Should biologists care about Quantum Computing

- The need
- QM is different
- Elements of QI
- Qubit is 2 bits
- Classical searches
- Grover search algorithm
- State manipulations

The need

If you are a:

- Physicist: Test QCD, Design materials for high Tc
- Chemist: Design large molecules, drugs
- Biologist: Simulate DNA, evolution

The obstacle:

76 quantum spins: matrices of Avogadro size

- Computer Scientist: Break RSA, new computing paradigm

QM is different

Two roads diverged in a yellow wood,
And sorry I could not travel both
And be one traveler, long I stood
And looked down one as far as I could
To where it bent in the undergrowth;

I shall be telling this with a sigh
Somewhere ages and ages hence:
two roads diverged in a wood, and I --
I took the one less traveled by,
And that has made all the difference
(R. Frost)

Quantum mechanics is like Yogi Berra

If you come to a fork in the road, take it

What we got used to

- A new fundamental constant: Planck $\frac{\hbar}{k_B} = 7.6 \times 10^{-12}\,[s \times K]$
- Discrete energy levels
- Tunneling
- Simple wave functions

$$a^*(x_1) \ldots a^*(x_n)\,|0\rangle$$

Properties of QM that have analogs in classical wave equations:

- Eignemodes of drums and strings, waveguides
- Interference
- Evanescent waves

What we still need to get used to

- Schrodinger: Not a wave equation in configuration space

$$\psi(\vec{x}_1, \vec{x}_2, \vec{x}_3, t), \quad \vec{E}(\vec{x}, t)$$

- Entanglement and unreasonable correlations

- The huge size of Hilbert space

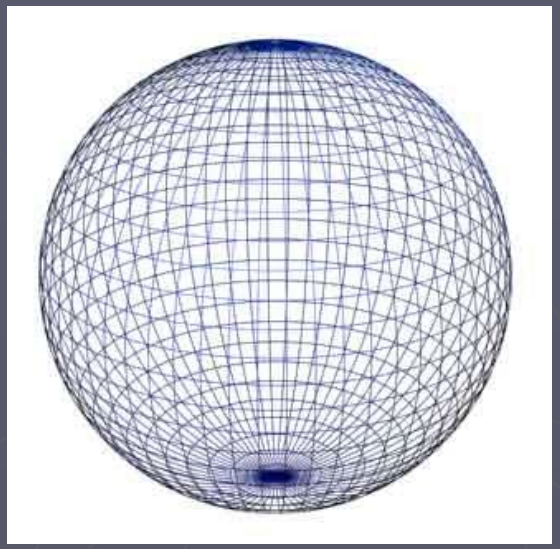
$$\dim [Hilbert] = 2^n$$

- The wave function collapse

- Decoherence

Qubit: Bloch sphere

$$|\psi\rangle = \cos\theta\,|0\rangle + e^{i\phi}\sin\theta\,|1\rangle$$



coordinates on a sphere

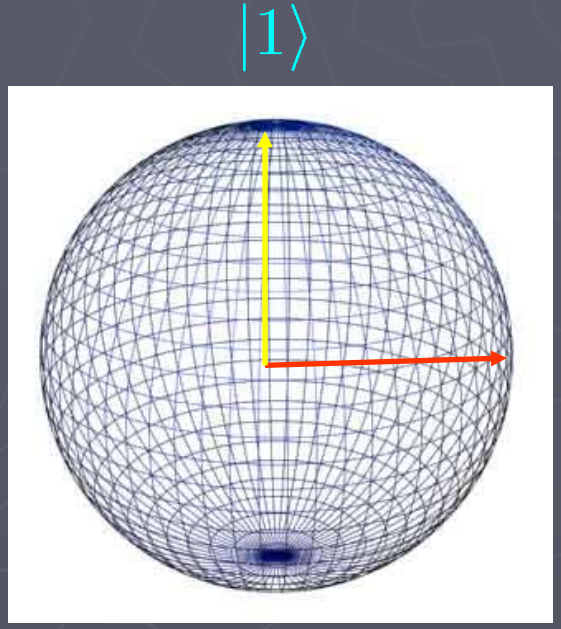
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

