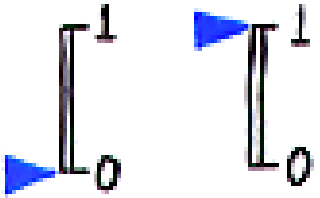
# INTRODUCTION TO QUANTUM INFORMATION

Richard Cleve
University of Calgary

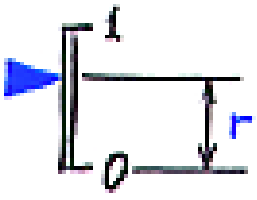
# TYPES OF INFORMATION

## DIGITAL




0 1

## ANALOG

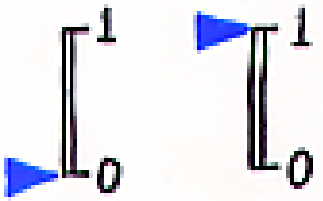



$r \in [0,1]$

- CAN EXPLICITLY EXTRACT $r$
- ISSUE OF PRECISION FOR SETTING & READING STATE
- PRECISION DOES NOT HAVE TO BE PERFECT TO BE USEFUL

# TYPES OF INFORMATION

## PROBABILISTIC DIGITAL

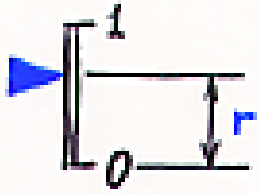



0 1

P Q

- PROBABILITIES $P, Q \in [0,1]$
  $P+Q=1$
- SOME "ANALOGNESS" HERE
- CANNOT EXPLICITLY EXTRACT $P, Q$ (ONLY STATISTICAL INFERENCE)
- IN ANY CONCRETE SETTING, EXPLICIT STATE IS 0 OR 1
- ISSUE OF PRECISION (IMPERFECT IS OK)

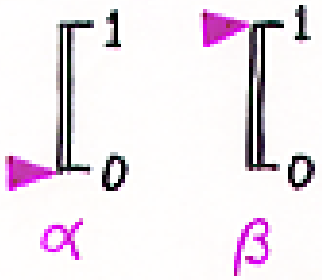
## ANALOG



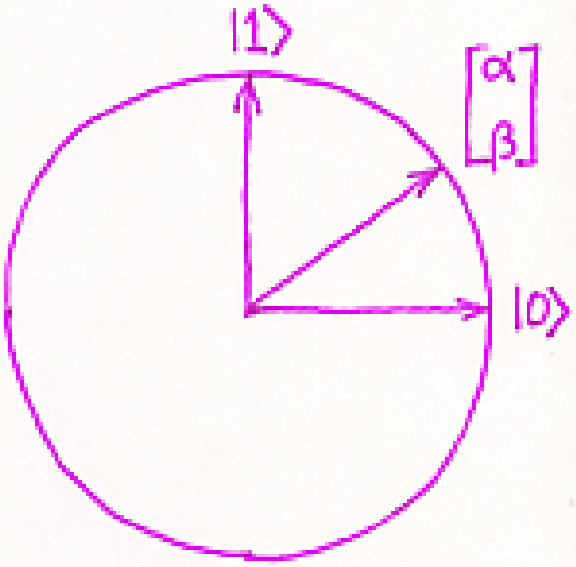

$r \in [0,1]$

- CAN EXPLICITLY EXTRACT $r$
- ISSUE OF PRECISION FOR SETTING & READING STATE
- PRECISION DOES NOT HAVE TO BE PERFECT TO BE USEFUL

# QUANTUM (DIGITAL) INFORMATION




- AMPLITUDES $\alpha, \beta \in \mathbb{C}$
  $|\alpha|^2 + |\beta|^2 = 1$
- EXPLICIT STATE IS $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- CAN'T EXPLICITLY EXTRACT $\alpha, \beta$ (ONLY STATISTICAL INFERENCE)
- ISSUE OF PRECISION (IMPERFECT IS OKAY)
- CAN BE USED TO PERFORM FEATS THAT CLASSICAL INFO CAN'T




