Quantum Information Processing (QIP)

QIP1

Information	vs.	Physics	
computation	$\longleftrightarrow$	physical process	
computer	$\longleftrightarrow$	physical system	
input	$\longleftrightarrow$	initial state	superpositions, entanglement!
00, 11 ...		$\alpha\|00\rangle + \beta\|11\rangle$	
rules (algorithm)	$\longleftrightarrow$	laws of motion	unitary evolution
output/readout	$\longleftrightarrow$	final state/measurement	

Why study QIP?

Potentially useful (!??): totally secure communication, fast factorization

Beautiful math / experimental challenge / deeper understanding of QM, and entanglement in correlated systems / better numerical codes!

QIP2

Classical bit: classical two-state system

Cbit: a = 0 or 1

Example: magnetization of domain: $\Uparrow$, $\Downarrow$

One measurement yields $M = x \in \{0,1\}$

and fully reveals state of Cbit.

Quantum bit: quantum two-state system: $\boxed{\text{QIP3}}$

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}$$

Qbit: $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle = \begin{pmatrix}\beta_0\\\beta_1\end{pmatrix}$ with $\beta_i \in \mathbb{C}$, $|\beta_0|^2 + |\beta_1|^2 = 1$

(or Qubit) superpositions are possible !! $\boxed{\text{QIP: tries to exploit this !!}}$

Example: spin of electron, polarization of photon

Let $|a\rangle$ $(a \in \{0,1\})$ be eigenstates of the observable $\hat{X}$:

$$\hat{A}\,|a\rangle = a\,|a\rangle \qquad (a \in \{0,1\})$$

One measurement of $\hat{A}$ projects $|\psi\rangle \longrightarrow |a\rangle$, with probability $|\beta_a|^2$

Infinitely many measurements are needed to accurately determine $|\alpha_x|$.

To determine phase of β_a, measure other observable not commuting with $\hat{A}$, e.g. with eigenstates $\frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$

---

2 - Bits: $\boxed{\text{QIP4}}$

2 Cbits: $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$

2-Qbit basis: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$

& all superpositions: $|\psi\rangle_2 = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

This includes "entangled states", that cannot be written as product of two single-qbit states: $\boxed{\text{QIP: tries to exploit this !!}}$

$$|\psi_{\text{entangled}}\rangle_2 \neq |\psi\rangle_1 |\psi'\rangle_1$$

Example: singlet: $\frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$

Multiple bits:

QIP5

n Cbits: $(a_1, \dots, a_n) \equiv \vec{a}$ $\qquad a_j \in \{0,1\}$

2^n distinct states

n Qbits: $|\psi\rangle = \sum_{\vec{a}} \beta_{\vec{a}} |\vec{a}\rangle \in \mathcal{H}_n$, $\sum_{\vec{a}} |\beta_{\vec{a}}|^2 = 1$

arbitrary linear combinations are possible!

$\mathcal{H}_n$ = Hilbert space (dim = 2^n) of n 2-state systems.

"Hilbert space is a large place" Carlton Caves

Reversible Single-Bit operations

QIP6

On Cbit: $0 \longrightarrow \text{NOT}(0) = 1$

$1 \longrightarrow \text{NOT}(1) = 0$

On Qbit: $|\psi\rangle \longrightarrow \mathcal{U}|\psi\rangle$ (typically: $\mathcal{U} = e^{-iHt/\hbar}$)

any unitary operation

$\boxed{\text{QIP: tries to exploit this!!}}$

Examples: $\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$: $\text{NOT}\begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_0 \end{pmatrix}$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$: $Z\begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ -\beta_1 \end{pmatrix}$

Hadamard gate: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$: $H\begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \beta_0 + \beta_1 \\ \beta_0 - \beta_1 \end{pmatrix}$

