The advantage of quantum computers

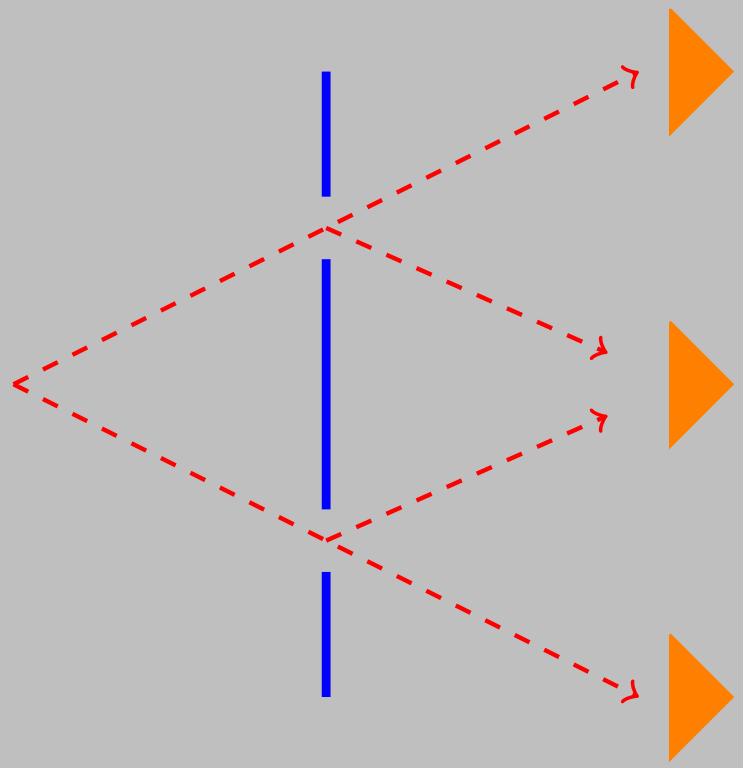
Deutsch algorithm

J Avron

July 26, 2018

Quantum mechanics is weird

Schrodinger's cat



The quantum world is different

Superpositions

Qubit

A probabilistic logical bit

- Qubit
  - Atoms with 2 levels
  - Nuclei with spin 1/2
  - Polarization of photons
  - Photon in a pair of fibers

