After Alice's measurement

| Measurement outcome | Bob's state | |
|---|---|---|
| 00 | $\alpha\|0\rangle + \beta\|1\rangle$ | ✓ |
| 01 | $\alpha\|1\rangle + \beta\|0\rangle$ | X |
| 10 | $\alpha\|0\rangle - \beta\|1\rangle$ | Z |
| 11 | $\alpha\|1\rangle - \beta\|0\rangle$ | XZ |

Then Bob fixes up the state! Cool :)

Lec 3

## Classical computation on a quantum computer

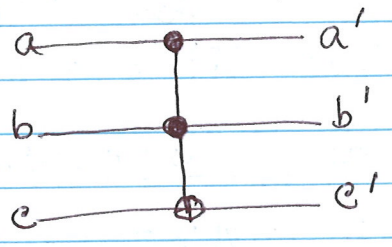
- Quantum logic gates are reversible.
- Classical logic gates are inherently irreversible. (eg. NAND)

Thm: Any classical circuit can be replaced by an equivalent circuit containing only reversible elements, by making use of a reversible gate called Toffoli gate.

Pf.

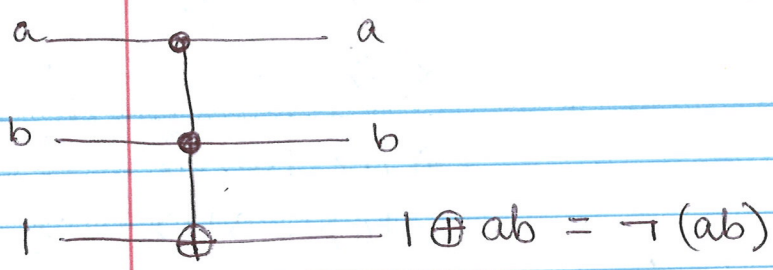
| Input | | | Output | | |
|---|---|---|---|---|---|
| a | b | c | a' | b' | c' |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 |

Circuit.

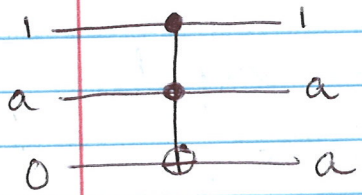



Toffoli gate.

1. Fact: Toffoli gate can simulate NAND gate.




2. Fact: Toffoli gate can simulate FANOUT gate.



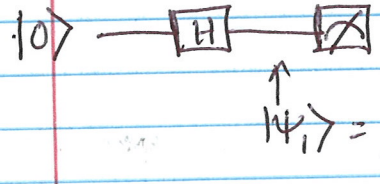

With NAND, FANOUT it becomes possible to simulate all other elements in <u>any</u> classical circuit.

But Toffoli gate is also a unitary transformation.
⇒ It can also be implemented as a <u>quantum logic gate</u>.

<u>Ex:</u> Write matrix representation of Toffoli gate.
[Hint: It is a 8×8 matrix].

**<u>Q. What about non-deterministic classical computers?</u>**

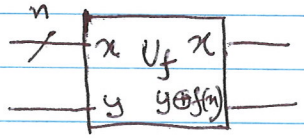
- It is sufficient to be able to simulate random fair tosses [HW: Find out why?]
- On a quantum computer this can be done by



## >>> First quantum algorithms

- Illustrate quantum parallelism.

**Lem:** The following transformation is an unitary transformation, where $f: \{0,1\}^n \to \{0,1\}$.




$$|x, y\rangle \to |x, y \oplus f(x)\rangle.$$

**Pf.** Check it is inner prod. preserving.

**Aside about Hilbert spaces ($\mathcal{H}$) over $\mathbb{C}$**

- Parallelogram law holds: $\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$
- Polarization identity holds:

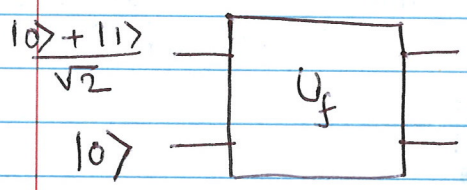
$$\langle x, y\rangle = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2 + i\|x-iy\|^2 - i\|x+iy\|^2\right)$$

$\forall x, y \in \mathcal{H}$.

↑ uses "conjugate-linearity in 1st slot" convention.

If in a normed vector space, Ilgm law holds, then it is also an inner-product space.