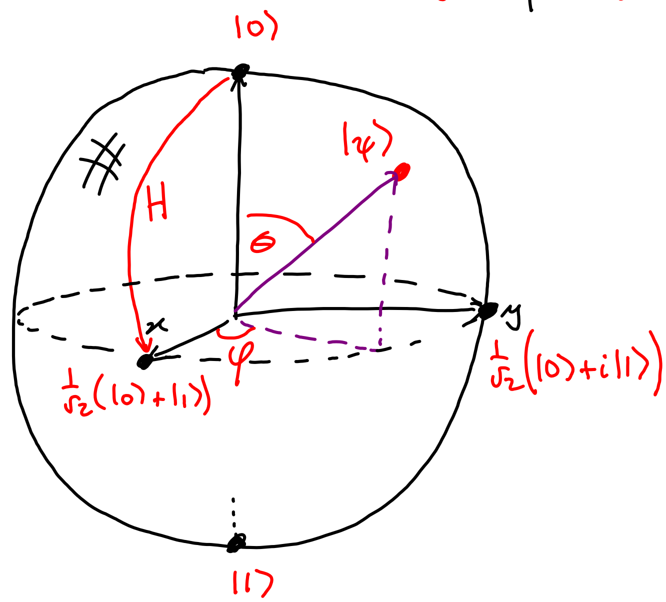
$$\left.\begin{aligned} H|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}\right\} \Rightarrow \text{produces superpositions !!}$$

Bloch sphere: any 1-Qbit state can be parametrized as: $\boxed{\text{QIP7}}$

$$|\psi\rangle = e^{i\gamma}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\theta/_2\,|1\rangle\right) \qquad 0 \le \theta \le \pi, \quad 0 \le \varphi < 2\pi$$

not observable phase prefactor

$\mathcal{U}$: maps one point on Bloch sphere to another.



<u>Reversible 2-Bit Operations</u> $\boxed{\text{QIP8}}$

Cbits: any permutation: $a_1 a_2 \to P(a_1 a_2)$ $\qquad a_i \in \{0,1\}$

Qbits: any $\mathcal{U}_{(4\times4)}$ acting on span$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

unitary

eg:
$$\mathcal{U}_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix} = \begin{pmatrix} |00\rangle \\ |01\rangle \\ |11\rangle \\ |10\rangle \end{pmatrix}$$

if $(\text{Qbit})_1 = 0$, leave $(\text{Qbit})_2$ unchanged

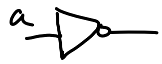
1, flip $(\text{Qbit})_2$

Theorem: "universality"

any multiple Qbit logic gate may be composed of CNOT and single Qbit gates.

Logical Circuits

$\boxed{\text{QIP9}}$

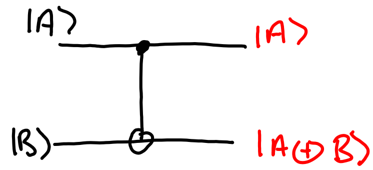
Classical circuit : 

NOT a , 

a AND B

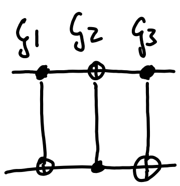
etc.

Quantum circuits:

e.g. CNOT: 

$$\left\{ \begin{array}{l} \oplus = \text{addition modulo } 2 \\ 0 \oplus 0 = 0 \\ 0 \oplus 1 = 1 \\ 1 \oplus 1 = 0 \end{array} \right.$$

compact notation: $|A, B\rangle \longrightarrow |A, A \oplus B\rangle$

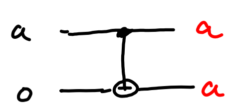
SWAP : (quantum implementation) 

$$|a, b\rangle \xrightarrow{g_1} |a, a \oplus b\rangle$$
$$\xrightarrow{g_2} |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle$$
$$\xrightarrow{g_3} |b, b \oplus (a \oplus b)\rangle = |b, a\rangle$$

Qbit copying circuit ?

$|\psi\rangle|0\rangle \longrightarrow |\psi\rangle|\psi\rangle$?