Photon in a pair of optical fiber

$|0\rangle$ ⟶

$|1\rangle$ ⟶

Qubit: Answers True/False questions probabilistically

Superposition

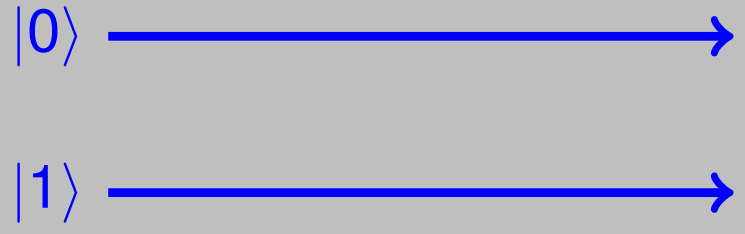
Key to quantum behavior

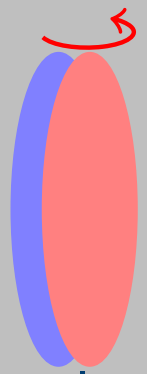
- Superposition

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}$$

- Schrodinger's cat

Photon in a pair of optical fiber





Spinning coin: Classical analog of a bit in superposition

Familiar superpositions

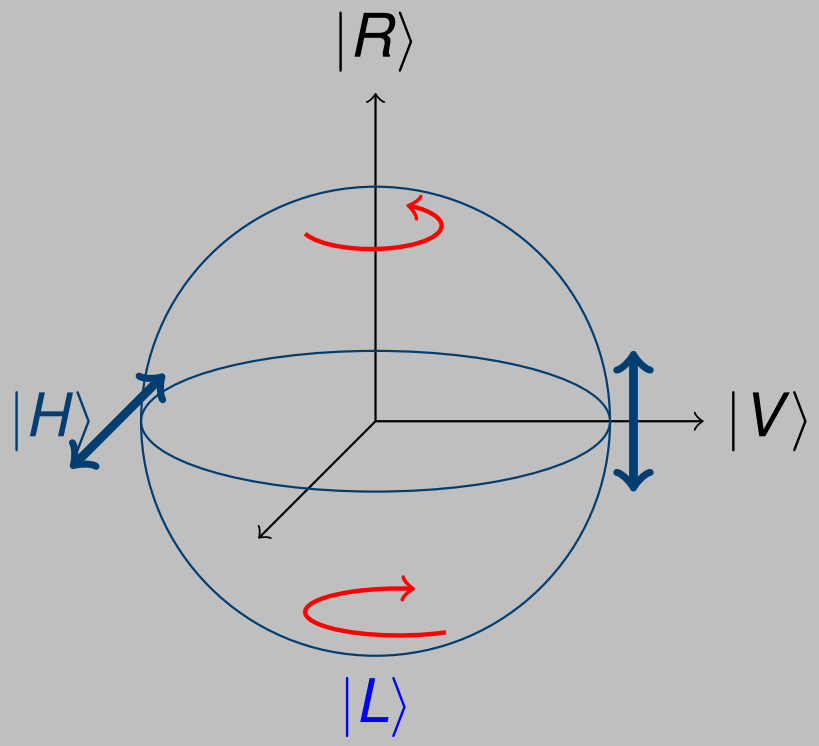
Polarization of photons

- Horizontal/vertical polarized

$$|H\rangle = |0\rangle, \quad |V\rangle = |1\rangle$$

- Right/Left circular polarized

$$|R/L\rangle = \frac{|H\rangle \pm i|V\rangle}{\sqrt{2}}$$

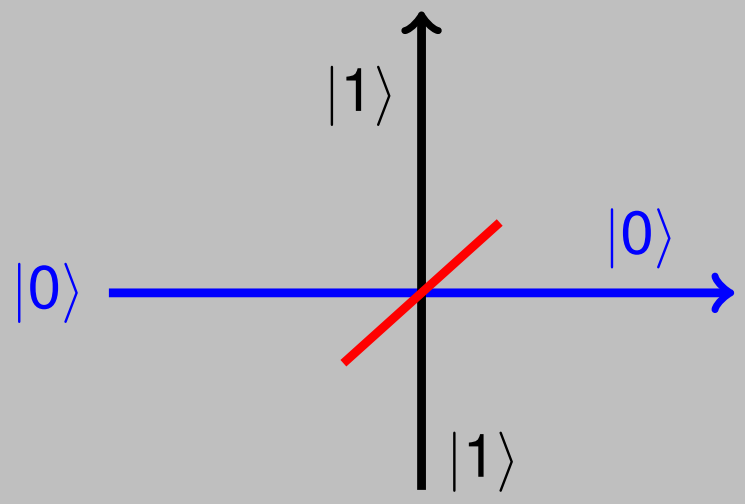


Weird superpositions

Schrodinger's cat

Half silvered mirror:

Photons with schizophrenia

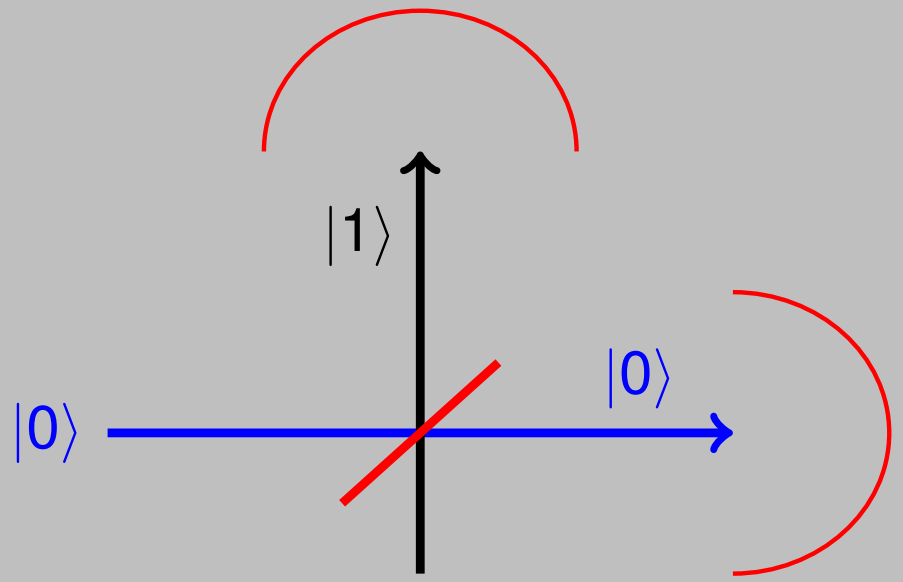


Superposition respects individuality

$$|0\rangle \mapsto |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \qquad |1\rangle \mapsto |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Quantum mechanics is probabilistic

Always, only one detector clicks, randomly



Deterministic preparation, random clicks

Qubits: probabilistic logical bits

Answer True/False questions, sometimes lie

Classical and quantum probabilities

Classical probability: consequence of incomplete information.

$$Prob(0) = 1/2, \quad Prob(1) = 1/2$$

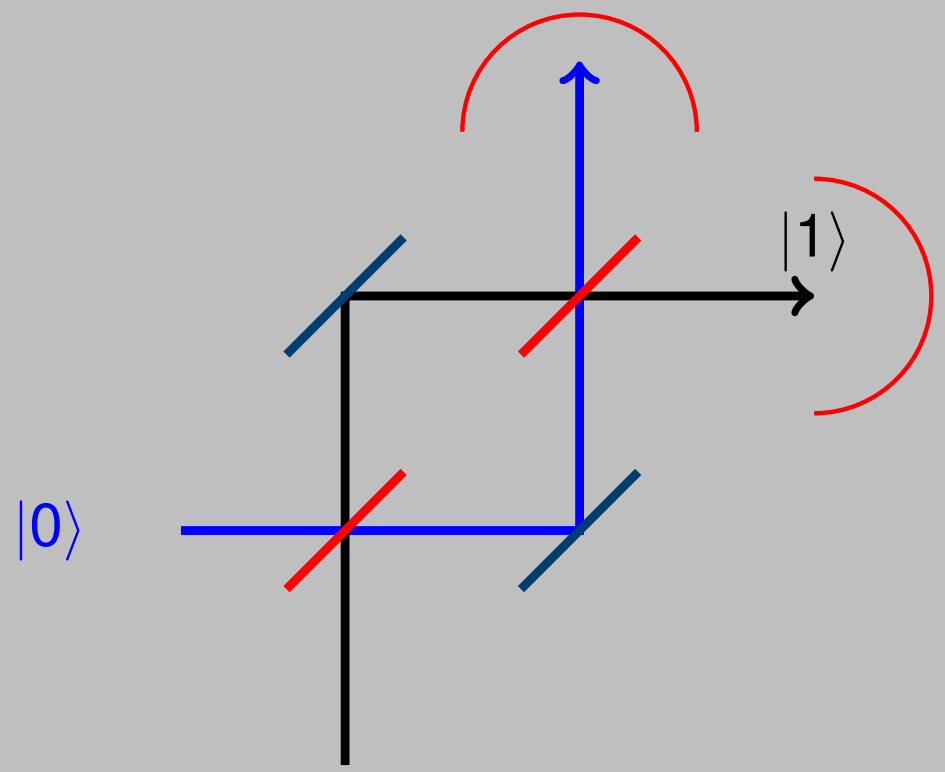
Quantum probabilities: emergent reality.

$$\underbrace{Prob(+) = 1}_{Reality} \Longrightarrow \underbrace{Prob(0) = 1/2, \quad Prob(1) = 1/2}_{emergent}$$