$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$

**QUBIT**

# DIRAC BRA-C-KET NOTATION

KETS: $|\psi\rangle$ ALWAYS DENOTES A COLUMN VECTOR

E.G. $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{bmatrix}$

BRAS: $\langle\psi|$ ALWAYS DENOTES A ROW VECTOR THAT IS THE CONJUGATE TRANSPOSE OF

E.G. $[\alpha_1^* \; \alpha_2^* \cdots \alpha_d^*]$

BRACKETS: $\langle\phi|\psi\rangle$ DENOTES $\langle\phi|\cdot|\psi\rangle = [\beta_1^* \cdots \beta_d^*] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{bmatrix}$

(INNER PRODUCT OF $|\phi\rangle$ AND $|\psi\rangle$)

# BASIC OPERATIONS ON QUBITS

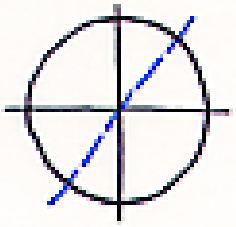
(0) INITIALIZE A QUBIT TO STATE $|0\rangle$ OR $|1\rangle$

(1) UNITARY OPERATION

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \qquad U \cdot U^{\dagger} = I$$

$\alpha|0\rangle + \beta|1\rangle \xrightarrow{U} \alpha'|0\rangle + \beta'|1\rangle$, WHERE $\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

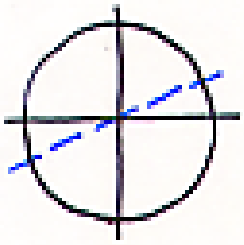
EXAMPLES: $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ ROTATION



NOT $= \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ REFLECTION

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

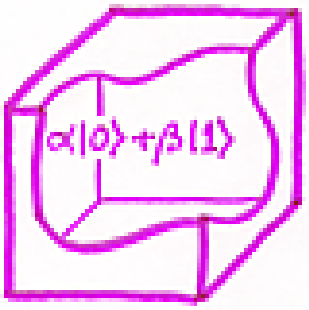
$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$ HADAMARD



$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ PHASE SHIFT

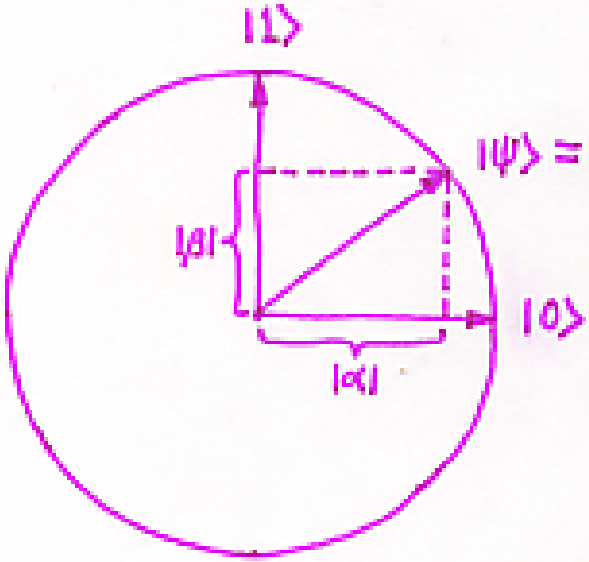
# BASIC OPERATIONS ON QUBITS (CONTINUED)

## (2) MEASUREMENT




$\longmapsto$ $\begin{cases} 0 & \text{WITH PROB } |\alpha|^2 \\ 1 & \text{WITH PROB } |\beta|^2 \end{cases}$