$\boxed{\text{QIP10}}$

classical version: use classical CNOT : 

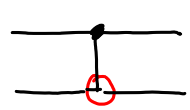
$$(a, 0) \xrightarrow{\text{CNOT}} (a, a \oplus 0) = (a, a)$$

Quantum version : $|\psi, 0\rangle \longrightarrow |\psi, \psi\rangle$ is impossible ! "no-cloning theorem"

For example, CNOT does not work: suppose $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$|\psi\rangle|0\rangle = \alpha|00\rangle + \beta|10\rangle \xrightarrow{\text{CNOT}} \alpha|00\rangle + \beta|11\rangle$$
$$\neq |\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \beta^2|11\rangle + \alpha\beta\left(|10\rangle + |01\rangle\right)$$

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

$|0\rangle$  $\alpha|00\rangle + \beta|11\rangle$

Proof of no-cloning theorem:

Suppose cloning gate U_{clone} exists.

Then $\quad U_{clone}\,|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad$ (1)

and $\quad U_{clone}\,|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle \quad$ (2)

for any $|\psi\rangle, |\varphi\rangle$

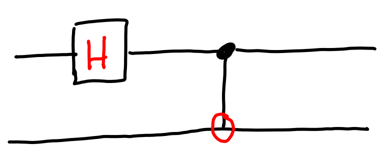
inner product of $\langle(1)|(2)\rangle$

$$\left(\langle\psi|\langle 0|\, \underbrace{U^{\dagger}_{clone}\right)\left(U_{clone}}_{=1}|\varphi\rangle|0\rangle\right) = \left(\langle\psi|\langle\psi|\right)\left(|\varphi\rangle|\varphi\rangle\right)$$

$$\langle\psi|\varphi\rangle\underbrace{\langle 0|0\rangle}_{=1} = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle$$

But : $y = y^2 \Rightarrow y = 0$ or 1, i.e. $|\psi\rangle$ and $|\varphi\rangle$ are either orthogonal or identical. So U_{clone} cannot work for for arbitrary $|\psi\rangle, |\varphi\rangle$. $\square$.

Circuit Generating Bell states:



"EPR pair" (Einstein, Rosen, Podolski, 1935)

In				Out	"Bell states"
$\|00\rangle$	$\xrightarrow{H_1}$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)\|0\rangle$	$\xrightarrow{CNOT}$	$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$	$\equiv \|B_1\rangle$
$\|01\rangle$	$\xrightarrow{H_1}$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)\|1\rangle$	$\xrightarrow{CNOT}$	$\frac{1}{\sqrt{2}}(\|01\rangle+\|10\rangle)$	$\equiv \|B_2\rangle$
$\|10\rangle$	$\xrightarrow{H_1}$	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)\|0\rangle$	$\xrightarrow{CNOT}$	$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$	$\equiv \|B_3\rangle$
$\|11\rangle$	$\xrightarrow{H_1}$	$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)\|1\rangle$	$\xrightarrow{CNOT}$	$\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)$	$\equiv \|B_4\rangle$

Quantum Teleportation

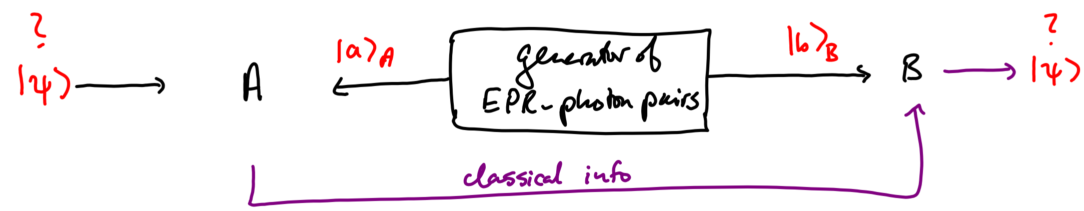
$\boxed{QIP13}$

Task: Alice (A) should deliver an unknown state $|\psi\rangle$ to Bob (B), by sending him only classical information

Allowed resource: a shared EPR pair.