Interference

Superpositions are reversible

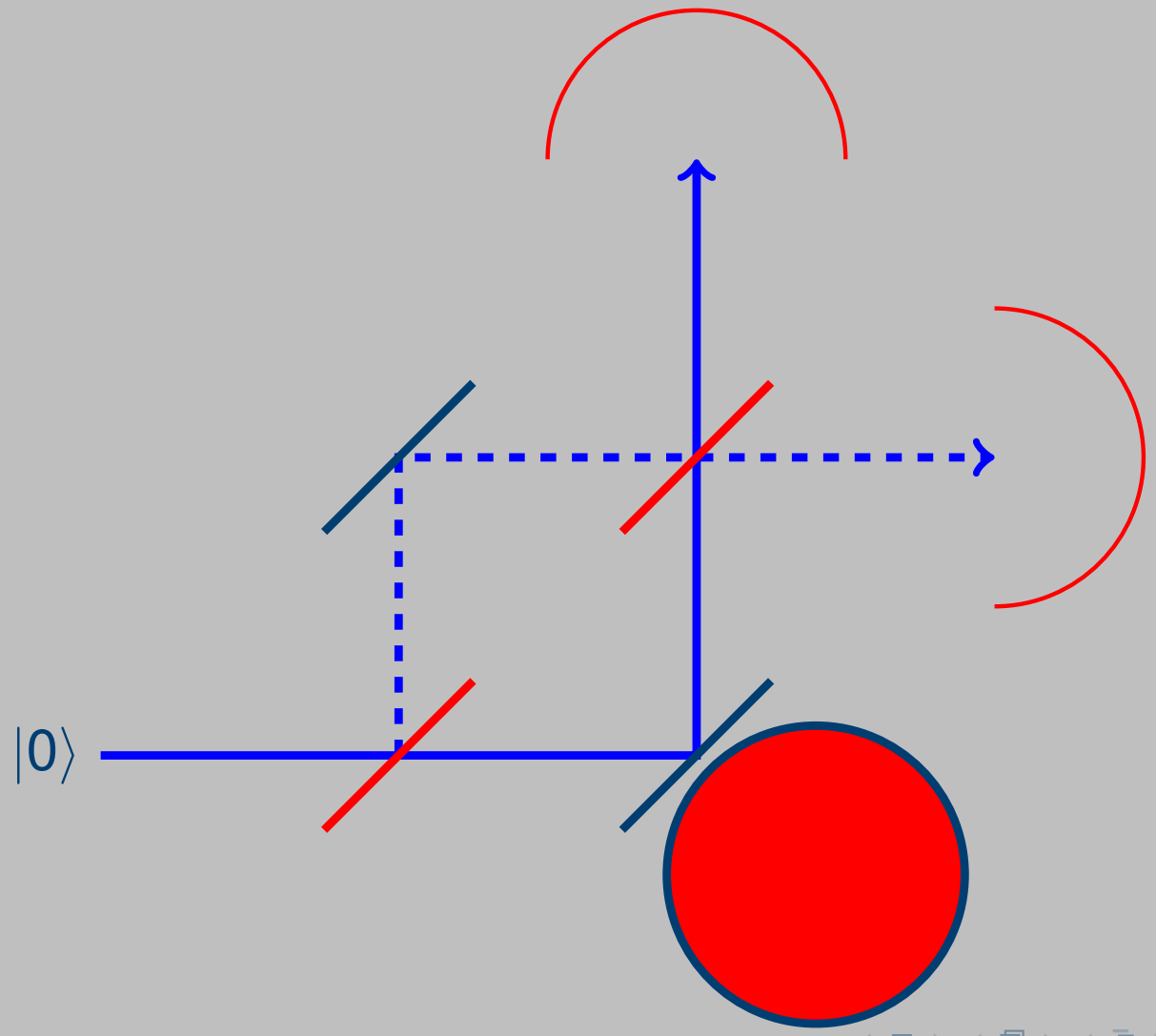
- $|0\rangle \mapsto |+\rangle \mapsto |1\rangle$
- $|1\rangle \mapsto |-\rangle \mapsto |0\rangle$



$$|0\rangle \mapsto |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \mapsto \frac{(-|0\rangle + |1\rangle) + (|0\rangle + |1\rangle)}{2} = |1\rangle$$