Operations

Rotation of Bloch sphere; Unitary maps

Example:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$



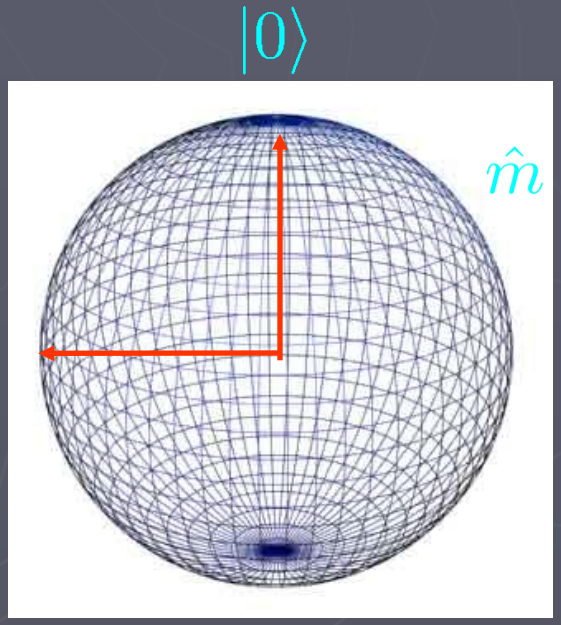
Circuit: Gate

Interrogation

Qubits can't always be trusted

Prepare the state: $|0\rangle$

Interrogate: Are you $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

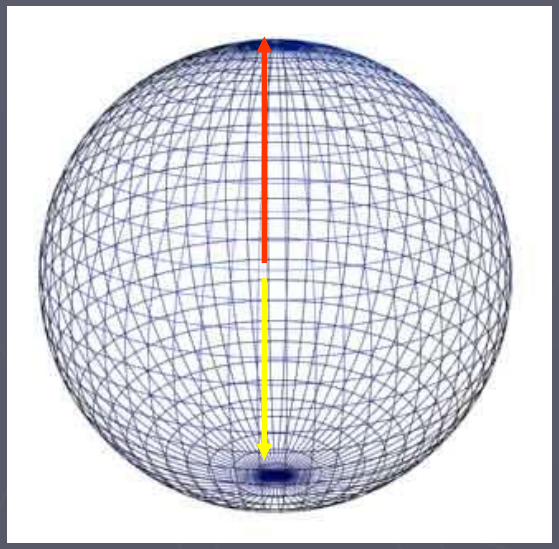


You'll get **yes** with probability

$$\cos^2(\theta/2) = \frac{1}{2}$$

Lying can be an advantage!

Truthful qubits



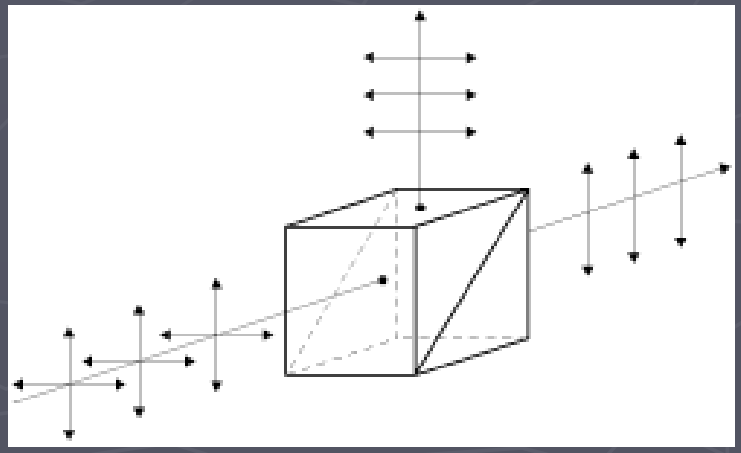
Dichotomic discrimination between 2 states

$$|0\rangle\,,|1\rangle$$

Orthogonal states are reliable

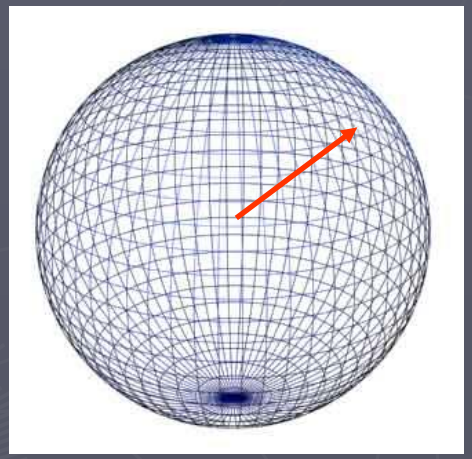
$$|\langle 0|0\rangle|^2 = |\langle 1|1\rangle|^2 = 1, \quad |\langle 0|1\rangle|^2 = 0$$

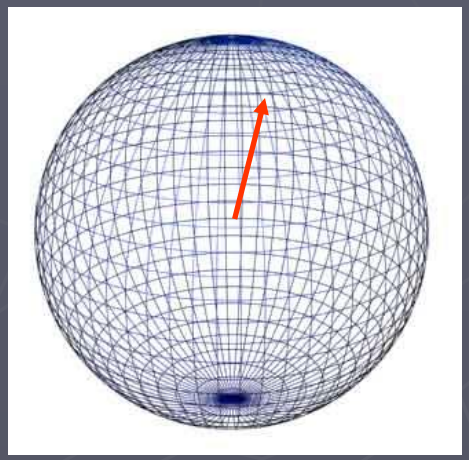
Example: Polarized Beam splitter
Distinguish reliably H from V



2 Qubits without correlations

$$|\psi\rangle = |\phi_a\rangle \otimes |\phi_b\rangle$$





Example

$$|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

With correlations: Entangled states

An entangled state: One that has no product form

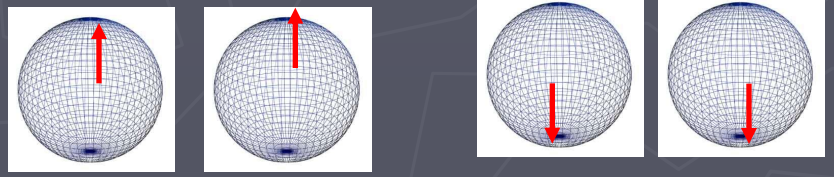
(Not represented by 2 Bloch spheres)

Example: Bell states

$$\sqrt{2}\ \left|\beta_{1,2}\right\rangle = |0\rangle \otimes |0\rangle \pm |1\rangle \otimes |1\rangle$$

$$\neq |\phi_a\rangle \otimes |\phi_b\rangle$$

Shadows



(2-qubits are not quite 4 Bloch spheres)