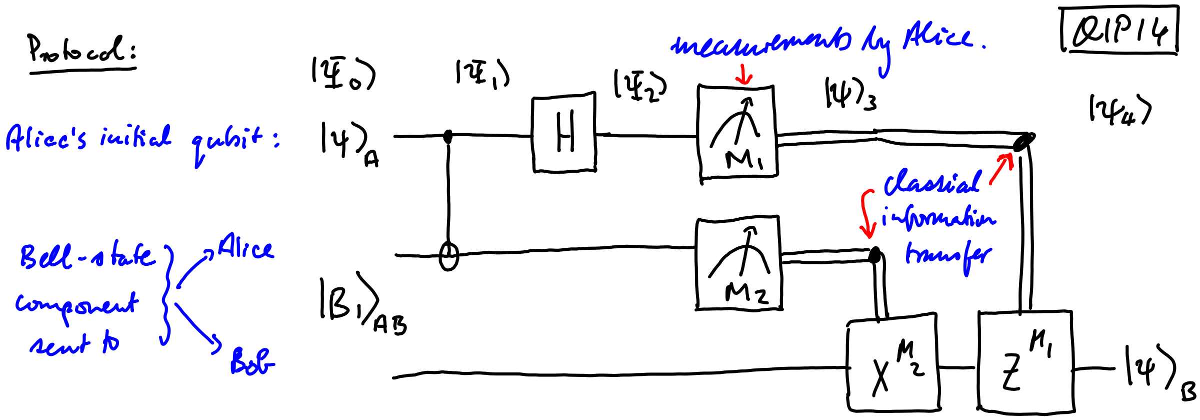
An EPR pair $|B_1\rangle$ is generated, one bit flies to Alice (A), the other to Bob (B)

$$|B_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B \right)$$



$\boxed{QIP14}$

Protocol:



Suppose $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$ = unknown, (1)

Input: $|\Psi_0\rangle = |\psi\rangle_A |B_1\rangle_{AB} = \left(\alpha|0\rangle_A + \beta|1\rangle_A\right) \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$ (2)

subscripts mean: available to A or B, will be dropped in intermediate steps

$$= \frac{\alpha}{\sqrt{2}}|0\rangle\left(|00\rangle + |11\rangle\right) + \frac{\beta}{\sqrt{2}}|1\rangle\left(|00\rangle + |11\rangle\right) \quad (3)$$

QIP15

$$|\Psi_0\rangle \xrightarrow{(CNOT)_A} |\Psi_1\rangle = \frac{\alpha}{\sqrt{2}}|0\rangle\big(|00\rangle + |11\rangle\big) + \frac{\beta}{\sqrt{2}}|1\rangle\big(|10\rangle + |01\rangle\big) \quad (1)$$

$$|\Psi_1\rangle \xrightarrow{H_A} |\Psi_2\rangle = \frac{\alpha}{2}\big(|0\rangle + |1\rangle\big)\big(|00\rangle + |11\rangle\big) + \frac{\beta}{2}\big(|0\rangle - |1\rangle\big)\big(|10\rangle + |01\rangle\big) \quad (2)$$

rearrange

$$= \Big[\underbrace{|00\rangle}_{|M_1^1, M_2^1\rangle}\underbrace{(\alpha|0\rangle + \beta|1\rangle)}_{|\psi_2^1\rangle_B}\tfrac{1}{2} + \underbrace{|01\rangle}_{|M_1^2, M_2^2\rangle}(\alpha|1\rangle + \beta|0\rangle)\tfrac{1}{2} + |10\rangle(\alpha|0\rangle - \beta|1\rangle)\tfrac{1}{2} + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\tfrac{1}{2}\Big] = \sum_{i=1}^{4}|M_1^i, M_2^i\rangle|\psi_2^i\rangle_B \quad (3)$$

$M_1^j, M_2^j \in \{0,1\}$

Now A measures her two qubits, which projects superposition onto one of four possible states:

$$|\psi_2\rangle = \sum_{i=1}^{4}|M_1^i, M_2^i\rangle_A|\psi_2^i\rangle_B \xrightarrow{M_1, M_2} |M_1^j, M_2^j\rangle|\psi_2^j\rangle_B \qquad j\in\{1,2,3,4\} \quad (4)$$

A sends her classical info (M_1, M_2) to B.

