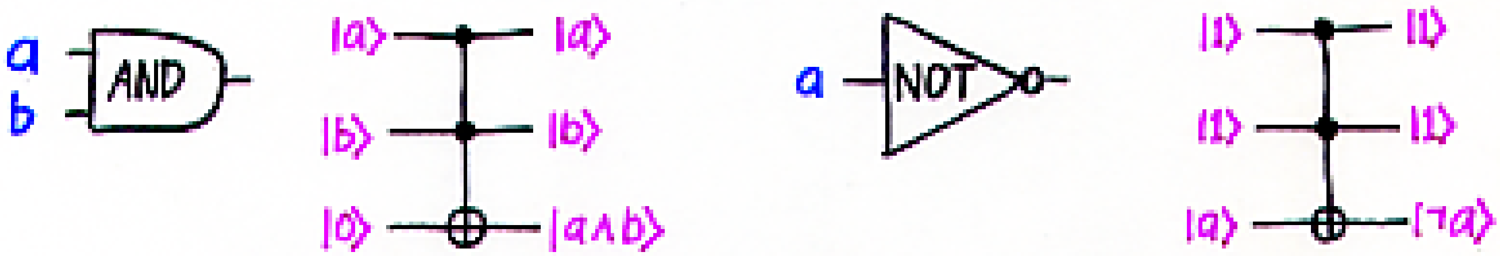
QUANTUM VS CLASSICAL CIRCUITS

THEOREM 1: A CLASSICAL CIRCUIT OF SIZE **S** CAN BE SIMULATED BY A QUANTUM CIRCUIT OF SIZE ***O(S)***

IDEA: USING TOFFOLI GATES, ONE CAN SIMULATE



IF CLASSICAL CIRCUIT COMPUTES $f:\{0,1\}^n \rightarrow \{0,1\}^m$ THEN RESULT IS A *QUANTUM* CIRCUIT THAT COMPUTES A UNITARY MAPPING SUCH THAT

$$|x_1 \cdots x_n\rangle|0\cdots 0\rangle|0\cdots 0\rangle \longmapsto |x_1\cdots x_n\rangle\underbrace{|f(x)\rangle}_{\text{OUTPUT}}\underbrace{|g(x)\rangle}_{\text{JUNK}}$$

THIS IS FINE AS LONG AS INPUT IS NOT IN *SUPERPOSITION*

IN QUANTUM ALGORITHMS, IT IS SOMETIMES USEFUL TO CONSTRUCT STATES OF THE FORM

$$\sum_x |x\rangle|f(x)\rangle$$

USING THEOREM 1, WE ONLY OBTAIN

$$\sum_x |x\rangle|f(x)\rangle|g(x)\rangle$$

WHICH MAY HAVE ENTANGLEMENT WITH THE LAST REGISTER

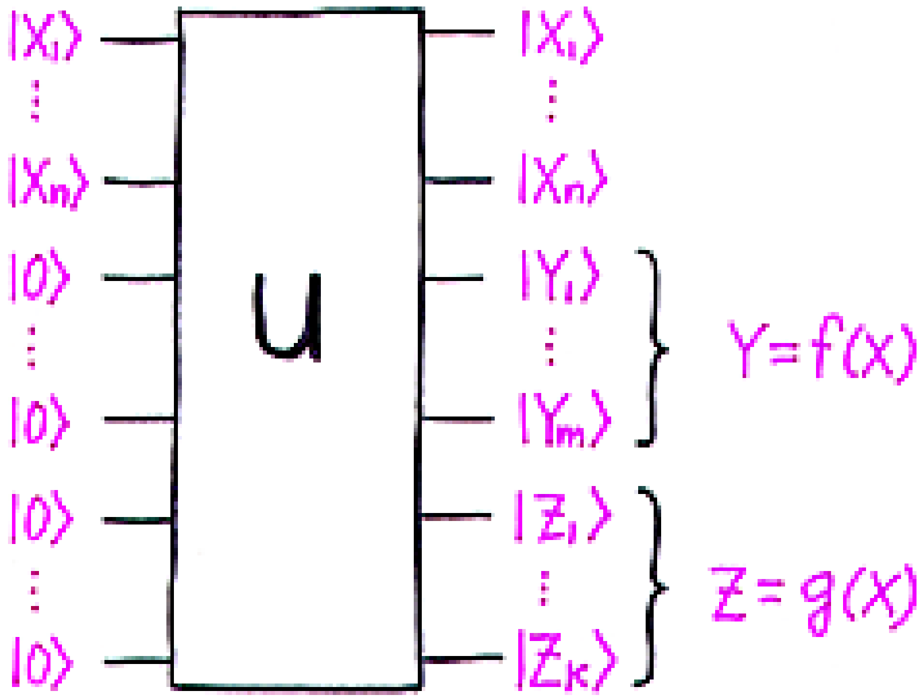
<u>THEOREM 2:</u> A CLASSICAL CIRCUIT OF SIZE **S** CAN BE SIMULATED BY A QUANTUM CIRCUIT OF SIZE **O(S)** THAT COMPUTES THE MAPPING