AND THE QUANTUM STATE COLLAPSES TO $|0\rangle$ OR $|1\rangle$



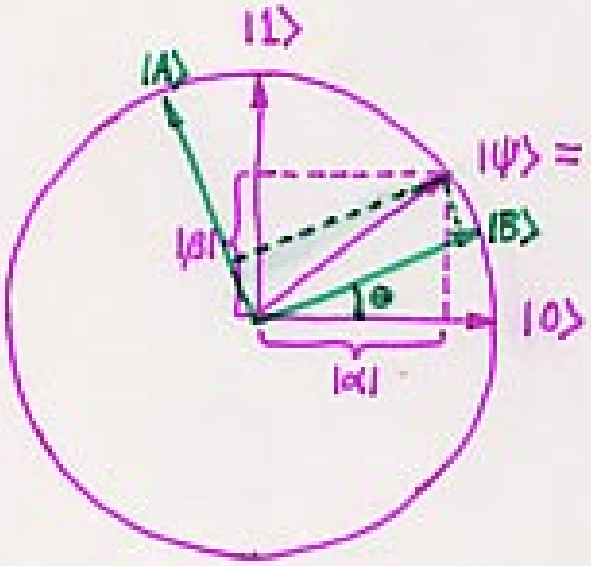

PROB OF 0 IS $|\langle\psi|0\rangle|^2$, THE LENGTH OF THE PROJECTION OF $|\psi\rangle$ ON $|0\rangle$ SQUARED

# BASIC OPERATIONS ON QUBITS (CONTINUED)

## (2) MEASUREMENT


$\longmapsto$ $\begin{cases} 0 & \text{WITH PROB } |\alpha|^2 \\ 1 & \text{WITH PROB } |\beta|^2 \end{cases}$

AND THE QUANTUM STATE COLLAPSES TO $|0\rangle$ OR $|1\rangle$




PROB OF 0 IS $|\langle\psi|0\rangle|^2$, THE LENGTH OF THE PROJECTION OF $|\psi\rangle$ ON $|0\rangle$ SQUARED

(*) THERE EXIST OTHER QUANTUM OPERATIONS BUT THEY CAN BE "SIMULATED" BY (0), (1), (2)

E.G. MEASUREMENTS WITH RESPECT TO DIFFERENT BASES

# EXAMPLES OF OPS ON QUBITS

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$|0\rangle \longleftrightarrow |1\rangle$

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

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

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

$|1\rangle \longleftrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

MEASURE

$|0\rangle \longmapsto 0$

$|1\rangle \longmapsto 1$

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \longmapsto \begin{cases} 0 & \text{PROB } \frac{1}{2} \\ 1 & \text{PROB } \frac{1}{2} \end{cases}$

$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \longmapsto \begin{cases} 0 & \text{PROB } \frac{1}{2} \\ 1 & \text{PROB } \frac{1}{2} \end{cases}$

QUESTION: SUPPOSE QUBIT  IS IN STATE $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ OR $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

CAN WE DISTINGUISH?

DISTINGUISHING PROCEDURE:

1. APPLY H
2. MEASURE

# n-QUBIT SYSTEMS

## STATE IS A $2^n$-DIMENSIONAL VECTOR

$$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{bmatrix} = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \cdots + \alpha_{111}|111\rangle$$

$$= \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

WHERE $\sum_x |\alpha_x|^2 = 1$

UNITARY OP:

$$\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \vdots \\ \alpha_{111} \end{bmatrix} \longmapsto \begin{bmatrix} U \end{bmatrix} \begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \vdots \\ \alpha_{111} \end{bmatrix}$$

MEASUREMENT:

$$\sum_x \alpha_x |x\rangle \longmapsto \begin{cases} 000 & \text{PROB} & |\alpha_{000}|^2 \\ 001 & \text{PROB} & |\alpha_{001}|^2 \\ \vdots & \vdots & \vdots \\ 111 & \text{PROB} & |\alpha_{111}|^2 \end{cases}$$

# HOW MUCH CLASSICAL INFORMATION IN $n$ QUBITS?

$2^n - 1$ COMPLEX NUMBERS NEEDED TO DESCRIBE AN ARBITRARY $n$-QUBIT (PURE) STATE:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \cdots + \alpha_{111}|111\rangle$$

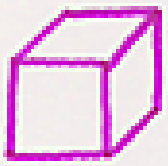
DOES THIS MEAN THAT AN EXPONENTIAL AMOUNT OF CLASSICAL INFORMATION IS SOMEHOW STORED IN $n$ QUBITS?

NO! HOLEVO'S THEOREM [1973] IMPLIES:
CANNOT EXTRACT MORE THAN $n$ BITS
FROM $n$ QUBITS

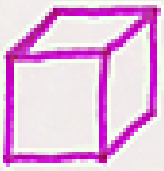
HOW MUCH INFORMATION DOES NATURE HAVE TO STORE TO MAINTAIN AN $n$-QUBIT STATE?

