Measurement "disturbs" the state.

Alice $\xrightarrow{|\psi\rangle \text{ or } |0\rangle}$ $\boxed{\text{Eve measures}}$ $\xrightarrow[|0\rangle \text{ or } |\psi\rangle]{\text{reprepares}}$ Bob.

Alice prepares state either $|0\rangle$ or $|\psi\rangle = a|0\rangle + b|1\rangle$

Eve: "intercept, resend!"

Let's say Eve wants to get $|0\rangle$ exactly right. What should she do?

Pick a basis: $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ if get outcome φ_0, send $|0\rangle$, if outcome φ_1, send $|\psi\rangle$.

---

if Alice prepares $|0\rangle$, $\quad Pr(\varphi_0) = |\langle\varphi_0|0\rangle|^2$.

needs to be 1 to always get $|0\rangle$ right.

so $|\langle\varphi_0|0\rangle|^2 = 1 \Rightarrow |\varphi_0\rangle = |0\rangle$.

but for $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ to be orthonormal

If alice sent $|\psi\rangle = a|0\rangle + b|1\rangle$, ($a \neq 0$)

$$Pr(0) = |\langle\psi|0\rangle|^2 = |a|^2 > 0$$

$$Pr(1) = |\langle\psi|1\rangle|^2 = 1-|a|^2$$

Some of the time the ~~signal~~ state ~~Alice~~ Eve sends on will be different from what Alice sent. "disturbance"

By chatting A & B can notice this.

$\boxed{3}$

Which ever pair of non-orthogonal states Alice sends, there's no measurement that distinguishes them perfectly.

~~App~~ ~~Applic~~

New Goal: just alice + bob.

Alice wants to use a qubit to send a classical message to bob → (group activity?)

She can send a bit: use $|0\rangle, |1\rangle$ basis.

If she tries to send more, there will be errors. Why?

$0 \rightarrow |\psi_0\rangle$
$1 \rightarrow |\psi_1\rangle$
$2 \rightarrow |\psi_2\rangle$

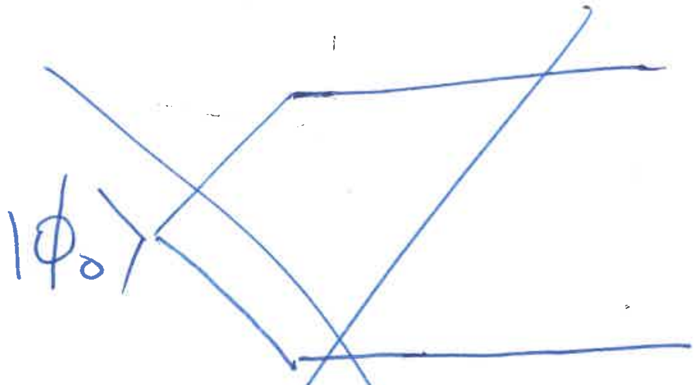
- not all pairs can be orthogonal in 2D space.
- any three vectors are lin-dep.
- so there will be a nonzero prob ~~error~~ of Bob decoding wrong

5

One qubit sends one bit.

Add an extra resource: Entanglement

first.



$|\phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

→ A 2 party state $|\psi\rangle_{AB}$ is "entangled" if there are no states $|\mu_A\rangle$ and $|\nu_B\rangle$

st

$$|\psi\rangle_{AB} = \underbrace{|\mu_A\rangle \otimes |\nu_B\rangle}_{\text{"product state"}}$$

Are these states entangled?