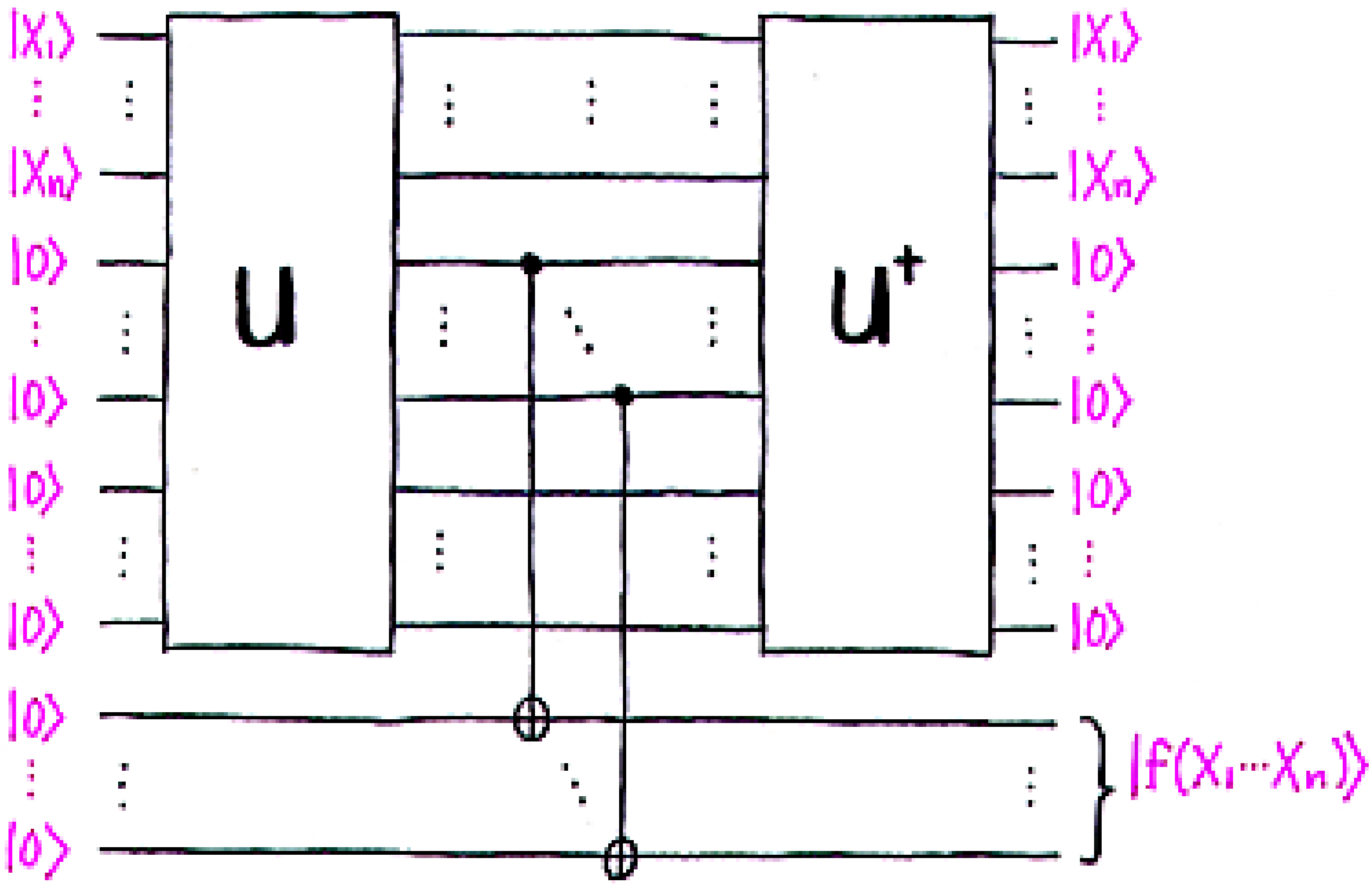
$$|x_1 \cdots x_n\rangle|0\cdots0\rangle|0\cdots0\rangle \longmapsto |x_1\cdots x_n\rangle|f(x)\rangle|0\cdots0\rangle$$

