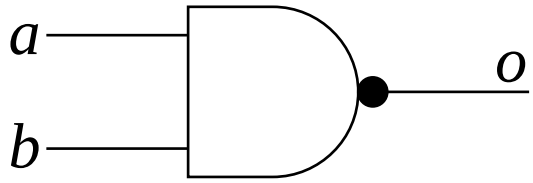
Processing bits

- Classical universal gate . . .



a	b	o
0	0	1
0	1	1
1	0	1
1	1	0

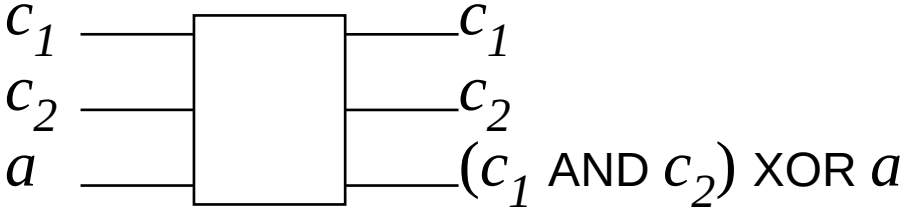
. . . is IRREVERSIBLE!

- Quantum mechanics . . .

$$|\Psi_{\text{in}}\rangle \rightarrow |\Psi_{\text{out}}\rangle = U|\Psi_{\text{in}}\rangle$$

. . . is REVERSIBLE!

- Classical reversible logic (Fredkin, Toffoli 1982)



Quantum gate = unitary operator $\hat{U}$

- Single-bit gate $\hat{U} \in U(2)$

: NOT ... $\hat{S} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

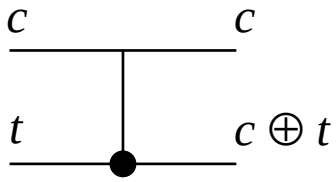
... but also "$\sqrt{\text{NOT}}$": $\hat{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

$\hat{T}|0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$

no such classical gate

- Two-bit gate $\hat{U} \in U(4)$

: CTRL-NOT



requires interaction!

: Cirac & Zoller (1995) "Cold Ions in a trap"

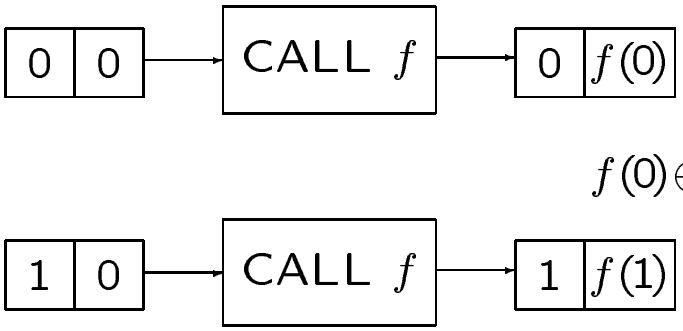
A Decision Problem

Given an oracle for a function

$$f : \{0, 1\} \to \{0, 1\}$$

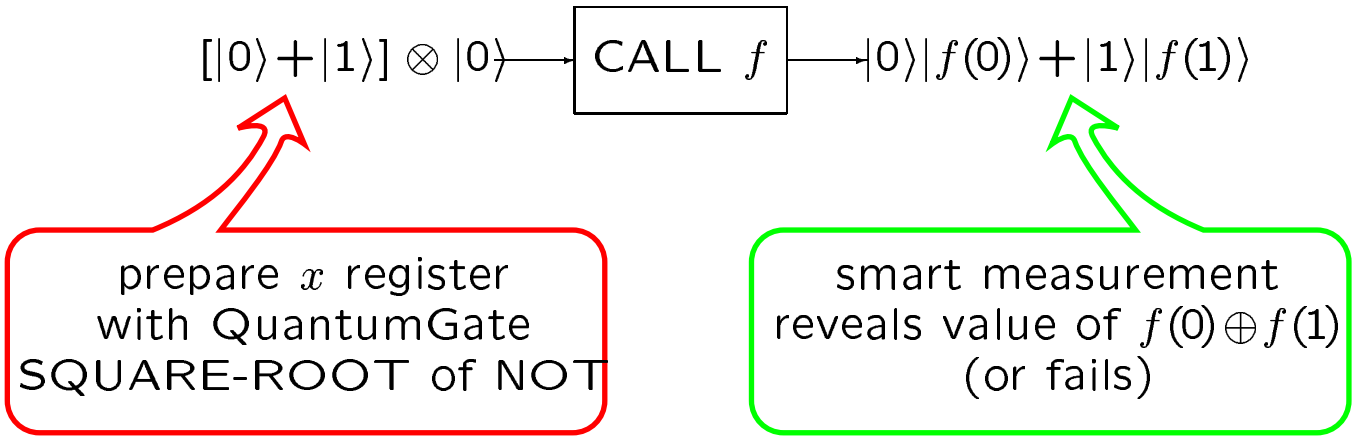
Is f constant or balanced?