Two qubits Hilbert space

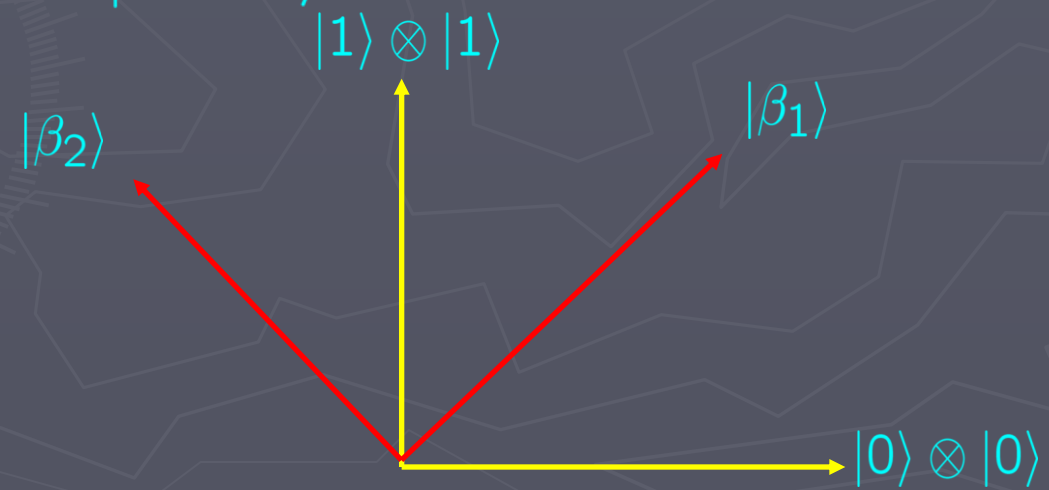
Space of states spanned by 4 reliable product states

$$|0\rangle \otimes |0\rangle\,, \quad |0\rangle \otimes |1\rangle\,, \quad |1\rangle \otimes |0\rangle\,, \quad |1\rangle \otimes |1\rangle$$

Space of states spanned by 4 reliable Bell states

$$\sqrt{2}\ \left|\beta_{1,2}\right\rangle = |0\rangle \otimes |0\rangle \pm |1\rangle \otimes |1\rangle$$

$$\sqrt{2}\ \left|\beta_{3,4}\right\rangle = |0\rangle \otimes |1\rangle \pm |1\rangle \otimes |0\rangle$$

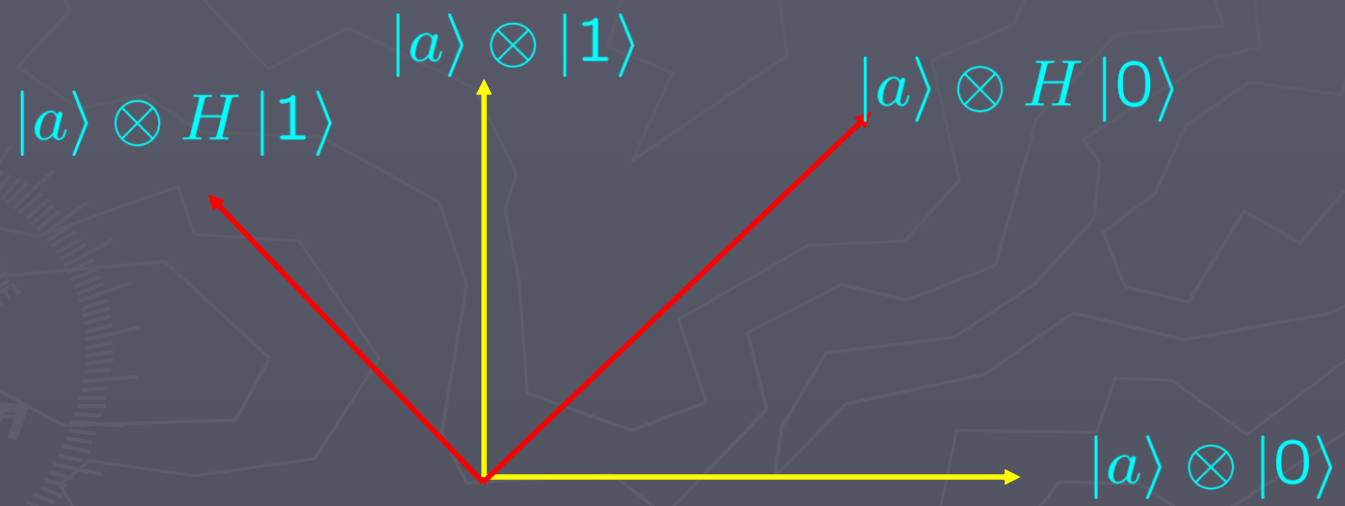


Local operations

Bob control only his qubit (can rotate his Bloch sphere)

$$|a\rangle_A \otimes |b\rangle_B \rightarrow |a\rangle_A \otimes H\,|b\rangle_B$$

Bob can rotate yellow to red



Bob cant rotate Alice's qubit: Half control

Entaglement is non-local

Neither Alice nor Bob can prepare a Bell state
from a product state by local operations
even if they choreograph anything they do