Vaidman Elitzur Bomb

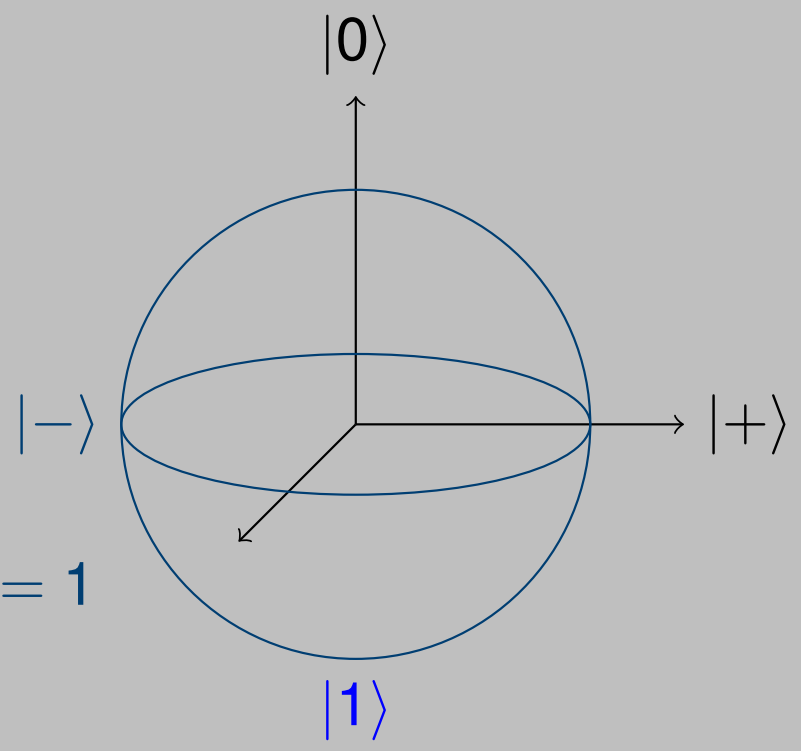
Action at a distance



Qubit

Bloch sphere

- $|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$
- $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$



Probabilistic logical bits

$$Prob(0||\psi\rangle) = |\alpha|^2, \quad Prob(1||\psi\rangle) = |\beta|^2$$

Quantum circuit

Hadamard gate

- $|0\rangle$ —— $\boxed{H}$ —— $|+\rangle$
- $|1\rangle$ —— $\boxed{H}$ —— $|-\rangle$

$|0\rangle$ —— $\boxed{H}$ —— $|+\rangle$

$|0\rangle$ —— $\boxed{H}$ —— $|+\rangle$

$|0\rangle$ —— $\boxed{H}$ —— $|+\rangle$

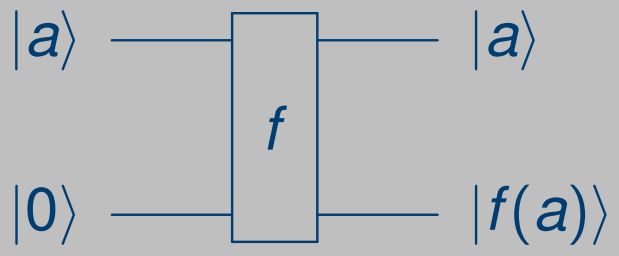
Massive parallelism

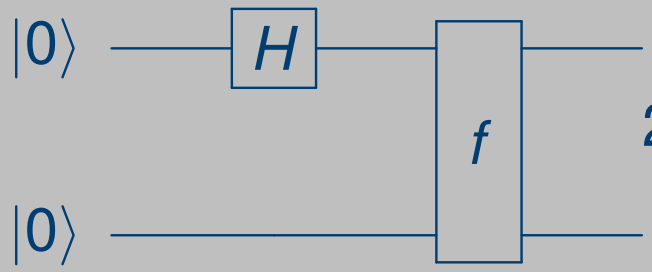
$$|+\rangle \otimes |+\rangle \otimes |+\rangle = \frac{|000\rangle + |001\rangle + \cdots + |110\rangle + |111\rangle}{2^{3/2}}$$

Function gate

Massive parallelism alone is useless

- Binary function: $a \in \mathbb{Z}_2$
- $f : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$
- General function: $a \in \mathbb{Z}_2^n$
- $f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^n$





$$2^{-n/2} \sum_a |a\rangle \otimes |f(a)\rangle \to |a\rangle \otimes |f(a)\rangle$$