IN SUPERPOSITION, THIS RESULTS IN

$$\left(\sum_x |x\rangle|f(x)\rangle\right)|0\cdots0\rangle$$

SKETCH OF PROOF OF THEOREM 2:





THEOREM: A QUANTUM CIRCUIT OF SIZE S CAN BE SIMULATED BY A CLASSICAL CIRCUIT OF SIZE $O(2^{cS})$ (FOR SOME CONSTANT c).

IDEA: TO SIMULATE AN n-QUBIT STATE, USE AN ARRAY OF SIZE 2^n CONTAINING VALUES OF 2^n AMPLITUDES WITH PRECISION 2^{-n}

α_{000}	α_{001}	α_{010}	$\cdots$				$\cdots$	α_{111}

- ADJUST THIS STATE VECTOR WHENEVER A UNITARY OP IS TO BE PERFORMED

- BY LOOKING AT FINAL AMPLITUDES, CAN DETERMINE HOW TO SET EACH OUTPUT BIT

EXERCISE: SHOW HOW TO DO THE SIMULATION USING ONLY A POLYNOMIAL AMOUNT OF SPACE (I.E. MEMORY)

SOME COMPLEXITY CLASSES

P **POLYNOMIAL TIME**

PROBLEMS SOLVED BY $O(n^c)$-SIZE CLASSICAL CIRCUITS (DECISION PROBLEMS AND UNIFORM CIRCUIT FAMILIES)

BPP **BOUNDED-ERROR ~~QUANTUM~~ PROBABILISTIC POLY-TIME**

PROBLEMS SOLVED BY $O(n^c)$-SIZE PROBABILISTIC CIRCUITS THAT ERR WITH PROB $\leq \frac{1}{4}$

BQP **BOUNDED-ERROR QUANTUM POLY-TIME**

PROBLEMS SOLVED BY $O(n^c)$-SIZE QUANTUM CIRCUITS THAT ERR WITH PROB $\leq \frac{1}{4}$

PSPACE **POLYNOMIAL-SPACE**

PROBLEMS SOLVED BY POLYNOMIAL-<u>SPACE</u> TURING MACHINES

EXPTIME **EXPONENTIAL-TIME**

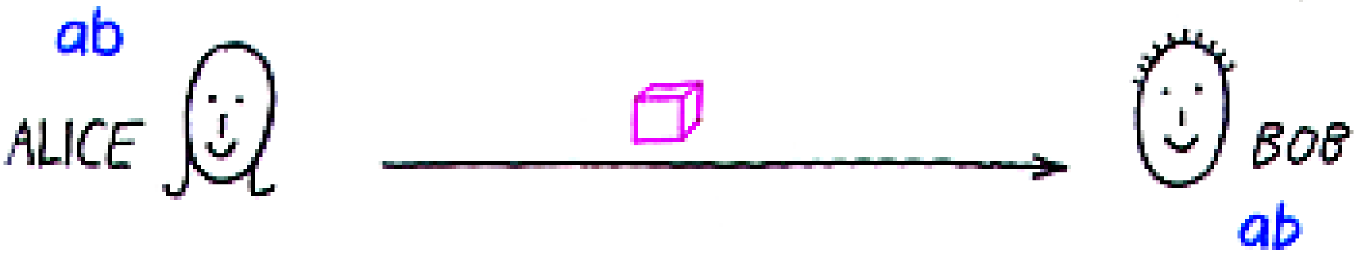
PROBLEMS SOLVED BY $O(2^{n^c})$-SIZE CIRCUITS