# EXAMPLES OF TWO-QUBIT STATES

TWO QUBITS:



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



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

JOINT STATE: $(\alpha|0\rangle+\beta|1\rangle)(\alpha'|0\rangle+\beta'|1\rangle)$

$= \alpha\alpha'|00\rangle+\alpha\beta'|01\rangle+\beta\alpha'|10\rangle+\beta\beta'|11\rangle$

WHERE WE IDENTIFY $|0\rangle|0\rangle=|00\rangle$, $|0\rangle|1\rangle=|01\rangle$ (ETC)

FORMALLY, WE ARE TAKING THE KRONECKER PRODUCT OF VECTORS: $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\otimes\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} = \begin{bmatrix}\alpha\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix}\\ \beta\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix}\end{bmatrix} = \begin{bmatrix}\alpha\alpha'\\ \alpha\beta'\\ \beta\alpha'\\ \beta\beta'\end{bmatrix}$

EXAMPLES:

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

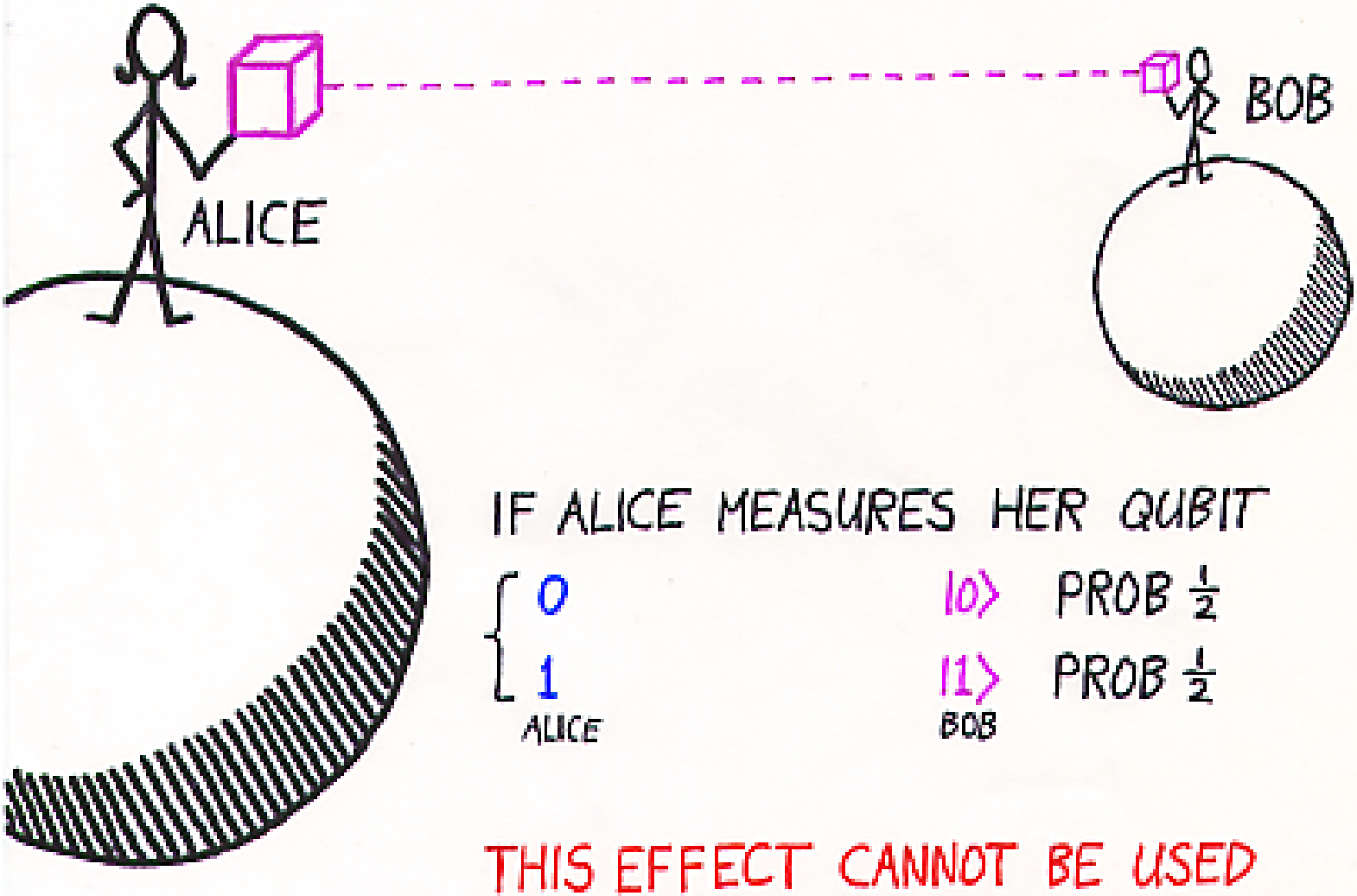
$\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle = ?$