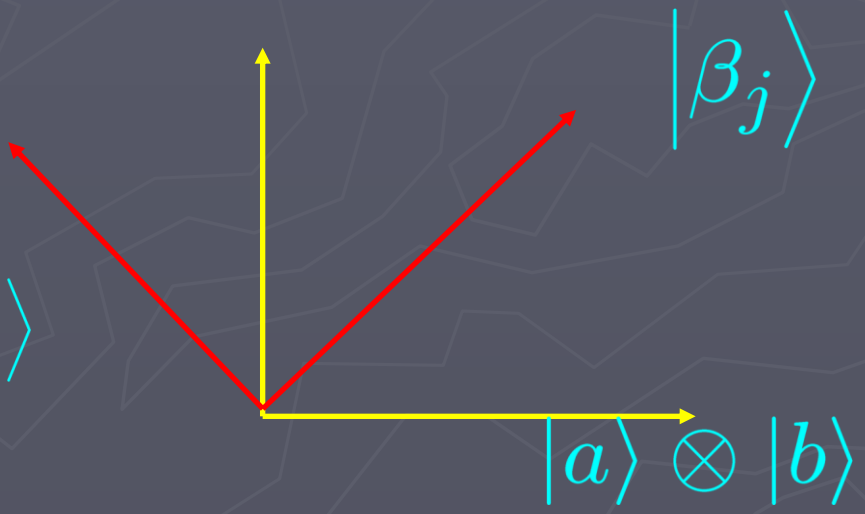
Entanglement requires the two qubits
To be localized in the same region and interact

Enhanced control

Bob can permute all the Bell basis:

$$1_A \otimes (\sigma_x)_B \left|\beta_{1,2}\right\rangle = \left|\beta_{3,4}\right\rangle$$

$$1_A \otimes (\sigma_z)_B \left|\beta_{1,3}\right\rangle = \left|\beta_{2,4}\right\rangle$$



Qubit =2 bits (Dense coding)

If Alice & Bob share a Bell state then
Bob's qubit is worth 2-bits

- Alice and Bob share $|\beta_1\rangle$
- Bob makes a local operation changing $|\beta_1\rangle \rightarrow |\beta_j\rangle$
- Bob send his qubit to Alice
- Alice reliably distinguishes the new Bell state $j \in 1, 2, 3, 4$

1 qubit is worth 2 bits

N qubits

$$|\psi\rangle = \sum \alpha_{a\ldots b} |a\rangle_A \otimes \ldots |b\rangle_B \qquad a, b \in 0, 1,$$

2^N complex amplitudes

Discounting normalization and phase: 2^N-2 real numbers.

N Bloch spheres: 2N real numbers

Exponentially more information in qubits

Computational basis

n qubits span a Hilbert space with huge dimension

$$N = 2^n$$

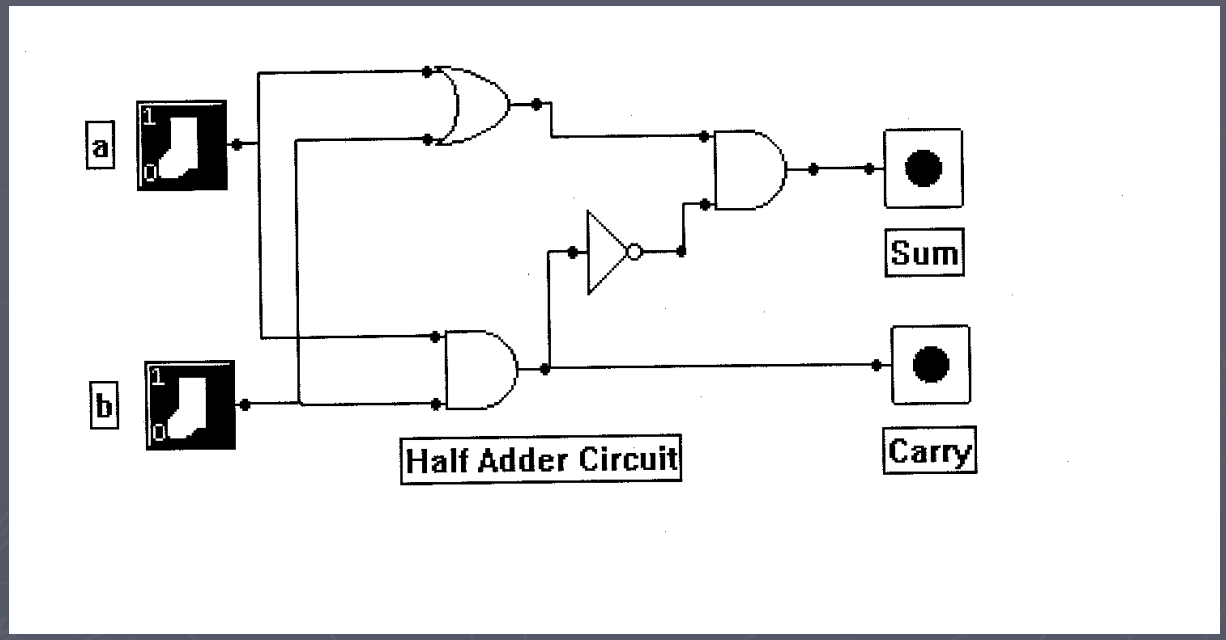
Binary representation of integers

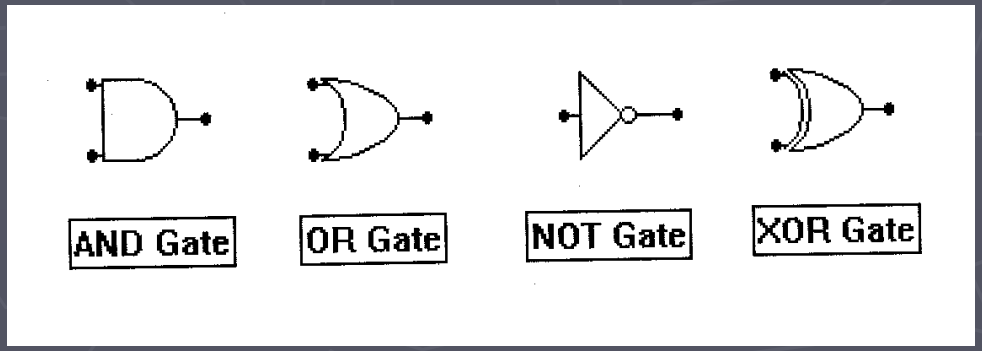
$$5 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 101$$