B performs on his bit, $|\psi_2^j\rangle_B$, the operations $X^{M_2^j}$ then $Z^{M_1^j}$ (5)

Claim: $Z^{M_1^j}X^{M_2^j}|\psi_2^j\rangle_B = |\psi\rangle_B$!! { now Bob has $|\psi\rangle$, without knowing its form! (6)

QIP16

Alice's measurement: phone line Bob's operation

$M|\Psi_3\rangle_A$ collapses to $|M_1^j, M_2^j\rangle_A$: $Z^{M_1^j}X^{M_2^j}|\psi_2^j\rangle_B$

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

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

$i=1$: $|0,0\rangle$: $\underbrace{Z^0X^0}_{=1}\big(\alpha|0\rangle_B + \beta|1\rangle_B\big) = \alpha|0\rangle_B + \beta|1\rangle_B = |\psi\rangle_B$

$i=2$: $|0,1\rangle$: $\underbrace{Z^0}_{=1}\cancel{X^1}\big(\alpha|1\rangle_B + \beta|0\rangle_B\big) = |\psi\rangle_B$

$i=3$: $|1,0\rangle$: $\cancel{Z^1}\underbrace{X^0}_{=1}\big(\alpha|0\rangle_B + \beta|1\rangle_B\big) = |\psi\rangle_B$

$i=4$: $|1,1\rangle$: $\cancel{Z^1}\cancel{X^1}\big(\alpha|1\rangle_B + \beta|0\rangle_B\big) = |\psi_B\rangle$

Final result: $|\psi\rangle_A|B_1\rangle_{AB} \longrightarrow |M_1, M_2\rangle_A|\psi\rangle_B$!!

□.

Quantum Parallelism

Literature: Nielsen & Chuang, "Quantum Computation & Quantum Simulation", section 1.4.2

or: D. Mermin, lecture notes on Quantum computation, Chapter 2
http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html

or: M. Christandl, "Quantum Information Processing", WiSe 09, LMU

Deutsch's Algorithm:

Let $f(x): \{0,1\} \to \{0,1\}$ be given function.

There are just four different such functions, f_i, $i = 0, 1, 2, 3$:

	$x=0$	$x=1$
$f_0(x)$	0	0
$f_1(x)$	0	1
$f_2(x)$	1	0
$f_3(x)$	1	1

but the rule specifying $f(x)$ can be complicated, e.g.:

$f(x)$ = millionth digit in binary expansion of $\sqrt{2+x}$

Challenge: decide whether or not $f(x)$ is constant or not!

Method: compute $f(0) \oplus f(1)$:

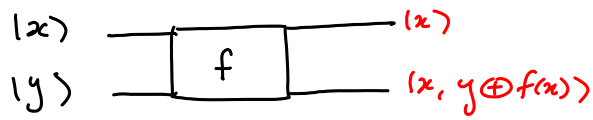
$$\begin{cases} \text{if } = 0 \Rightarrow f = \text{constant} \\ \text{if } = 1 \Rightarrow f \neq \text{constant} \end{cases} \quad (1)$$

Classically: need two queries of f, to get $f(0)$ and $f(1)$. $\boxed{\text{QIP 19}}$

Claim: quantum computer needs only 1 query of f to compute $f(0) \oplus f(1)$.

Implementation of f on 2-qubit quantum computer:

$$|x\rangle|y\rangle \longrightarrow |x\rangle, |y \oplus f(x)\rangle \qquad (1)$$



Explicitly:

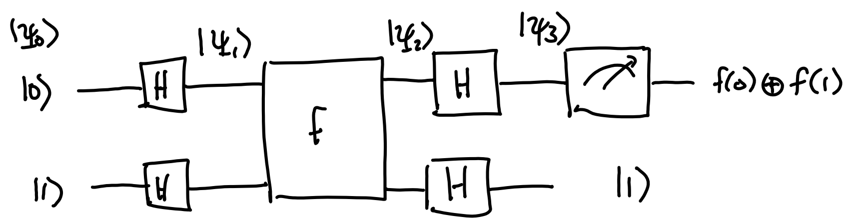
$$|x\rangle|0\rangle \xrightarrow{f} |x\rangle|f(x)\rangle, \qquad |x\rangle|1\rangle \xrightarrow{f} |x\rangle|\underbrace{\overline{f(x)}}_{=1 \oplus f(x)}\rangle \qquad (2)$$

$$|x\rangle(|0\rangle - |1\rangle) \xrightarrow{f} |x\rangle\left(|f(x)\rangle - |\overline{f(x)}\rangle\right) = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \qquad (3)$$