# ENTANGLED QUBITS

CANNOT BE FACTORED

E.G. $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

CAN EXHIBIT SOME STRANGE CORRELATIONS

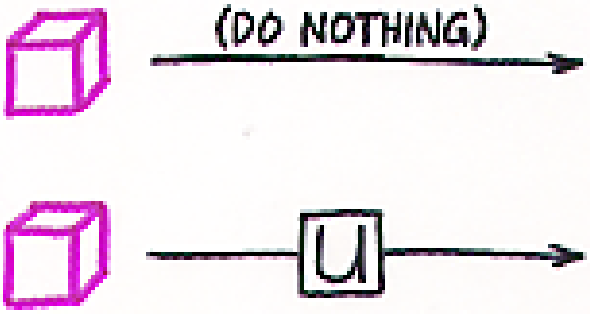



IF ALICE MEASURES HER QUBIT

| | | |
|---|---|---|
| 0 | $\|0\rangle$ | PROB $\frac{1}{2}$ |
| 1 | $\|1\rangle$ | PROB $\frac{1}{2}$ |
| ALICE | BOB | |

THIS EFFECT CANNOT BE USED TO COMMUNICATE

# ONE QUBIT OPS ON TWO-QUBIT SYSTEM




$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

$$(\alpha|0\rangle+\beta|1\rangle)(\alpha'|0\rangle+\beta'|1\rangle) \longmapsto (\alpha|0\rangle+\beta|1\rangle)(U(\alpha'|0\rangle+\beta'|1\rangle))$$

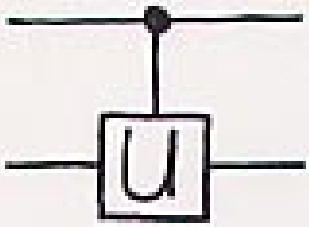
IN PARTICULAR:

$$\begin{aligned} |00\rangle &\longmapsto |0\rangle U|0\rangle \\ |01\rangle &\longmapsto |0\rangle U|1\rangle \\ |10\rangle &\longmapsto |1\rangle U|0\rangle \\ |11\rangle &\longmapsto |1\rangle U|1\rangle \end{aligned}$$

4×4 MATRIX IS $I \otimes U = \begin{bmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$

AND $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \longmapsto \frac{1}{\sqrt{2}}|0\rangle U|0\rangle + \frac{1}{\sqrt{2}}|1\rangle U|1\rangle$

# TWO-QUBIT GATES



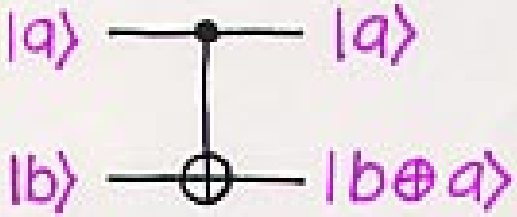

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

$|00\rangle \longmapsto |0\rangle|0\rangle$
$|01\rangle \longmapsto |0\rangle|1\rangle$
$|10\rangle \longmapsto |1\rangle U|0\rangle$
$|11\rangle \longmapsto |1\rangle U|1\rangle$