A representation of *computational basis*

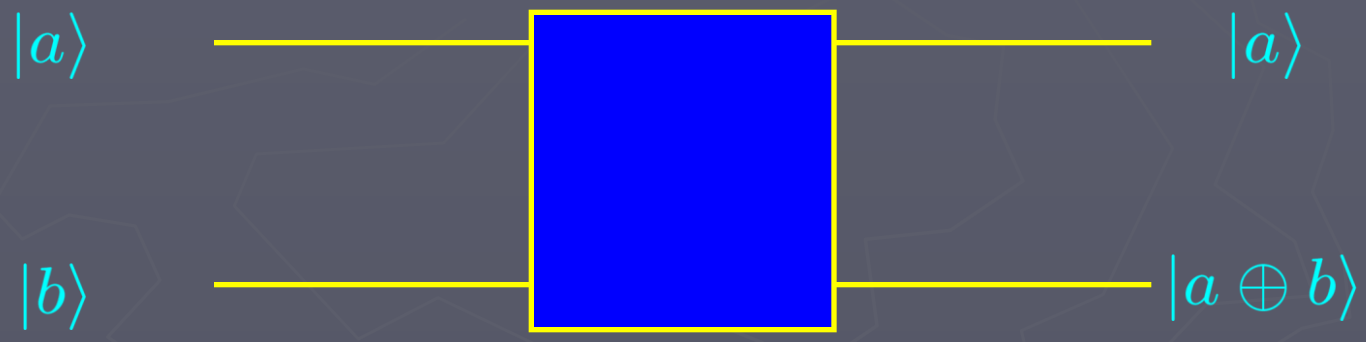
$$|5\rangle = |101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$$

Classical computer





Quantum computer



If input a superposition output is a superposition

$$\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|01\rangle \rightarrow \frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle$$

With probability 0.75 the output is

$$|11\rangle$$

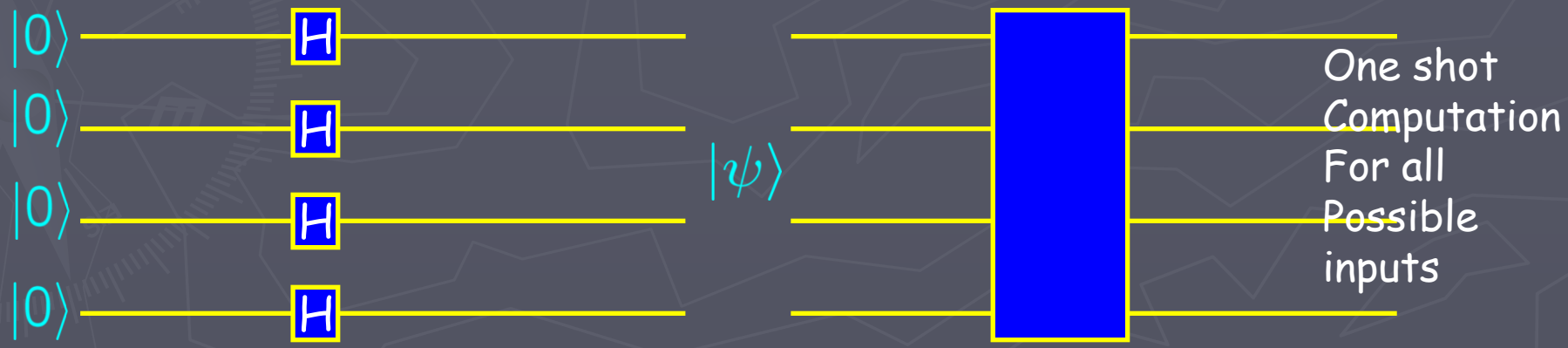
Massive parallelism

A state is product or huge superposition depends on basis

$$|\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \ldots = \frac{1}{\sqrt{N}} \sum |k\rangle$$

Huge superposition translates to massive parallelism

A circuit implementing $|0\rangle \rightarrow |\psi\rangle$

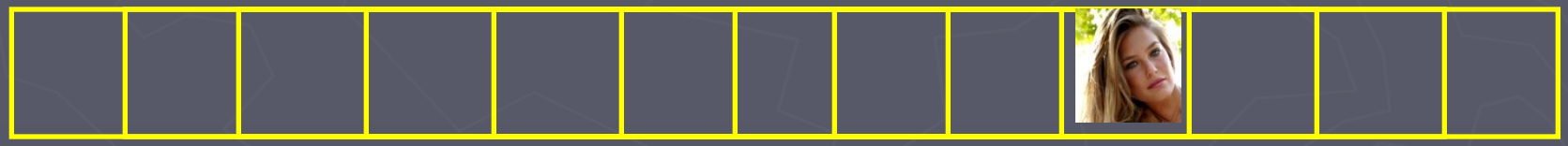


Searching

Find Bar Rephaeli in LA phone book with *million* entries

Need $\log_2 10^6 \sim 20$ *divide and conquer*

Very efficient



Find the person whose number is `` 626-375-5074 ``
in LA phone book

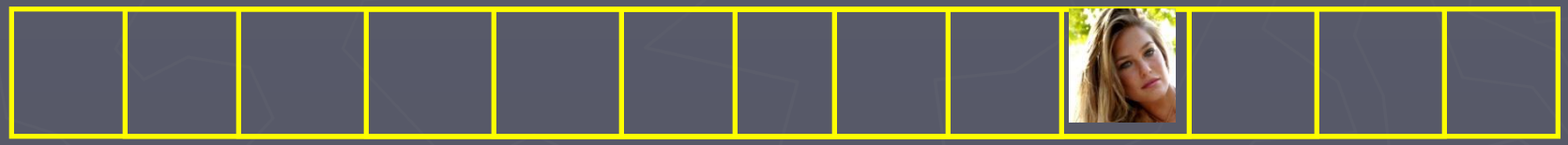
Need about million operations: linear search