- Classical computer . . . . . . calls f TWICE!

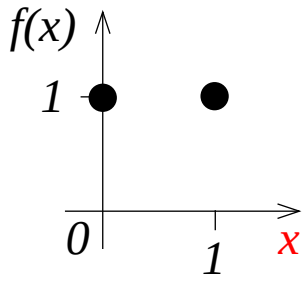


$$f(0) \oplus f(1) = \begin{cases} 0 & f \text{ is constant} \\ 1 & f \text{ is balanced} \end{cases}$$

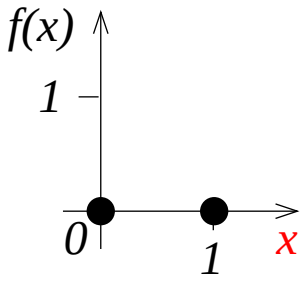
- Quantum computer . . . . . . calls f ONCE!



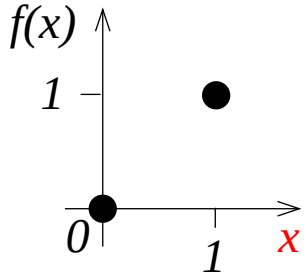
Possible Out states . . .



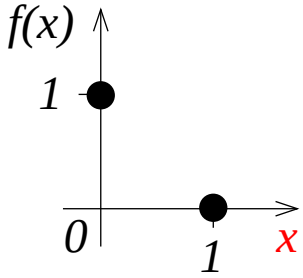
$|f_1\rangle = |01\rangle + |11\rangle$



$|f_2\rangle = |00\rangle + |10\rangle$



$|f_3\rangle = |00\rangle + |11\rangle$



$|f_4\rangle = |01\rangle + |10\rangle$

. . . are not independent!

Measurement basis . . .

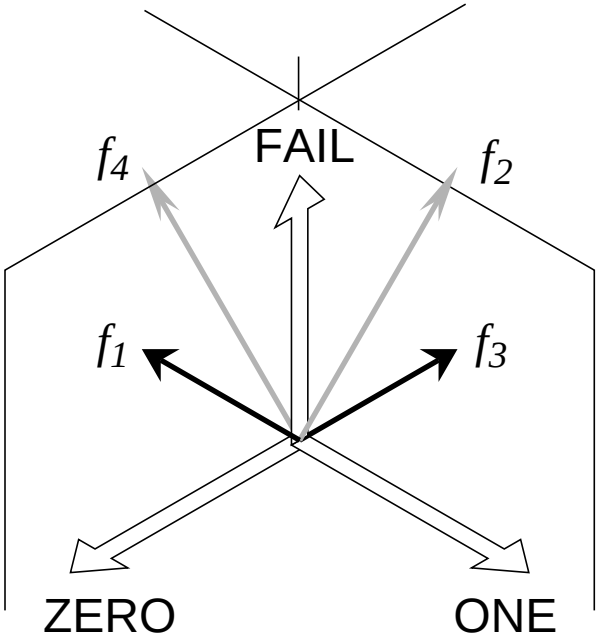
$$|\text{ZERO}\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle$$