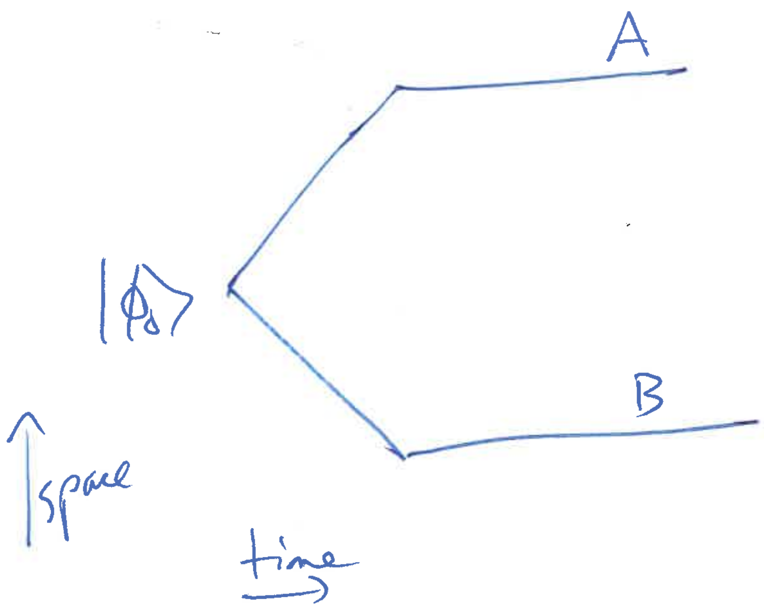
Go to clickers.

A) $|+\rangle \otimes |0\rangle$

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

Suppose alice and Bob share

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$



Can they use this to communicate?

NO. They can measure, and have correlated outcomes

but no way for Alice to tell Bob measured.

USELESS!

Sending 1 qubit, sharing 1 bell state $\rightarrow$ send 2 classical bits.

"Dense Coding"

Bell States

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right]$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle - |10\rangle\right]$$

$$|\phi_3\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right]$$

11

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

$$|\phi_1\rangle = (X \otimes \mathbb{I})\ \cancel{(\mathbb{I} \otimes X)}\ |\phi_0\rangle_{AB}$$

$$|\phi_2\rangle = (ZX) \otimes \mathbb{I}\ \cancel{\mathbb{I} \otimes (XZ)}\ |\phi_0\rangle_{AB}$$

$$|\phi_3\rangle = \cancel{(\mathbb{I} \otimes Z)}\ |\phi_0\rangle_{AB}$$

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

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

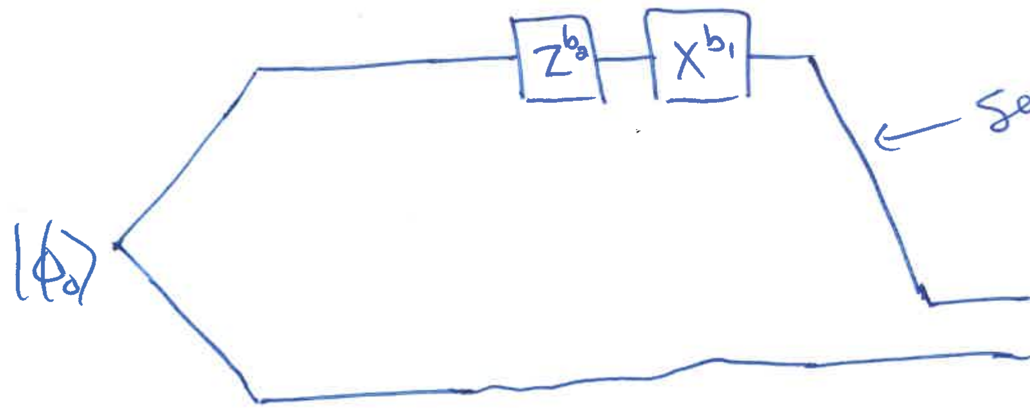
These are orthogonal.

$\Rightarrow$ there is a measurement

The plan:

1) show $|\phi_0\rangle$

Alice has 2 bits b_1, b_2:



$\leftarrow$ sends 1 qubit.

measures in $\{|\phi_i\rangle\}_{i=0}^{3}$ basis

13

if time: interesting property:

signals sent across qubit channel are all indep of b_1, b_2 from perspective of eavesdropper.

Show it?