**Ex:** What is output of following circuit?

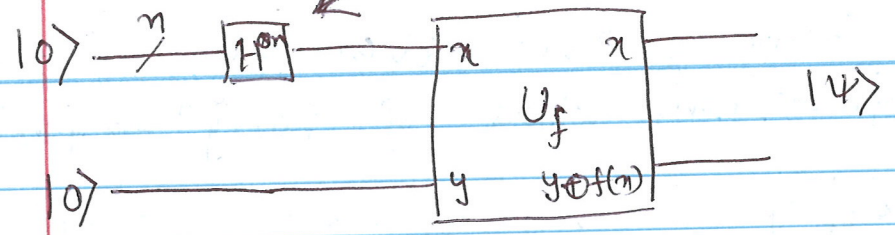



$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}.$$

↑ Remarkable state: contains information about both $f(0)$ and $f(1)$.

Generalization to $n$-qubit.

Walsh-Hadamard transform.




What is $|\psi\rangle$?

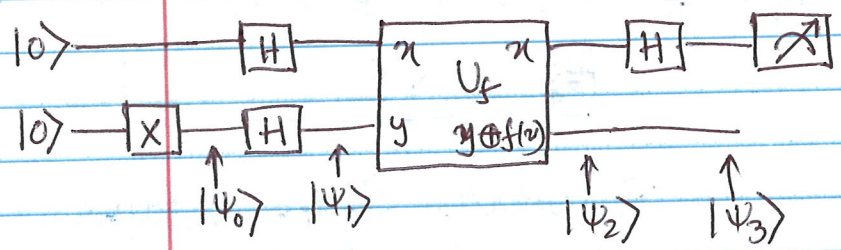
$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle$$

*** [Discussion: This parallelism is not immediately useful, as measurement collapses state to one particular state.] n+1 qubits.

[Sometimes though you want to extract global properties of $f$. Then it becomes useful] !!

## Deutsch's Algorithm

Let $f: \{0,1\} \to \{0,1\}$. Can you find $f(0) \oplus f(1)$ with one evaluation of $f$? [How about classically?]. (atleast 2).




$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Verify: $U_f\left(|x\rangle \cdot \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$.

$$\| \qquad\qquad \|$$

$$|x\rangle\left(\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}\right) = |x\rangle\left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}}\right).$$

$$|\psi_2\rangle = \begin{cases} \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm |0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm |1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1). \end{cases}$$

Note: $f(0) \oplus f(1) = \begin{cases} 0 & \text{if } f(0) = f(1) \\ 1 & \text{if } f(0) \neq f(1) \end{cases}$

$$\Rightarrow |\psi_3\rangle = \pm |f(0)\oplus f(1)\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Measuring 1st qubit thus gives $f(0) \oplus f(1)$. ∎

## Deutsch - Jozsa Algorithm (generalization of Deutsch).

$f : \{0,1\}^n \to \{0,1\}$ → either constant
→ or balanced functions [0 on $2^{n-1}$ inputs

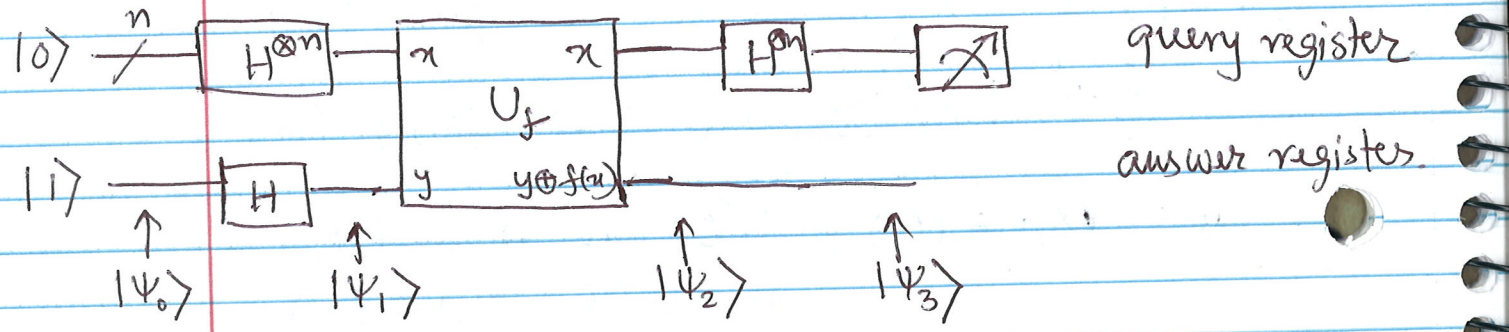
Alice Bob

Q. Classically what is the # of queries Alice needs to make to Bob in worst case?

Ans: $2^{n-1}+1$ queries.