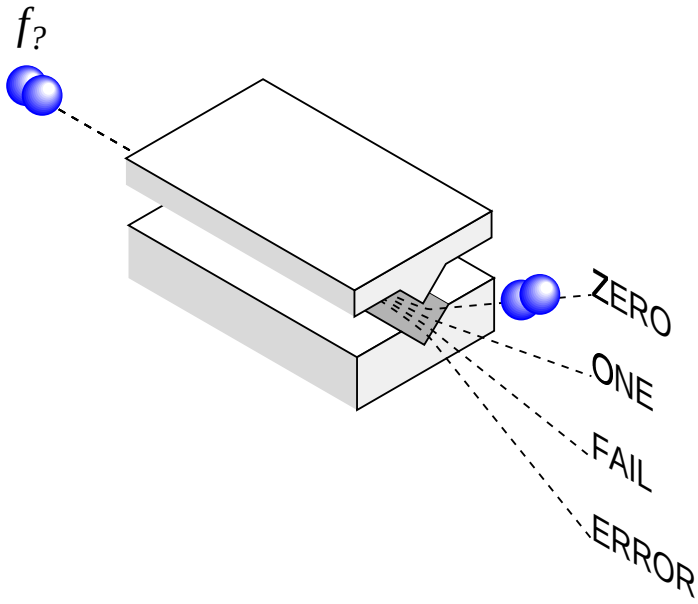
$$|\text{ONE}\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle$$

$$|\text{FAIL}\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$

$$|\text{ERROR}\rangle = |00\rangle + |01\rangle - |10\rangle - |11\rangle$$

. . . is complete and orthogonal


f4
FAIL
f2
f1
f3
ZERO
ONE



ERROR never occurs

If "CLICK" in channel ZERO: f is constant with certainty

If "CLICK" in channel ONE: f is balanced with certainty

If "CLICK" in channel FAIL: no inference possible

Prob(FAIL)=50% independent of f

in remaining 50% you know answer FOR SURE

impossible on a classical computer

Even better:

If FAIL, then guess. Successrate 50%.

Total successrate: 75% i.e. better than classical (50%).

Every second time (on average) you know something FOR SURE

This is impossible with a classical deterministic computer

Factoring

- Problem: find a factor of N
- Solution:

  : Choose any integer a coprime with N

  : Find period r of function

  $$f_{a,N}(x) \equiv a^x \bmod N$$

  : If r is even, and $r \bmod N \neq -1$, then a factor is the largest of $gcd(a^{r/2} \pm 1, N)$ [easy with Euclid's Algorithm].

- hard problem is to find r

Shor's Algorithm

- Prepare x register

$$\underbrace{\hat{T}\otimes\hat{T}\otimes\ldots\hat{T}}_{2L\,\text{times}}|\underbrace{00\cdots0}_{2L\,\text{bits}}\rangle = \frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle$$

Wow – 2^k numbers from only k operations!

- Prepare f register

$$|\underbrace{00\cdots0}_{L\,\text{bits}}\rangle$$

- Call $f_{a,N}$

$$\frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle|f_{a,N}(x)\rangle$$

- Measure on f-register only
  $\Rightarrow$ x-register is left in post-measurement state

$$|\psi\rangle \propto \sum_{j=0}^{2^{2L}/r}|jr+l\rangle$$

where offset l depends on outcome of f-measurement.

- Get rid of offset by Discrete Fourier Transform

$$\hat{S}_{\text{DFT}}|x\rangle \equiv \frac{1}{2^L}\sum_{y=0}^{2^{2L-1}}\exp\left(2\pi i\frac{xy}{2^{2L}}\right)|y\rangle$$

- CASE A (very unlikely, but instructive):
  r divides 2^L exactly; then after DFT

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(2\pi i l k/r)|k2^L/r\rangle$$

  Read off r from a couple of repetitions.

- CASE B (usual case):
  same as above, but some neighboring channels may click.

- You know when you are successfull!

- Repetition $poly(L)$ is sufficient to bring probability of success as close to 1 as desired.

Shors algorithm is EFFICIENT
but probabilistic

. . . but what about IMPLEMENTATION?

Enemies

- Manipulation and Control $\Leftrightarrow$ Coupling to World
- Coupling to world $\Leftrightarrow$ ERRORS in Computing

  : due to bit flip

$$\varrho \propto (|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \longrightarrow |0\rangle\langle 0|$$

  : due to PHASE DECOHERENCE

$$\varrho \longrightarrow |0\rangle\langle 0| + |1\rangle\langle 1|$$