CONTROLLED-$U$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

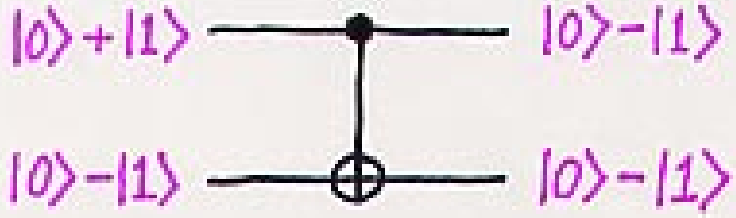
E.G. CONTROLLED-NOT (C-NOT)




⊕ DENOTES "XOR"

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

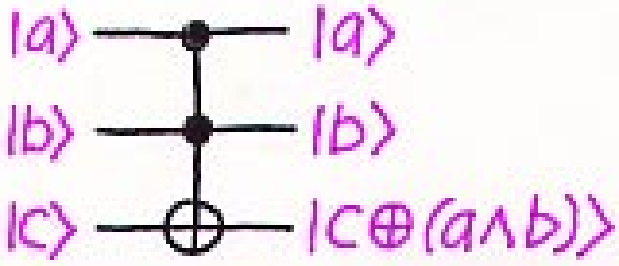
NOTE: "CONTROL" QUBIT MAY CHANGE ON SOME INPUT STATES



# MULTI-QUBIT GATES

THEOREM: ANY UNITARY OPERATION CAN BE DECOMPOSED INTO C-NOT AND ONE-QUBIT GATES

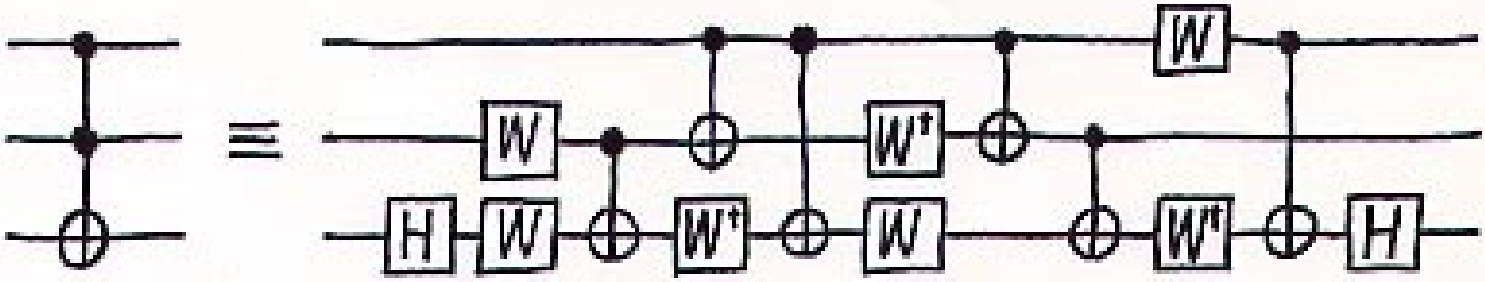
E.G. TOFFOLI GATE




FOR ALL $a, b, c \in \{0, 1\}$

$\wedge$ DENOTES "AND"