Check:

$$\text{if } f(x) = \begin{cases} 0 : & |x\rangle(|0\rangle - |1\rangle) \\ 1 : & |x\rangle(|1\rangle - |0\rangle) \end{cases} \checkmark = \begin{Bmatrix} 1 \\ -1 \end{Bmatrix} |x\rangle(|0\rangle - |1\rangle) \qquad (4)$$

Quantum circuit for implementing Deutsch's algorithm: $\boxed{\text{QIP 20}}$



$$|\Psi_0\rangle = |0\rangle|1\rangle \xrightarrow{H \times H} |\Psi_1\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

use: $|x\rangle(|0\rangle - |1\rangle) \xrightarrow{f} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$

$$|\Psi_1\rangle \xrightarrow{f} |\Psi_2\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-)^{f(1)}|1\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\Psi_2\rangle \xrightarrow{H \times H} |\Psi_3\rangle = \tfrac{1}{2}\left((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\right)|1\rangle$$

$\boxed{\text{QPI 21}}$

rearrange:

$$|\psi_3\rangle = \Big\{ \underbrace{\tfrac{1}{2}\big((-1)^{f(0)} + (-1)^{f(1)}\big)}_{a_0}|0\rangle + \underbrace{\tfrac{1}{2}\big((-1)^{f(0)} - (-1)^{f(1)}\big)}_{a_1}|1\rangle \Big\}|1\rangle \qquad (1)$$

$$a_0 = \begin{cases} \pm 1 & \text{if } f \text{ is const.} \\ 0 & \text{if } f \text{ is not const.} \end{cases} \qquad a_1 = \begin{cases} 0 & \text{if } f \text{ is const.} \\ \pm 1 & \text{if } f \text{ is not const.} \end{cases} \qquad (2)$$

prefactors depend on details of f that we do not care about.

$$\text{So:} \quad |\psi_3\rangle = \pm\, |\underbrace{f(0) \oplus f(1)}_{(18.1)}\rangle\, |1\rangle \qquad (3)$$

$$(18.1) = \begin{cases} |0\rangle & \text{if } f \text{ is const} \\ |1\rangle & \text{if } f \text{ is not const.} \end{cases}$$

measure first qubit of $|\psi_3\rangle$: if result is $\begin{cases} |0\rangle, & \overset{\text{conclude}}{\Longrightarrow} \quad f = \text{const.} \\ |1\rangle, & \Longrightarrow \quad f \neq \text{const.} \end{cases}$ (4)

Remarkably, f had to be applied only <u>once</u>!

$\boxed{\text{QPI 22}}$

what was the trick that caused the speedup?

put input states in a <u>superposition</u>!

$$\text{if} \quad |x\rangle|0\rangle \xrightarrow{f} |x\rangle|f(x)\rangle$$

$$|\tilde{\psi}_0\rangle = \sum_{x=0,1} |x\rangle|0\rangle \xrightarrow{f} \sum_{x=0,1} |x\rangle|f(x)\rangle = |\tilde{\psi}_1\rangle$$

a single application of f produces a state whose specification requires knowledge of both $f(0)$ <u>and</u> $f(1)$. "quantum parallelism"

Note, however, that we do <u>not</u> actually know $|\tilde{\psi}_1\rangle$.

And if we would measure it, we would only obtain $|x_0\rangle|f(x_0)\rangle$, i.e., the value of f at one, <u>randomly</u> determined, value of x_0.

$|\hat{\Psi}_1\rangle$ is useful, nevertheless, since by manipulating it in particular ways, certain of its contributions can be made to cancel due to destructive interference, (see 21.1) depending on the relation between $f(0)$ and $f(1)$ (see 21.2). Thus, information about such relations (but not the actual values of $f(0)$ and $f(1)$ themselves) can be extracted with a single measurement, which reveals which contributions to $|\hat{\Psi}_1\rangle$ vanish or not. (see 21.4)

$\boxed{\text{QPI 23}}$

Generalization of Deutsch algorithm to n qubits

$\boxed{\text{QPI 24}}$

Let $|x\rangle_n = |x_1\rangle|x_2\rangle \dots |x_n\rangle$ be an n-qubit "register", $(x_i \in \{0,1\})$ with $x = (x_1, \dots x_n) \in \{0, 2^n-1\}$ (in binary representation).