OUR RESULTS IMPLY THAT

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE \subseteq EXPTIME$$

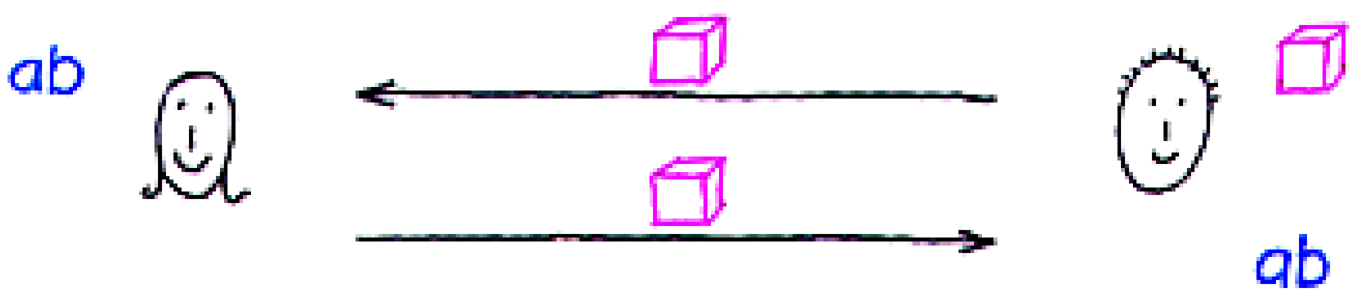
SUPERDENSE CODING

SUPPOSE ALICE WANTS TO CONVEY TWO CLASSICAL BITS TO BOB SENDING JUST ONE QUBIT



RECALL THAT, BY HOLEVO'S THEOREM, THIS IS IMPOSSIBL

IN SUPERDENSE CODING, BOB CAN SEND A QUBIT TO ALICE FIRST



HOW CAN THIS HELP?

HERE'S HOW SUPERDENSE CODING WORKS:

- BOB CREATES THE STATE $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ AND SENDS THE <u>FIRST</u> QUBIT TO ALICE

- ALICE: IF $a = 1$ THEN APPLY $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ TO QUBIT
  IF $b = 1$ THEN APPLY $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ TO QUBIT

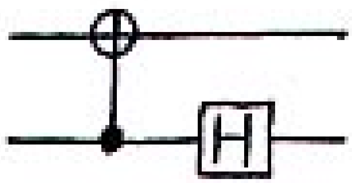
ab	STATE
00	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$
01	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$
10	$\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$
11	$\frac{1}{\sqrt{2}}\|01\rangle - \frac{1}{\sqrt{2}}\|10\rangle$

"BELL BASIS"

THEN ALICE SENDS THE QUBIT BACK TO BOB

- BOB MEASURES THE TWO QUBITS "IN BELL BASIS"

SPECIFICALLY, BOB APPLIES



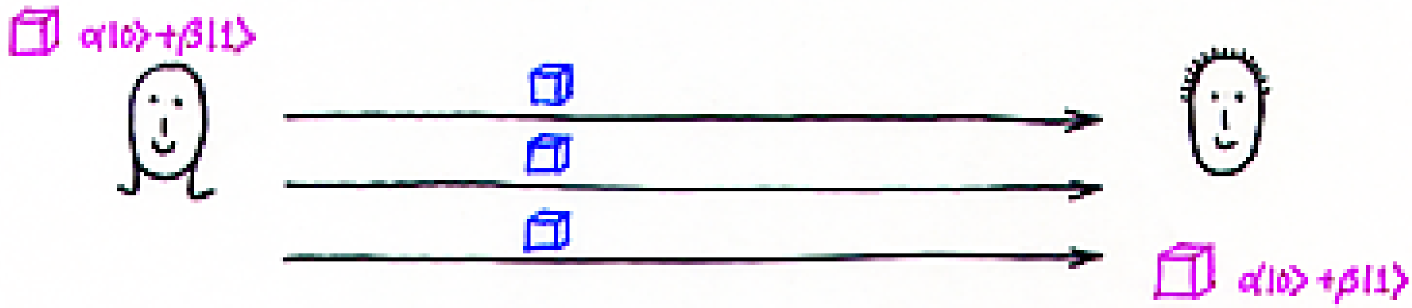
TO THE TWO QUBITS

INPUT	OUTPUT
$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\|00\rangle$
$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\|01\rangle$
$\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$	$\|10\rangle$
$\frac{1}{\sqrt{2}}\|01\rangle - \frac{1}{\sqrt{2}}\|10\rangle$	$-\|11\rangle$