$0 \wedge 0 = 0$
$0 \wedge 1 = 0$
$1 \wedge 0 = 0$
$1 \wedge 1 = 1$

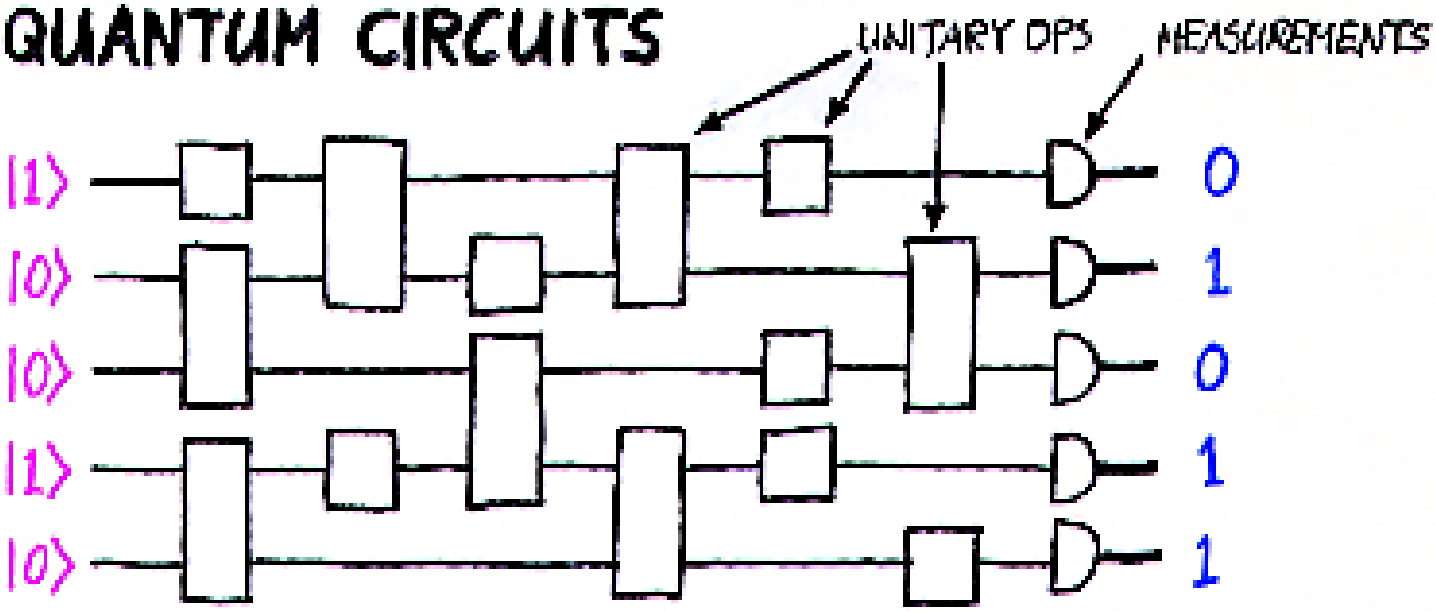



WHERE $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$ AND $W = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

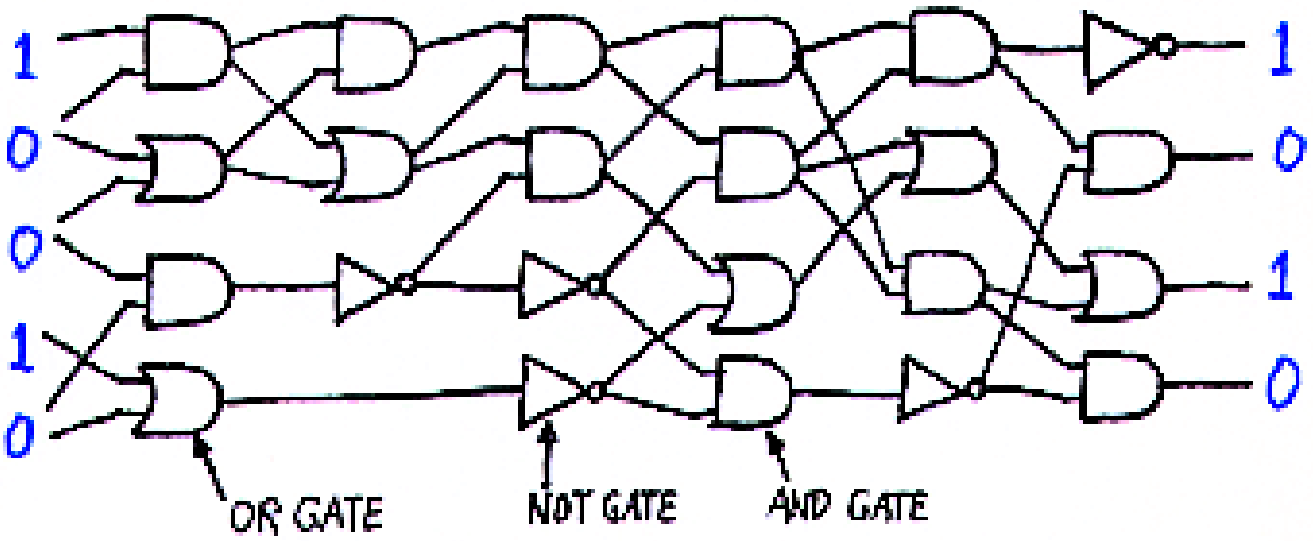
$\sqrt{i}$

# MODELS OF COMPUTATION

## QUANTUM CIRCUITS




## CLASSICAL (BOOLEAN) CIRCUITS



# MULTIPLICATION

INPUT 2 $n$-BIT NUMBERS (E.G. 101, 111)
OUTPUT THEIR PRODUCT (E.G. 100011)