Let $f(x) : \{0, 2^{n-1}-1\} \to \{0,1\}$ be a given ($n \to 1$ qubit) function.

Quantum implementation: $|x\rangle_n|0\rangle \longrightarrow |x\rangle_n|f(x)\rangle$

Thus: $\underbrace{H_1 \otimes H_2 \otimes \dots \otimes H_n}_{H^{\otimes n}} |0\rangle \dots |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 + |1\rangle_1) \frac{1}{\sqrt{2}}(|0\rangle_2 + |1\rangle_2) \dots \frac{1}{\sqrt{2}}(|0\rangle_n + |1\rangle_n)$

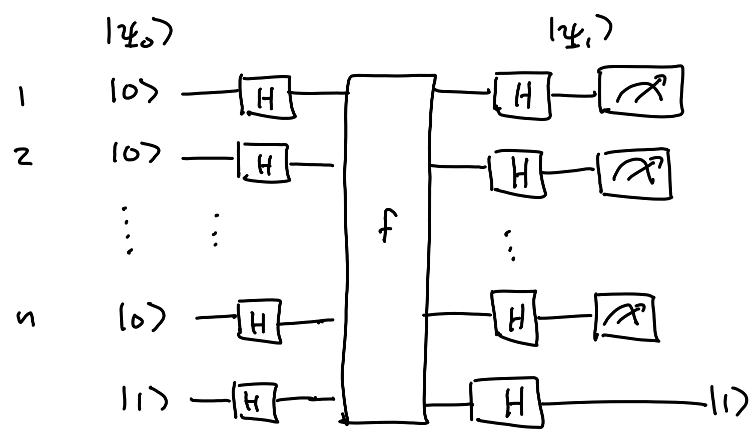
$= \frac{1}{\sqrt{2}^n} \sum_x |x\rangle_n \qquad (\sum_{x = \{0, \dots, 2^n-1\}})$

So: $|0\rangle_n|0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2}^n} \sum_x |x\rangle_n|0\rangle \xrightarrow{f} \frac{1}{\sqrt{2}^n} \sum_x |x\rangle_n|f(x)\rangle$

"massive quantum parallelism"

all values $f(x)$ are needed to describe this state!

QIP 25



Claim: $|\Psi_0\rangle = |0\rangle_n|1\rangle \longrightarrow |\Psi_1\rangle = \sum_{y\in\{0,1\}^n} a_y |y\rangle|1\rangle$,

where $$a_y = \frac{1}{2^n}\sum_{z\in\{0,1\}^n} (-1)^{f(z) + \sum_{i=1}^n y_i z_i} \qquad (1)$$

recall:
$$|\Psi_3\rangle \overset{(21.1)}{=} \left\{ \frac{1}{2}\Big(\underbrace{(-1)^{f(0)} + (-1)^{f(1)}}_{a_0}\Big)|0\rangle + \frac{1}{2}\Big(\underbrace{(-1)^{f(0)} - (-1)^{f(1)}}_{a_1}\Big)|1\rangle \right\}|1\rangle$$

QIP 26

Suppose we are told that $f(x)$ is either constant or balanced. We can determine which it is by applying f only once:

"Balanced": the $f(x)=0$ or $f(x)=1$ occur an equal number of times as x steps through all 2^n values.

Reason: $$a_0 \overset{(25.1)}{=} \frac{1}{2^n}\sum_{z\in\{0,1\}^n} (-1)^{f(z)}$$

So: $$|a_0|^2 = \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced.} \end{cases}$$

So: measure first n qubits of $|\psi_1\rangle$.

If all are found in state 0, $\overset{\text{conclude}}{\Longrightarrow}$ f = constant;

otherwise, (one or more found in state 1), $\overset{\text{conclude}}{\Longrightarrow}$ f = balanced!

Again: to extract useful information on f from $|\psi_1\rangle$, we need to exploit destructive interference!!