## Quantum version

- Suppose Alice & Bob agreed to exchange qubits instead, and Bob agrees to calculate $f(x)$ using a unitary transform $U_f$, then Alice can achieve the task with just one correspondence with Bob.




$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).$$

Check

$$H|x\rangle = \sum_z \frac{(-1)^{xz}|z\rangle}{\sqrt{2}}.$$

$$|\psi_2\rangle = \sum_x (-1)^{f(x)} \frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$|\psi_3\rangle = \sum_x \frac{(-1)^{f(x)}}{\sqrt{2^n}}\left(\sum_z \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \sum_z \left(\sum_x \frac{(-1)^{f(x)+x\cdot z}}{2^n}|z\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right).$$

After measuring query register,

$$\mathbb{P}[\text{getting } |0\rangle^{\otimes n}] = \left( \sum_x (-1)^{f(x)}/2^n \right)^2.$$

If $f$ is constant, $\mathbb{P} = 1$

- if you measure $|0\rangle^{\otimes n}$, then $f$ is constant
- if you measure any other state, then $f$ is balanced.

[Ex. if $f$ balanced $\mathbb{P}[\text{getting } |0\rangle^{\otimes n}] = 0$].

[Ex. Show $\sum_x \frac{(-1)^{x \cdot z}}{2^n} = 0$ if $z \neq (0, \cdots, 0)$].

>>> Prove Kochen-Specker theorem in class if there is time!

# Linear Algebra — some necessary facts.

- Pauli matrices

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Outer products and completeness relation

$$\sum_i |i\rangle\langle i| = I \quad , \{|i\rangle\} \text{ orthonormal basis set.}$$

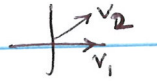
- Notice book defn of "diagonalizable matrices" incorrect. OK for Hermitian matrices.

- Hermitian matrices: $H^* = H$.
  - have real eigenvalues
  - eigenvectors corresponding to distinct eigenvals are orthogonal.

[Need defn of adjoint: $(H^*v, w) = (v, Hw)$]

- Projectors: $P^2 = P$ — have eigenvals 0, 1.
  - orthogonal projectors
  - $\sum |i\rangle\langle i|$, $\{|i\rangle\}$ are orthonormal vectors for range of projector.
  - doesn't depend on basis choice.

[there are oblique projectors which we won't need.

e.g. 

$Pv_2 = 0$
$Pv_1 = v_1$ ]

- Normal operators: $AA^\dagger = A^\dagger A$. — square matrices
  - Hermitian ops are normal
  - Unitary ops are normal

- Spectral theorem: An op. is normal iff it is diagonalizable.

$$A = \sum_i \lambda_i |i\rangle\langle i| \quad , \{|i\rangle\} \text{ orthonormal set of vectors.}$$

$$= U \Lambda U^*$$

— normal op is Hermitian iff it has real eigenvals.

- Eigenvals of unitary ops have modulus 1.
  i.e. of the form $e^{i\theta}$.

- Positive ops: $\forall v$, $\langle v|A|v\rangle = (|v\rangle, A|v\rangle)$ real, non-negative number.
  - strictly positive if $\langle v|A|v\rangle > 0$ $\forall v$.
  - (**) Positive op. is necessarily Hermitian. [Prove in class].

- Tensor products (defined last time). [Read pg 73].
  - $(P\otimes Q)(v\otimes w) = Pv \otimes Qw$.
  - $(v'\otimes w', v\otimes w) = (v', v)_{\mathcal{H}_1} \cdot (w', w)_{\mathcal{H}_2}$

  $v, v' \in \mathcal{H}_1$
  $w, w' \in \mathcal{H}_2$
  $P: \mathcal{H}_1 \to \mathcal{H}_1$
  $Q: \mathcal{H}_2 \to \mathcal{H}_2$

[Ex: - tensor prod of unitary op is unitary
- tensor prod of Hermitian op is Hermitian
- tensor prod of positive op is positive
- tensor prod of projectn is projectn. ].