- "GRADE SCHOOL" METHOD COSTS $O(n^2)$
- BEST CURRENTLY-KNOWN CLASSICAL METHOD COSTS $O(n \log n \log\log n) \approx n$
- QUANTUM METHODS: SAME

# FACTORING

INPUT AN $n$-BIT NUMBER (E.G. 100011)
OUTPUT PRIME FACTORS (E.G. 101, 111)

- TRIAL DIVISION COSTS $\approx 2^{n/2}$
- BEST CURRENTLY-KNOWN CLASSICAL METHOD COSTS $\approx 2^{n^{1/3}}$
- HARDNESS OF FACTORING IS THE BASIS OF THE SECURITY OF MANY CRYPTOSYSTEMS (E.G. RSA)
- SHOR'S QUANTUM ALGORITHM COSTS $\approx n^2$
- IMPLEMENTATION WOULD BREAK RSA, AND MANY OTHER CRYPTOSYSTEMS

# IMPLEMENTATIONS?

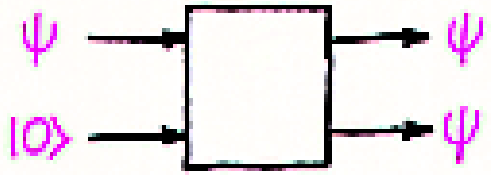
- SO FAR, A **7**-QUBIT QUANTUM COMPUTER HAS BEEN IMPLEMENTED THAT FACTORS **15** [IBM, ALMADEN]
- MANY RESEARCH GROUPS ARE EXPERIMENTING WITH VARIOUS TECHNOLOGIES

"Computers in the future may weigh no more than 1.5 tons"

—Popular Mechanics, 1949

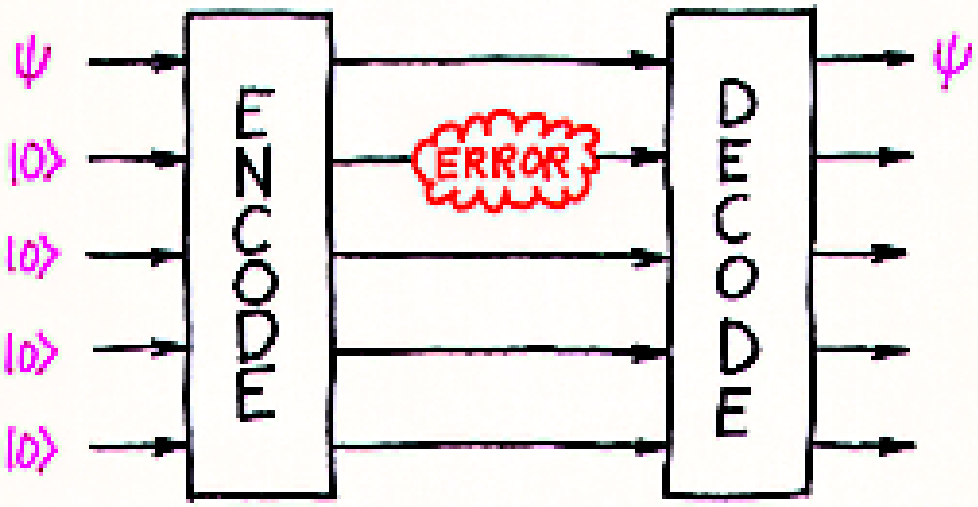
# WHAT ABOUT ERRORS?

NOTE: QUANTUM INFORMATION CANNOT BE COPIED




IS IMPOSSIBLE

NEVERTHELESS, ERROR-CORRECTION IS POSSIBLE!




## ACCURACY THRESHOLD THEOREM

IF ERROR RATE PER GATE IS $< 10^{-6}$ THEN IT IS POSSIBLE TO QUANTUM COMPUTE AND COMMUNICATE WITH ARBITRARY ACCURACY