AND MEASURES HIS TWO QUBITS, YIELDING ab

TELEPORTATION

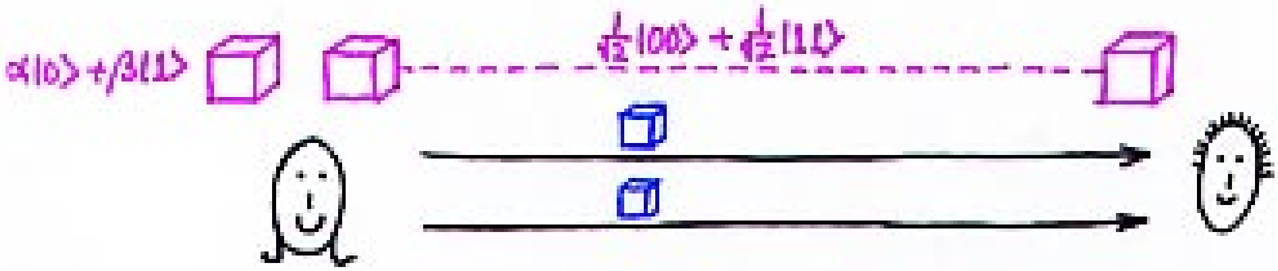
SUPPOSE ALICE WISHES TO CONVEY A QUBIT TO BOB SENDING JUST CLASSICAL BITS



IF ALICE KNOWS α AND β, SHE CAN SEND APPROXIMATIONS OF THEM — HOWEVER, THIS REQUIRES INFINITELY MANY BITS FOR PERFECT PRECISION

MOREOVER, IF ALICE DOES NOT KNOW α AND β, SHE CAN AT BEST ACQUIRE 1 BIT OF INFORMATION ABOUT THEM BY A MEASUREMENT

IN TELEPORTATION, ALICE AND BOB ALSO SHARE A BELL STATE



AND ALICE CAN SEND TWO CLASSICAL BITS TO BOB

HERE'S HOW IT WORKS:

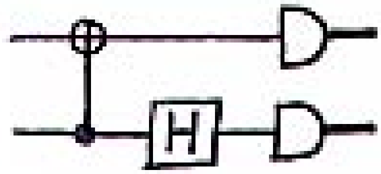
INITIAL STATE $(\alpha|0\rangle+\beta|1\rangle)(\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle)$

$$= \frac{\alpha}{\sqrt{2}}|000\rangle+\frac{\alpha}{\sqrt{2}}|011\rangle+\frac{\beta}{\sqrt{2}}|100\rangle+\frac{\beta}{\sqrt{2}}|111\rangle$$

$$\begin{aligned}
&= \tfrac{1}{2}\left(\tfrac{1}{\sqrt{2}}|00\rangle+\tfrac{1}{\sqrt{2}}|11\rangle\right)(\alpha|0\rangle+\beta|1\rangle) \\
&+\tfrac{1}{2}\left(\tfrac{1}{\sqrt{2}}|00\rangle-\tfrac{1}{\sqrt{2}}|11\rangle\right)(\alpha|1\rangle+\beta|0\rangle) \\
&+\tfrac{1}{2}\left(\tfrac{1}{\sqrt{2}}|01\rangle+\tfrac{1}{\sqrt{2}}|10\rangle\right)(\alpha|0\rangle-\beta|1\rangle) \\
&+\tfrac{1}{2}\left(\tfrac{1}{\sqrt{2}}|01\rangle-\tfrac{1}{\sqrt{2}}|10\rangle\right)(\alpha|1\rangle-\beta|0\rangle)
\end{aligned}$$

- ALICE MEASURES HER TWO QUBITS IN THE BELL BASIS AND SENDS THE RESULTS TO BOB

SPECIFICALLY, ALICE APPLIES



YIELDING THE STATE

$$\begin{cases} (00,\ \alpha|0\rangle + \beta|1\rangle) & \text{PROB } \frac{1}{4} \\ (01,\ \beta|0\rangle + \alpha|1\rangle) & \text{PROB } \frac{1}{4} \\ (10,\ \alpha|0\rangle - \beta|1\rangle) & \text{PROB } \frac{1}{4} \\ (11,\ \beta|0\rangle - \alpha|1\rangle) & \text{PROB } \frac{1}{4} \end{cases}$$

ALICE SENDS HER TWO CLASSICAL BITS TO BOB WHO THEN ADJUSTS HIS QUBIT TO BE $\alpha|0\rangle + \beta|1\rangle$ WHATEVER CASE OCCURS

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \sigma_x\sigma_z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

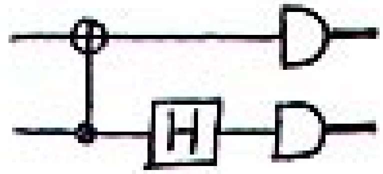
00 $\alpha|0\rangle + \beta|1\rangle$

01 $\sigma_x(\beta|0\rangle + \alpha|1\rangle) = \alpha|0\rangle + \beta|1\rangle$