Very inefficient

Quantum search does it in *thousand operations*

Searching & Oracles

An oracle, (a phone book),
tell you if answer is correct



$$f(k) = \begin{cases} 0, & k \neq R; \\ 1, & k = R. \end{cases}$$

Function is easy to compute: You guess the name and use phone book to check quickly the guess

626-375-5074 is Bar Refaeli number-Wrong,
f(refaeli== 626-375-5074)=0

Quantum Oracle

The Oracle marks the answer with a phase:

$$G\,|k\rangle = (-1)^{f(k)}\,|k\rangle$$

The second idea: Use massive parallelism

$$G\,|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{1}^{N}(-1)^{f(k)}\,|k\rangle$$

We have now computed f for million entries
With 1 query of the phone book.

Key observation

The fully mixed state has a large overlap with the solution

$$\langle R|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{1}^{N} \langle R|k\rangle = \frac{1}{\sqrt{N}}$$

Amplitudes are larger that the probabilities

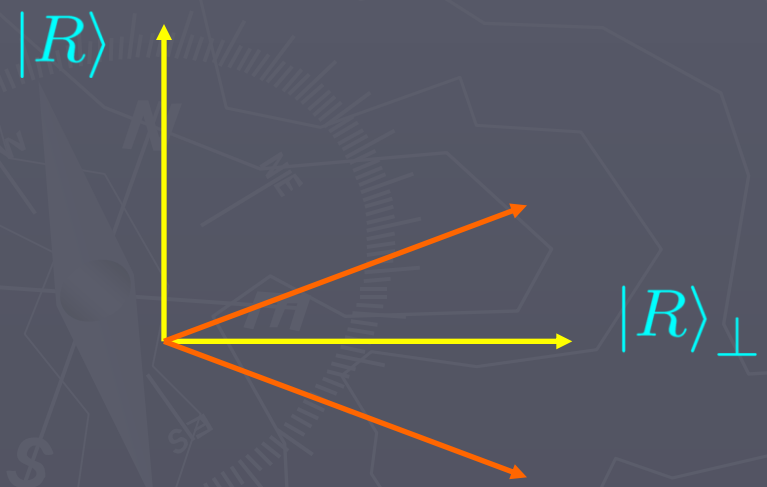
Doubling the amplitude- Constructive interference- quadruple the probability

Grover as a reflection

If K denotes the solution we can write the oracle as

$$G = 1 - 2\,|R\rangle\,\langle R|$$

(We are given the oracle, a black box, not K)

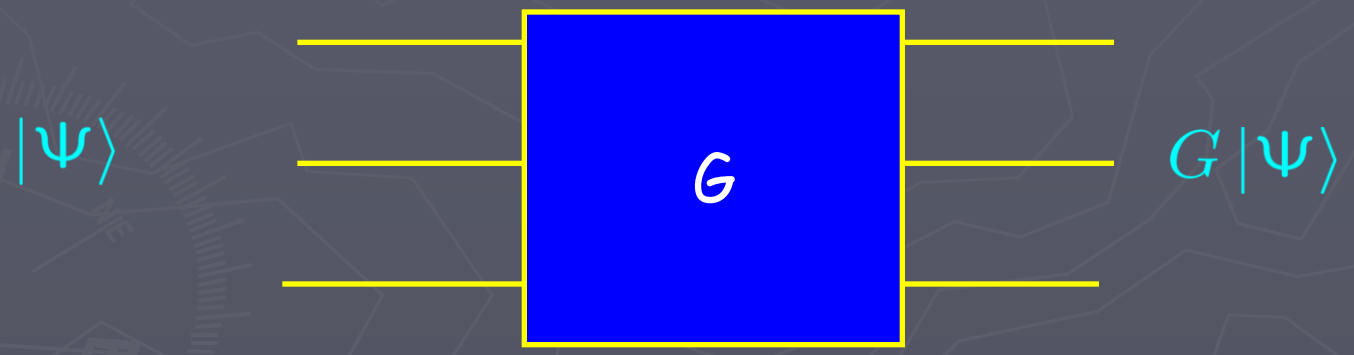


The oracel is a reflection

$$G^2 = 1 - 4\,|R\rangle\,\langle R| + 4\,|R\rangle\,\langle R|R\rangle\,\langle R| = 1$$

