

**Matrices & QCs: Conjugate Transpose**  $A^* = \bar{A}^T$ , eg  $A = \begin{bmatrix} 1+i & 1-i \\ i & -1 \end{bmatrix}$ ,  $A^* = \begin{bmatrix} 1-i & i \\ 1+i & -1 \end{bmatrix}$

**Defn:**  $A$  is unitary if  $AA^* = I$  (necessant also  $A^*A = I$ ).  
 $A$  is Hermitian if  $A = A^*$ .

Matrices can be both, eg.  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ,  $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ ,  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$  Pauli matrices

$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$  is unitary but not Hermitian:  $S^* = S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$ ,  $S^2 = Z$ . "Phase Matrix"

$T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$  goes through 8 phases.  $T^2 = S$ ,  $T^4 = Z$  etc.

$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  is both:  $H^\dagger = H$  and  $H^2 = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$ . Compare:  $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ ,  $I \otimes X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

**Hadamard**

**Facts:**

- If  $A$  and  $B$  are unitary, then so are  $AB$  and  $A \otimes B$ . Note:  $(AB)^* = B^*A^*$
- If  $A$  is unitary, then for any unit vector  $\phi$ ,  $A\phi$  is a unit vector.
- If  $A$  is unitary and  $N \times N$ , then  $CNOT \cdot A$  is a unitary  $2N \times 2N$  matrix. As a permutation of  $(1, \dots, N)$ ,  $w = (2, 3)$ ,  $CNOT = (3, 4)$ .
- Every permutation matrix  $P$  is unitary,  $W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$  gives the inverse permutation. Eg.  $W \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ ,  $W \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ ,  $W \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ ,  $W \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ . As actions:  $W|e_{00}\rangle = |e_{00}\rangle$ ,  $W|e_{10}\rangle = |e_{01}\rangle$  Swapping the 2nd and 3rd amplitudes effectively, swaps qubits 1 and 2.

**Theorem (Ch 4)** Pol. circ. in

Because of Fact 1, diagram QCs as compositions of gates left to right.

**Quantum circuit of  $S$  qubit** all but  $n$  initialized to  $|1\rangle$  and the same # of Toffoli gates. except for  $|1\rangle$  &  $|0\rangle$  used to clone input wires.  $CNOT$  gates used for the cloning.

**Theorem (Ch 4)** Polynomial-size classical circuits  $C_n$  of size  $S$  in wires, with  $n$  inputs.

Moreover, the output wire  $w_0$  of  $C$  becomes an output qubit  $w_0$  of the QC  $C'$ , and  $w_0 = 1 \Rightarrow$  measuring  $C'(x)$  at  $w_0$  gives 1 with certainty. Since matrices compose right to left, this is  $(CNOT)(H \otimes I)X$ .

**Basis Cloning Theorem:** We can clone basis values.

**ancillas or ancillae**

$P \subseteq BQP$

**Diagram:** A quantum circuit with input wires  $x_1, x_2, \dots, x_n, w_1, \dots, w_m$ . The  $w$  wires are initialized to  $|0\rangle$ . A CNOT gate has  $x_i$  as source and  $w$  as target. The output wire  $w_0$  is measured.

