Let's say we have a function

$$f : \{0, \ldots, N-1\} \longrightarrow \{0, 1\}$$

such that there is a unique w such that $f(w) = 1$.

Problem: Write an algorithm to find w given f.

E.g. Solutions to a sudoku, finding a prime factor of a composite number

Classically, we would need to call f $N-1$ times to be sure we have found w. If we only want a 50% chance of finding w, then we would need to call f $\frac{N}{2}$ times.

Always need $O(N)$ calls to f

to get to w.

But with a quantum algorithm we can get a 50% chance of finding w using only $\mathcal{O}(\sqrt{N})$ calls to f.

Grover's algorithm

- We encode f using a Grover oracle U_w

U_w is a unitary gate satisfying

$$U_w: |k\rangle \mapsto \begin{cases} |k\rangle & \text{if } f(k)=0 \\ -|k\rangle & \text{if } f(k)=1 \\ & (k=w) \end{cases}$$

(not every problem encodes efficiently this way, but some do)

1. Put your system into the state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

(an equal superposition of every basis vector)

If our initial state is $|0^n\rangle$,
then applying $\boxed{H}$ to every qubit
will cause the state to become $|s\rangle$

2. Define $U_s = 2|s\rangle\langle s| - I$.

↑ the Grover diffusion operator

Apply $U_s U_\omega$ to the current state $\sim \frac{\pi}{8}\sqrt{N}$ times

3. Measure relative to the standard basis

I claim: If this algorithm is performed, then the chance that the output will be $|w\rangle$ is at least 50%.

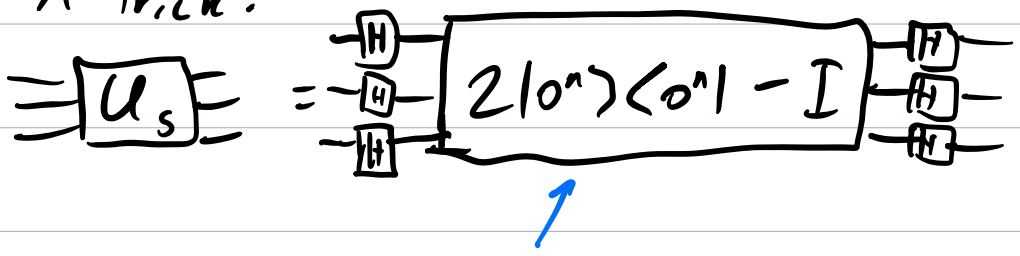
So we keep running til we get the right answer (most likely on the first or second try).

To see why this works, here's a problem.

So Grover's algorithm works because quantum circuits can efficiently implement reflection operators, which can be composed into rotation operators, which can bring

A generic state close to a desired state.

A trick:



$|0^n\rangle \mapsto |0^n\rangle$

$|k\rangle \mapsto -|k\rangle \quad k \neq 0$

Ex: Using $U_w = CZ$

which is a Grover oracle

on 2-qubits for which $w = 3$

$|w\rangle = |11\rangle$

Adjoint operators

Goal: Construct orthogonal decomposition from the eigenspaces of "nice"

linear operators.

To describe what makes an operator nice, we need to introduce adjoint operators.

Def: Let L be a linear operator on an inner product space V. We say that an operator L^* on V is an **adjoint** of L if

$$\langle Lv, w \rangle = \langle v, L^* w \rangle$$

for all $v, w \in V$.

Thm: Any operator L on $\mathbb{C}^n$ has a unique adjoint L^*.

If M is the matrix for L in an orthonormal basis,

then $M^\dagger$ = the Hermitian adjoint of M = conjugate transpose of M

is the matrix for L^* in that basis.

Lemma: The assignment $L \mapsto L^*$ has the following properties

a) $L^{**} = L$

b) $(L_1 L_2)^* = L_2^* L_1^*$

c) $(\lambda L)^* = \lambda^* L^*$

d) $(|v\rangle\langle w|)^* = |w\rangle\langle v|$

e) $(L_1 + L_2)^* = L_1^* + L_2^*$

Pf: We'll show (b).

WTS that $L_2^* L_1^*$ is an adjoint of $L_1 L_2$

$$\langle v, L_2^*(L_1^* w)\rangle \overset{\text{WTS}}{=} \langle L_1 L_2 v, w\rangle$$

$$= \langle L_2 v, L_1^* w\rangle$$

$$= \langle L_1 L_2 v, w\rangle \quad \checkmark$$

Def: A **unitary map** between inner product spaces V and W is a linear map U which preserves inner products and is surjective.

If we drop the surjectivity requirement, we get an **isometry** from V to W.
Isometries are always injective, so **unitary maps are always bijective** (isomorphisms).

Any isometry on $\mathbb{C}^n$ is a unitary operator, so that definition is unchanged.

Thm: An operator U on $\mathbb{C}^n$ is unitary iff $U^*U = UU^* = Id$.

In other words, U is invertible and

$$U^{-1} = U^*.$$

Thm: A projection operator Π on $\mathbb{C}^n$ is an orthogonal projection iff $\Pi^* = \Pi$.

Def: If an operator satisfies

$$L^* = L$$

then we say L is **self-adjoint.**

Def: An **eigenvector** of a linear operator L is a nonzero vector $|v\rangle$ such that

$$L|v\rangle = \lambda|v\rangle$$

for some scalar λ (the eigenvalue).

Def: A normal operator U is one such that

$$UU^* = U^*U$$

Thursday:

An operator is normal iff there is an orthonormal basis consisting of eigenvectors for the operator.

↑ The Spectral Theorem