2 bits $\leq$ 1 ebit + 1 qubit

Also: 1 bit $\leq$ 1 qubit

1 ebit $\leq$ 1 qubit (can prepare EPR pair and send 1 qubit)

1 qubit $\leq$ 1 ebit +2 bits (teleportation)

Dense coding (cont.)



message 00

encoding

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{Z^{b_1}X^{b_2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{H} |00\rangle$$

message 01

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{X} \frac{|10\rangle + |01\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|11\rangle + |01\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{H} |01\rangle$$

message 10

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{Z} \frac{|00\rangle - |11\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{|00\rangle - |10\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle \xrightarrow{H} |10\rangle$$

message 11

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{ZX} \frac{-|10\rangle + |01\rangle}{\sqrt{2}} \xrightarrow{\text{CNOT}} \frac{-|11\rangle + |01\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|1\rangle \xrightarrow{H} |11\rangle$$

Classical and quantum cryptography

Old-fashioned cryptography: need to share a secret (need to meet or transfer the secret)

Modern cryptography (RSA): no need to meet (public key, private key), based on a computationally hard problem

Theoretically insecure, with a QC becomes practically insecure

How to combine security and no need to meet? $\Rightarrow$ **quantum cryptography**

Usually two steps:

1) Quantum key distribution
Alice and Bob share a long random sequence of 0s and 1s (key K)

2) one-time pad coding
Encoding: $M \oplus K = \widetilde{M}$, decoding: $\widetilde{M} \oplus K = M \oplus K \oplus K = M$

message key encoded message

Quantum cryptography addresses step 1: quantum key distribution

Idea: collapse by measurement $\Rightarrow$ possible to see if somebody tries to listen. No cloning.

Usual terminology: Alice, Bob, Eve (eavesdropper)

BB84 protocol (Bennet-Brassard, 1984)

Based on non-orthogonal states

1) Alice sends Bob qubits (photons), randomly choosing basis and state in this basis

basis 1: $|0\rangle$ (probability 25%), $|1\rangle$ (25%)

basis 2: $(|0\rangle + |1\rangle)/\sqrt{2}$ (25%), $(|0\rangle - |1\rangle)/\sqrt{2}$ (25%)

Photon polarizations

2) Bob measures qubits in the randomly chosen basis 1 (50%) or basis 2 (50%)
(QC terminology: either apply Hadamard or not before meas.)

3) Alice and Bob tell their bases publicly ("newspaper"), so that they know when they used the same basis (for N qubits sent, approximately in $N/2$ cases)

If nobody disturbs the communication channel, then Bob's results should be exactly what Alice sent

4) Alice and Bob choose a fraction of bits and check publicly if they are the same

If OK $\Rightarrow$ secure, use remaining bits as the key

If different $\Rightarrow$ discard everything (somebody disturbs the channel, eavesdropping?)
(for weak eavesdropping it is possible to use privacy amplification)

Why secure? Measuring and substituting does not work. Even QC does not help Eve.

Security of BB84 protocol

Suppose Eve has QC and tries to extract (weakly) at least some information

Still cannot get even a little of information without disturbing qubits

Assume

$$|\Phi_\mu\rangle \otimes |\Psi_{in}\rangle \longrightarrow U\left(|\Phi_\mu\rangle \otimes |\Psi_{in}\rangle\right) = |\Phi_\mu\rangle \otimes |\Psi_\mu\rangle$$

Alice's $\mu = 1,2,3,4$

Eve's

Eve tries to entangle. However, Alice's qubit should come out unchanged, therefore still a direct product

Unitary operation preserves inner product

$$\langle\Phi_\mu|\Phi_\nu\rangle \underbrace{\langle\Psi_{in}|\Psi_{in}\rangle}_{1} = \langle\Phi_\mu|\Phi_\nu\rangle\,\langle\Psi_\mu|\Psi_\nu\rangle$$

$$\Rightarrow \quad \langle\Psi_\mu|\Psi_\nu\rangle = 1$$

All of them are the same, not sensitive to μ!

Privacy amplification in quantum cryptography

Suppose Eve intercepts fraction $p \ll 1$ of qubits, then out of $\sim N/2$ shared bits, fraction $\sim p/2$ of them are known to Eve, and $\sim p/4$ are wrong

Two stages in the procedure: 1) eliminate errors, 2) amplify privacy

Stage 1: Eliminate errors

Random grouping of bits into pairs, then calculate and publicly compare parities for each pair. If Alice's and Bob's parities do not match, then discard the pair. If the parities match, keep one bit.

Then fraction of wrong bits becomes $(p/4) \to (p/4)^2$ (both bits in a pair should be wrong to survive)

Iterate $(p/4) \to (p/4)^2 \to (p/4)^4 \to (p/4)^8 \to \dots$
until no wrong bits remain (< 1 bit by estimate)

Actually, Stage 1 can be done using the standard classical error correction (then only slight decrease in the number of bits)

Privacy amplification in q. crypt. (cont.)

Stage 1: Eliminate errors

Note that all bits known to Eve pass Stage 1, while number of bits decreases by a factor 2^k after k iterations. Therefore, their fraction increases, $p/2 \to \tilde{p} = 2^k\, p/2$.