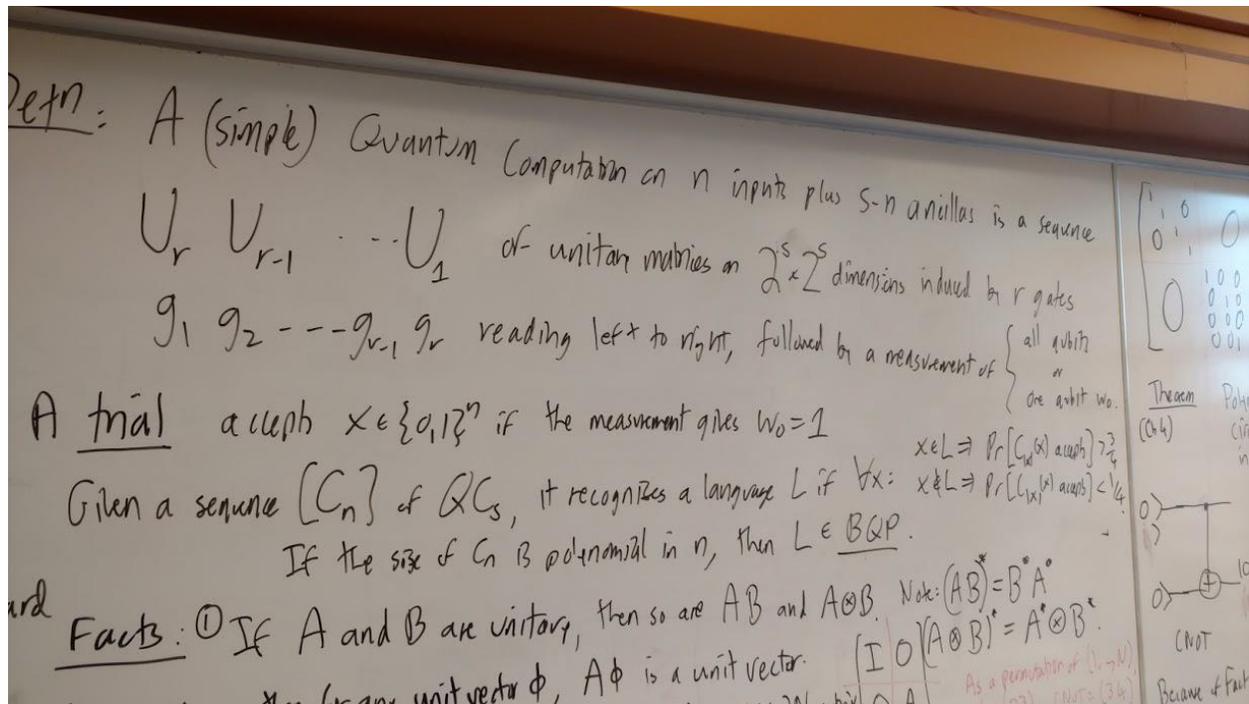
**Equations:**  $w' = W \otimes (u \otimes v)$ . If we fix  $w=1$ , then  $w' = U \text{ NAND } V$ .

**Matrix:**  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$  CNOT-CNOT also works CCX or Toffoli for Toffoli.

**TOFFOLI:**  $TOFF_{110} = E_{111}$ ,  $TOFF_{111} = E_{110}$  otherwise identity.

**Pauli matrices:**  $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ ,  $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ,  $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ ,  $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

The red at top center says, "As a permutation, TOF = (7 8). As a mapping of the standard basis it is: ..." -- then follows the part to its right in black. The red in the middle notes that to represent multiple wires  $w$  out of an input gate  $x_i$ , we need to make the ancilla qubit for  $w$  have the same value of  $x_i$ , so we initialize  $w$  to 0 not 1 and make it the target of a CNOT with  $x_i$  as source. *Basis inputs can be cloned.*



I intended to finish by stating the *amplification theorem* for BQP and BPP both: If you have a language  $L$  that belongs to BQP (respectively, BPP) via a predicate  $R(x,y)$  where

$$x \text{ is in } L \rightarrow \Pr_y[R(x,y) > 2/3]$$

$$x \text{ not in } L \rightarrow \Pr_y[R(x,y) < 1/3],$$

then for any  $m$  one can define  $R'(x,Y)$  where  $Y$  is a tuple of  $m$  strings to hold if the *majority* of  $R(x,y_j)$  values hold,  $1 \leq j \leq m$ . This gives

$$x \text{ is in } L \rightarrow \Pr_y[R(x,y) > 1 - 1/g(m)]$$

$$x \text{ not in } L \rightarrow \Pr_y[R(x,y) < 1/g(m)],$$

Where the function  $g(m)$  is exponential in  $m$ . In particular, with  $m = O(\log n)$ , one can get " $> 1 - 1/3^n$ " and " $< 1/3^n$ " in the two branches as stated in problem (1) of HW6. You can get " $> 1 - 1/6^n$ " and " $< 1/6^n$ " if you want, or " $> 1 - 1/n^3$ " vs. " $< 1/n^3$ " or whatever. This is called "amplification by majority vote" and is a powerful technique.