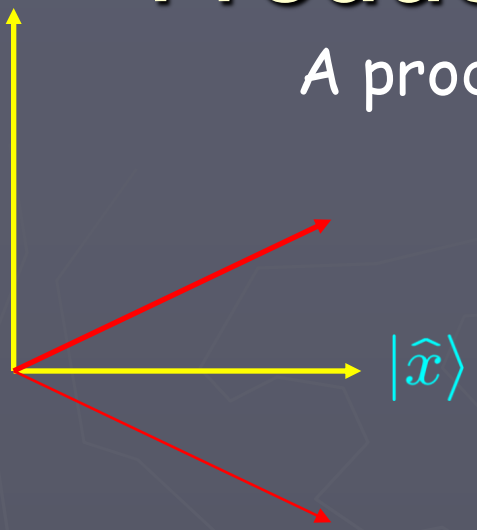
The oracle: black box

$$G = 1 - 2\,|R\rangle\,\langle R|$$

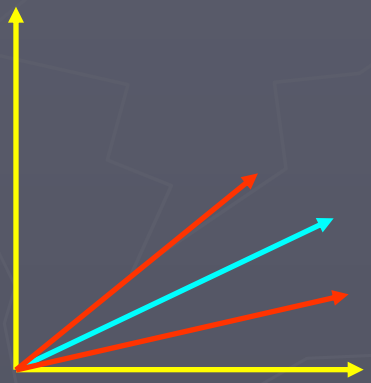


Product of reflections=Rotation

A product of two reflections is a rotation



$$R = 2\,|\hat{x}\rangle\,\langle\hat{x}| - 1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



$$G = -1+2\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}(\cos\theta, \sin\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

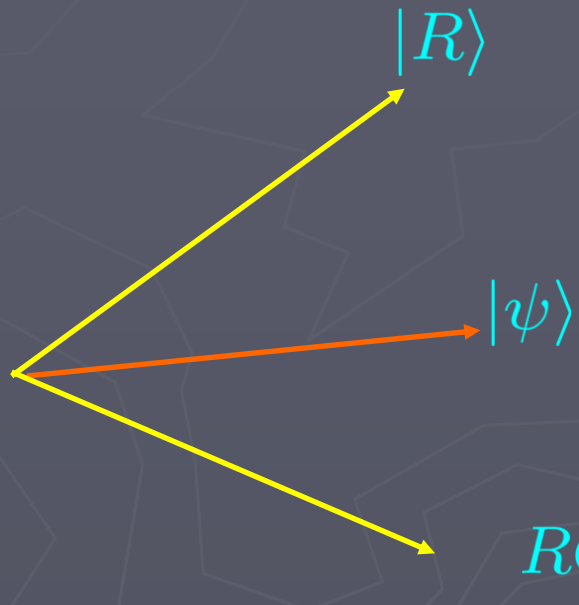
$$RG = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}$$

Rotation

Grover Rotation

A product of two reflections is a rotation

$$-R = 2\,|\psi\rangle\,\langle\psi| - 1, \qquad -G = 2\,|R\rangle\,\langle R| - 1$$

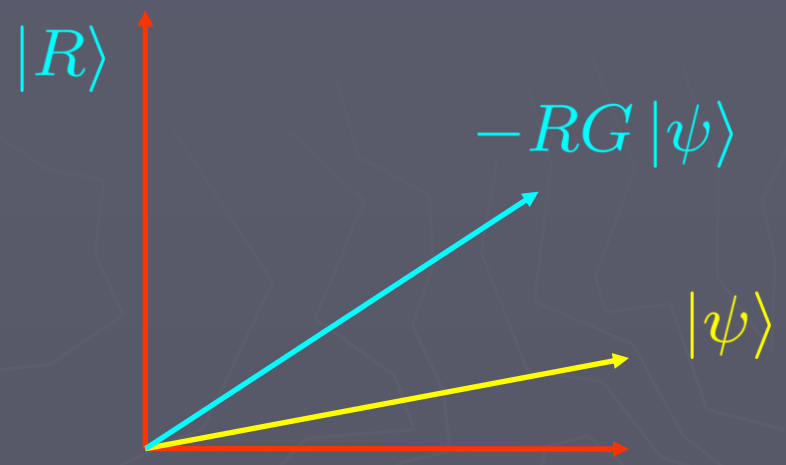


RG a rotation by $2\arccos\langle\psi|R\rangle$

$$2\arccos\left(\frac{1}{\sqrt{N}}\right) \approx 2\left(\frac{\pi}{2} - \frac{1}{\sqrt{N}}\right) = \pi - \frac{2}{\sqrt{N}}$$

Grover search algorithm

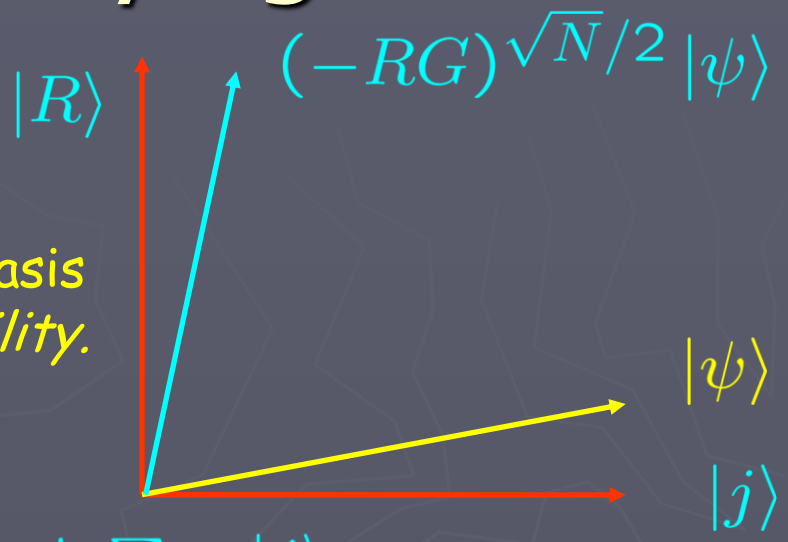
$-RG$ rotatets by $\frac{2}{\sqrt{N}}$



After $\frac{\sqrt{N}}{2}$ iterations you are close to the target

The benefit of lying

Interrogate all the qubits in computational basis you get the *precise* answer with *high probability.*