Assume $\tilde{p} \ll 1$.

Stage 2: Amplify privacy

Remaining bits are again randomly paired, but now parities are used as secret bits.

Eve knows parity only if she knows both bits $\Rightarrow$ fraction of bits known to Eve becomes $\tilde{p} \to \tilde{p}^2$

Iterate $\tilde{p} \to \tilde{p}^2 \to \tilde{p}^4 \to \tilde{p}^8 \to \ldots$ until Eve knows < 1 bit

Example: $N/2 = 10^8, \tilde{p} = 0.1$

First iteration: 5×10^7 bits, fraction 10^{-2} of bits is known to Eve
Second iteration: 2.5×10^7 bits, fraction 10^{-4} known to Eve
Third iteration: 1.25×10^7 bits, fraction 10^{-8}, OK, sufficient

Stage 2 does not change the number of errors (increases percentage)

Stage 2 can also be done using hash functions, decreasing the number of bits

Ekert-91 protocol

Based on entanglement and Bell inequality

Alice and Bob share EPR pairs

Alice measures spins along directions  (fraction 1/3 each)

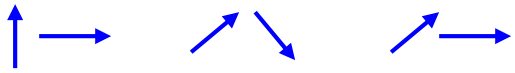
Bob measures spins along directions  (fraction 1/3 each)

Directions are publicly announced

In fraction $2/9$ of the cases, the same directions $\Rightarrow$ should perfectly anticorrelate, use as the key

The fraction $4/9$ is used to check violation of CHSH (Bell) inequality

Idea: if Eve produces pairs herself (if the qubit states exist before measurement), then CHSH inequality will not be violated.

The fraction $1/3$ is wasted 

The Ekert-91 protocol seems very different from BB84; however it was shown to be equivalent to BB84

Bit commitment

Does not work (but not trivial why), no classical protocol either

Goal: Alice decides "yes" or "no", but does not reveal her decision until some date. Bob should not be able to know her decision until that date (when Alice shares some information). Alice should not be able to cheat.

Consider the following protocol, which seems to work:

If "yes", Alice prepares $N \gg 1$ qubits randomly in states $|0\rangle$ or $|1\rangle$
If "no", then prepares qubits randomly in states $(|0\rangle + |1\rangle)/\sqrt{2}$ or $(|0\rangle - |1\rangle)/\sqrt{2}$

(Alice knows states of all qubits)

Bob cannot learn "yes" or "no", because if he measures any qubit in any basis, he gets results 50%-50% (density matrix $\rho = (|0\rangle\langle 0| + |1\rangle\langle 1|)/\sqrt{2}$)

To reveal decision, Alice tells the states, and Bob checks them
(Alice apparently cannot change decision)

Surprising loophole: actually Alice can cheat.

To cheat, Alice prepares entangled pairs $(|0_A 0_B\rangle + |1_A 1_B\rangle)/\sqrt{2}$ and keeps one qubit out of each pair. Later (when she needs to reveal decision), she measures all her qubits either in basis $\{|0\rangle, |1\rangle\}$ or in $\{|+\rangle, |-\rangle\}$ (applies Hadamard before meas.) Then "spooky action at a distance" makes Bob's qubits to become either $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$.

GHZ puzzle (Greenberg, Horne, Zeilinger, 1980s)

Similar to violation of Bell inequality, but deterministic result

GHZ state: $\frac{|000\rangle + |111\rangle}{\sqrt{2}}$ (maximally entangled, though not clear what this means)

We will discuss a modified version of the paradox

Consider state $|\psi\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$

Note: invariant under permutation of qubits

If measure, will obtain $x_1 \oplus x_2 \oplus x_3 = 0$ (easy to see)

Now apply $H_2 H_3$ and then measure.

$$0(0+1)(0+1) - 1(0-1)(0+1) - 0(0-1)(0-1) - 1(0+1)(0-1) =$$
$$= 0[(0+1)(0+1) - (0-1)(0-1)] - 1[(0-1)(0+1) + (0+1)(0-1)] =$$
$$= 0(01+10) - 1(00-11)$$ (simplified notation)

We can then write $x_1 \oplus x_2^H \oplus x_3^H = 1$

Similarly, applying $H_1 H_2$ or $H_1 H_3$ before measurement, we find (permutations)

$$x_1^H \oplus x_2^H \oplus x_3 = 1$$
$$x_1^H \oplus x_2 \oplus x_3^H = 1$$

GHZ puzzle (cont.)

$$|\psi\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$$

$$x_1 \oplus x_2 \oplus x_3 = 0$$

$$x_1 \oplus x_2^H \oplus x_3^H = 1$$

$$x_1^H \oplus x_2^H \oplus x_3 = 1$$

$$x_1^H \oplus x_2 \oplus x_3^H = 1$$

If we think that these results existed before measurement (hidden variables), then contradiction

Sum (XORed) of all 4 equations is

$$2x_1 \oplus 2x_2 \oplus 2x_3 \oplus 2x_1^H \oplus 2x_2^H \oplus 2x_3^H = 1$$

which gives $0 = 1$