10 $\sigma_z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle$

11 $\sigma_x\sigma_z(\beta|0\rangle - \alpha|1\rangle) = \alpha|0\rangle + \beta|1\rangle$

SPECIFICALLY, ALICE APPLIES



YIELDING THE STATE

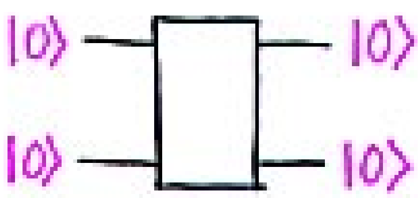
$$\begin{cases} (00,\ \alpha|0\rangle + \beta|1\rangle) & \text{PROB } \tfrac{1}{4} \\ (01,\ \beta|0\rangle + \alpha|1\rangle) & \text{PROB } \tfrac{1}{4} \\ (10,\ \alpha|0\rangle - \beta|1\rangle) & \text{PROB } \tfrac{1}{4} \\ (11,\ \beta|0\rangle - \alpha|1\rangle) & \text{PROB } \tfrac{1}{4} \end{cases}$$

ALICE SENDS HER TWO CLASSICAL BITS TO BOB WHO THEN ADJUSTS HIS QUBIT TO BE $\alpha|0\rangle + \beta|1\rangle$ WHATEVER CASE OCCURS

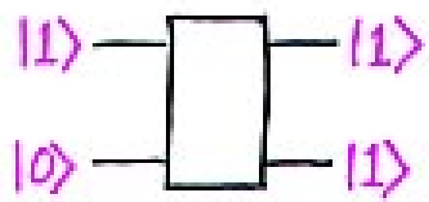
DOES THIS RESULT IN TWO COPIES OF $\alpha|0\rangle + \beta|1\rangle$? <u>NO</u>, ALICE'S COPY OF THE QUBIT GETS DESTROYED WHEN SHE MEASURES IT

NO-CLONING THEOREM: IT IS IMPOSSIBLE TO BUILD A QUANTUM "COPIER" THAT MAPS $(\alpha|0\rangle+\beta|1\rangle)|0\rangle$ TO $(\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle)$

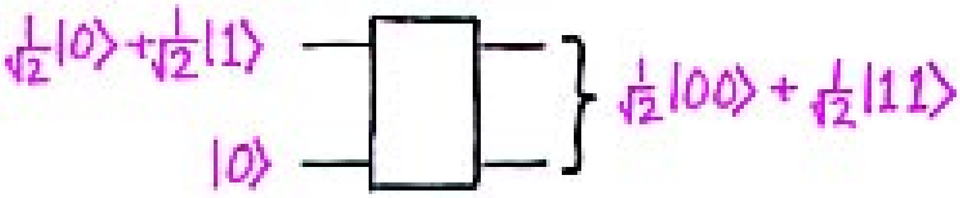
PROOF IDEA:



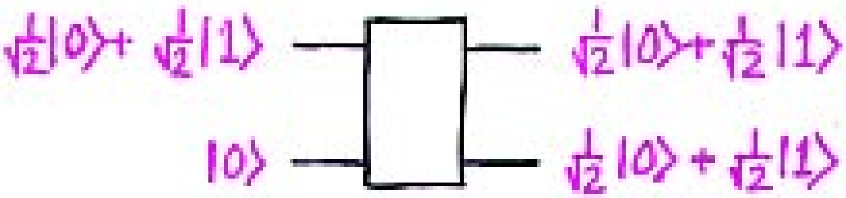
AND



SO, BY LINEARITY,



WHICH IS INCONSISTENT WITH



CONCLUSION

- WE HAVE INTRODUCED THE CONCEPT OF QUANTUM INFORMATION, A GENERALIZATION OF CLASSICAL INFORMATION

- QUANTUM INFORMATION IS THE BASIS OF NEW FAST ALGORITHMS

- QUANTUM INFORMATION IS THE BASIS OF NEW SECURE CRYPTOSYSTEMS

- QUANTUM INFORMATION CAN BE USED TO PERFORM VARIOUS OTHER FEATS IN INFORMATION PROCESSING, SUCH AS SUPER-DENSE CODING AND TELEPORTATION — AND OTHERS THAT WE'LL SEE LATER