$$(-RG)^{\sqrt{N}/2}|\psi\rangle = (1-\epsilon)|R\rangle + \sum \epsilon_j |j\rangle$$

$$\sum |\epsilon_j|^2 = 2\epsilon$$

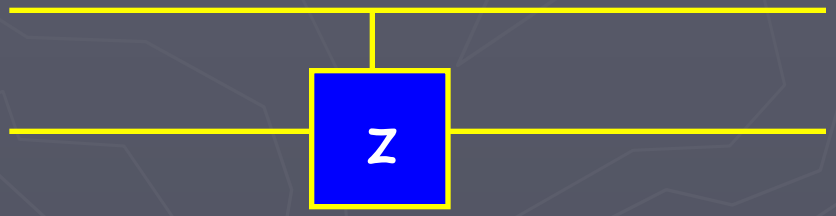
If all errors are equally probable, the probability of any one error is ridiculously small

$$|\epsilon_j|^2 = \frac{2\epsilon}{N}$$

Need to build

$$R = 1 - 2\,|\psi\rangle\,\langle\psi|$$

Example for $|\psi\rangle = |11\rangle$



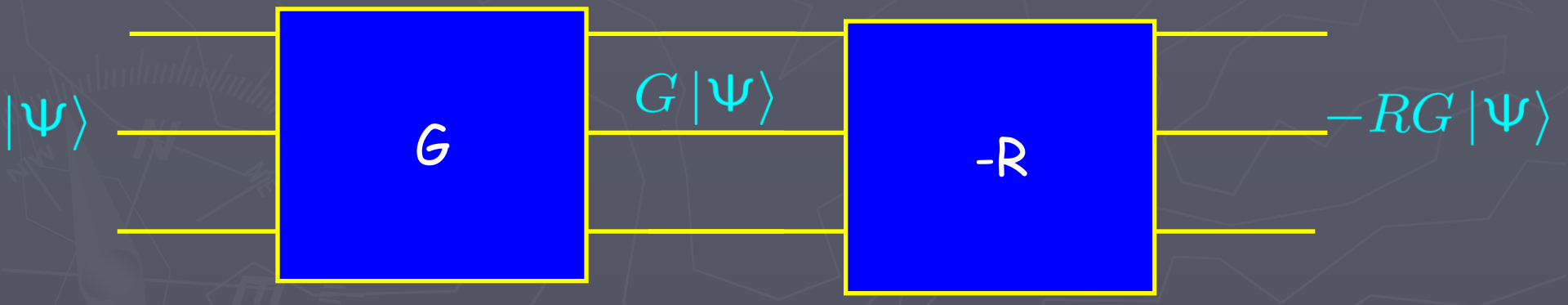
CZ gate

$$|ab\rangle \rightarrow (-1)^{ab}\,|ab\rangle$$

The Grover machine

The reflection G is given by the black box

-R is a reflection about a known state, that you build



Concatenate $N^{1/2}$ times

Energy uncertainty=Angular velocity

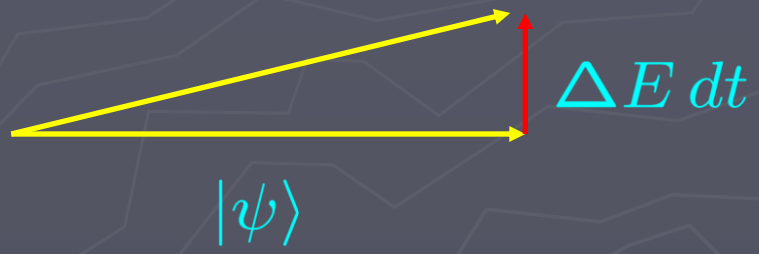
(S. Hillel)

$$i\hbar|\dot{\psi}\rangle = H\,|\psi\rangle$$

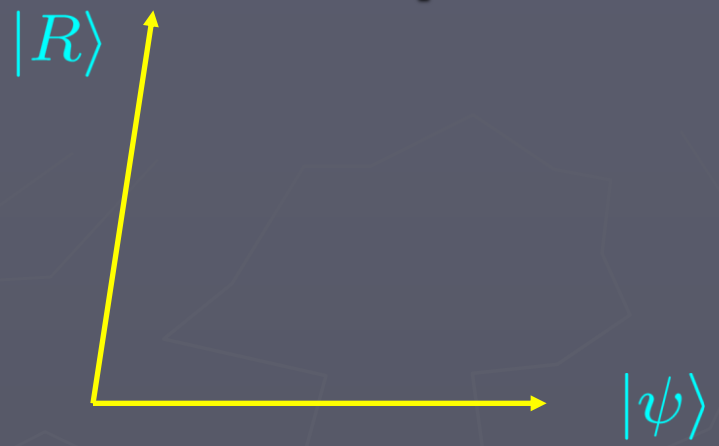
$$\Delta E^2 = \langle\psi|\,H^2|\psi\rangle - (\langle\psi|\,H|\psi\rangle)^2$$

$$\Delta E = \hbar\left\|(1 - |\psi\rangle\,\langle\psi|\,)\,\left|\dot{\psi}\right\rangle\right\|$$

Angular velocity



State manipulation



How long does it take to evolve a state to an orthogonal state?

$$\Delta E \, dt \geq \frac{h}{4}$$

$$\Delta E \propto |\langle \psi | R \rangle| = \frac{1}{\sqrt{N}}$$

Should biologists care about QM?