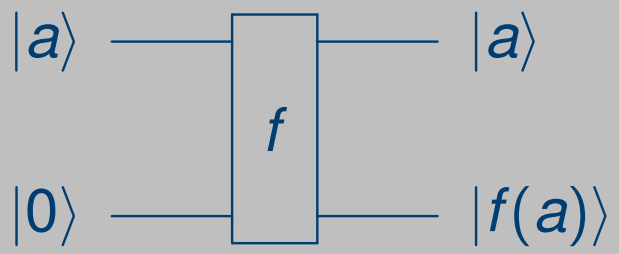
Readout: Picks a single term, randomly

Parity of binary function

Constant and odd functions

- Binary function $f : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$
- Const: $f(0) = f(1)$
- Odd: $f(0) \neq f(1)$
- Parity

$$\pi(f) = f(0) + f(1) \mod 2$$



Parity: A global property of f

$$\pi(f) = \begin{cases} 0 & \text{f=const} \\ 1 & \text{f= odd} \end{cases}$$

Deutsch task

Determine the parity $\pi(f)$

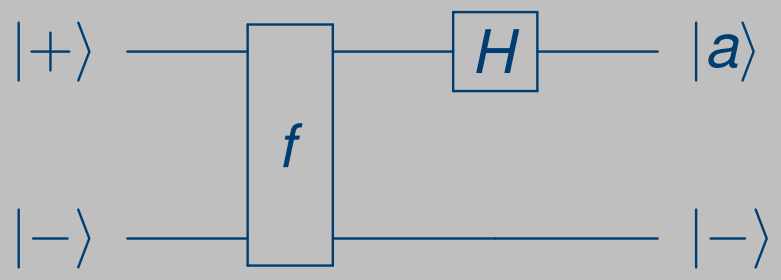
- Need to query the oracle twice
- $|0\rangle$ —— $\boxed{f}$ —— $|f(0)\rangle$
- $|1\rangle$ —— $\boxed{f}$ —— $|f(1)\rangle$

Classical parity algortihm

Needs two evaluations of f

Deutsch algoritm

Determines parity of f with a single query

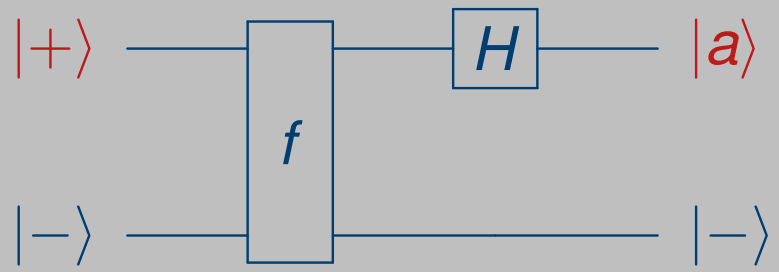


Measure $|a\rangle$

$$\pi(f) = a$$

Deutsch algoritm

Computation



$$
\begin{aligned}
|+\rangle \otimes |-\rangle &\propto |00\rangle - |01\rangle + |10\rangle - |11\rangle \\
&\xrightarrow{f} |0\rangle\Big(|f(0)\rangle - |f(0)\oplus 1\rangle\Big) + |1\rangle\Big(|f(1)\rangle - |f(1)\oplus 1\rangle\Big) \\
&\propto (-)^{f(0)}|0\rangle|-\rangle + (-)^{f(1)}|1\rangle|-\rangle \\
&\propto \Big(|0\rangle + (-)^{\pi}|1\rangle\Big)|-\rangle \\
&\propto \Big|(-)^{\pi(f)}\Big\rangle|-\rangle \\
&\xrightarrow{H} |\pi(f)\rangle|-\rangle
\end{aligned}
$$

Shor and Grover algoritms

- Shor: Factors n digits integers in $Poly(n)$
- Grover: Search an unstructured data base with n entries in time $O(\sqrt{n})$.

Successful quantum algorithms rely on

- Superposition: Create massive parallelism to explore all possible inputs simultaneously
- Interference: Manipulate quantum data to increase probability of desired outcome

References

- M. Nielsen and I. Chuang (Mike & Ike)
- Quantum Computing for Computer Scientists (YouTube)