Pf. $\langle z|P\otimes Q|z\rangle$, $|z\rangle = \sum_{ij} a_{ij} |i\rangle\otimes|j\rangle$

$(P\otimes Q)|z\rangle = \sum_{ij} a_{ij} P|i\rangle \otimes Q|j\rangle$

$\langle z|P\otimes Q|z\rangle = \sum_{ij}\sum_{i'j'} a^*_{i'j'} a_{ij} \langle i'|P|i\rangle\langle j'|Q|j\rangle > 0.$

[by choosing correct basis]

- Operator functions:

If you have a diagonalizable matrix (normal matrix)

$A = \sum_i \lambda_i |i\rangle\langle i|$

$f(A) = \sum_i f(\lambda_i) |i\rangle\langle i|$ → uniquely defined.

- sq. root of positive op.
- log of pos. def op.
- exp. of normal op.

- Trace of matrix: $\boxed{tr(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle}$
  - sum of diagonal elements (matrix rep chosen w.r.t orthonormal basis).
  - invariant under similarity transformation

$tr(AB) = tr(BA)$.
$tr(A+B) = tr(A) + tr(B)$.

- H-S Inner product (Hilbert-Schmidt):
  - $L(\mathcal{H},\mathcal{H})$ is a vector space.
  - It can be made an inner prod space by choosing $(A,B) \equiv tr(A^\dagger B)$, $A,B \in L(\mathcal{H},\mathcal{H})$.

  [Ex: What is dimension of $L(\mathcal{H},\mathcal{H})$?].

- Simultaneous diagonalisation theorem $AB=BA$
  - two matrices are s.d if they commute.
  - Hermitian matrices are s.d iff they commute.

  [Ex: Look up if we have "iff" is ops are not Hermitian].
  True in general for diagonalizable matrices.

- SVD $A=P\Sigma Q^\dagger$, $P,Q$ are unitary.

  if $A$ is Hermitian, $A=P|\Lambda|Q^\dagger$, $P,Q$ related by factors of $\pm 1$, for each column.

- Polar Decomp.

$$A = P\Sigma Q^\dagger, \quad A^\dagger A = Q\Sigma^2 Q^\dagger, \quad \sqrt{A^\dagger A} = Q\Sigma Q^\dagger$$
$$A^\dagger = Q\Sigma P^\dagger, \quad AA^\dagger = P\Sigma^2 P^\dagger, \quad \sqrt{AA^\dagger} = P\Sigma P^\dagger$$

$$A = P\Sigma Q^\dagger = PQ^\dagger(Q\Sigma Q^\dagger) = (PQ^\dagger)(\sqrt{A^\dagger A}).$$
$$= (P\Sigma P^\dagger)PQ^\dagger = (\sqrt{AA^\dagger})(PQ^\dagger)$$

If $A$ is linear op, $\exists$ unitary $U$ & positive ops $J,K$ s.t
$A = UJ = KU$.

- Also, $J,K$ are unique
- if $A$ is invertible then $U$ is unique.
  $U = AJ^{-1}$. [if $A$ invertible, $J$ also invertible].

$\rightarrow$ $A = UJ$, $A^\dagger = JU^\dagger$
$A^\dagger A = J^2$, so $J$ is unique.
-similarly $K$ is unique.

# Postulates of QM.

**P1:** Associated to any isolated (closed) physical system there is a Hilbert space known as state space of the system. The system is completely determined by its state vector which is a unit vector in $\mathcal{H}$.

[normalization condition].

**P2:** Evolution of closed quantum system is described by a unitary transformation.

$$|\psi(t_2)\rangle = U(t_2, t_1)\,|\psi(t_1)\rangle.$$

[Discuss with class: Measurement of qubits is non-unitary].

$$i\hbar \frac{d}{dt}|\psi\rangle = H|\psi\rangle \qquad \text{[Schrödinger equation]}.$$

($H$: Hermitian op.)

$$H = \sum_E E\,|E\rangle\langle E| \qquad \text{eigen decomposition}$$

$\{|E\rangle\}$ are called stationary states, lowest $E$ is called ground state energy, & corresponding $|E\rangle$ is ground state.

if $|\psi(t=0)\rangle = |E\rangle$, then $|\psi(t)\rangle = e^{-iEt/\hbar}|E\rangle$.

[from 1st order ODE theory].

— as $E$ is ~~matrix~~ scalar, $e^{-iEt/\hbar}$ is well defined. series converges.

$$|\psi(t)\rangle = e^{\frac{-it}{\hbar}H}|\psi(t=0)\rangle.$$

← also well defined as $H$ is a finite dim matrix.

[Discuss this notation of matrix exponential].