4. Grover's algorithm

For many hard computational problems, it is possible to check a solution efficiently, but we don't know how to find it.

So-called "NP problems" (non-deterministic polynomial)

Many interesting problems are of this type:

- graph coloring
- factoring
- 3-SAT
- tiling problems
- Hamiltonian path
- travelling salesman (suitably phrased)

⋮

Reformulation of NP problems:

We have an efficiently computable function

$$f(x) \in \{0,1\} \; ; \quad x \in \{0,1,\dots,N-1\}$$

efficient =

— where $f(x)$ is a "verifier" for a given "solution" x,

i.e. $f(x)=1$ if & only if x is a correct solution —

and we want to find an x_0 s.th. $f(x_0)=1$

(i.e. a correct solution).

(Can be interpreted as "database search": Want to find a "marked element" x_0 in an unstructured database.)

We assume for now that $x_0 : f(x_0)=1$ is unique.

(Generalization: later/homework)

Classically: Will need $O(N)$ queries to f for an unstructured search (i.e., without using properties of f).

Quantumly: Will see that $O(\sqrt{N})$ queries are enough.

(<u>Note</u>: This is only a <u>quadratic speedup</u>, but it applies to a <u>very large class</u> of very relevant problems.)

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

$N = 2^n$: n qubits

<u>Ingredient 1</u>:

Oracle

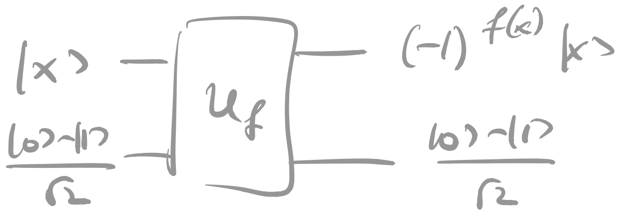
$$O_f : |x\rangle \longmapsto (-1)^{f(x)} |x\rangle = (-1)^{\delta_{x,x_0}} |x\rangle$$

i.e. O_f flips amplitude of "marked" element.

Can also write as

$$\boxed{O_f = I - 2|x_0\rangle\langle x_0|}$$

(<u>Note</u>: Can build O_f from U_f via phase kick-back technique:

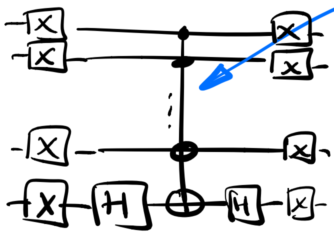


)

Ingredient 2:

Unitary $O_0 : |x\rangle \longmapsto (-1)^{\delta_{x,0}} |x\rangle$

n-qubit Toffoli!

Corresponds to  , or O_f, $f(x)=\delta_{x,0}$

$\longrightarrow$ can be realized efficiently.

Again, write $O_0 = I - 2|0\rangle\langle 0|$

Define

$$\boxed{O_\omega := H^{\otimes n} O_0 H^{\otimes n} = I - 2|\omega\rangle\langle\omega|},$$

with $|\omega\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.

Grover's algorithm:

① Start from $|\psi_0\rangle = |\omega\rangle = H^{\otimes n}|0\rangle$

② Repeat: Apply Grover iteration

$$G = -H^{\otimes n} O_0 H^{\otimes n} O_f = (-O_\omega) O_f$$

$$|\psi_k\rangle \xmapsto{G} |\psi_{k+1}\rangle = G|\psi_k\rangle = (-O_\omega)O_f|\psi_k\rangle.$$

(How many times? — Soon!)

How to analyze "trajectory" $|\psi_0\rangle \to |\psi_1\rangle \to |\psi_2\rangle \to \dots$?

<u>Recall</u>: $O_f = I - 2|x_0\rangle\langle x_0|$

$-O_\omega = 2|\omega\rangle\langle\omega| - I$

and moreover, $|\psi_0\rangle = |\omega\rangle$.

$\Longrightarrow$ Only two <u>special vectors</u> in $|\psi_0\rangle, O_f, -O_\omega$: $|x_0\rangle$ and $|\omega\rangle$. The identity I will not change these vectors.

$\Longrightarrow$ The dynamics $|\psi_0\rangle \to |\psi_1\rangle \to |\psi_2\rangle \to \dots$ takes place in span$\{|x_0\rangle, |\omega\rangle\}$, i.e., a two-dimensional space!

Two natural ONBs for this space:

$$|x_0\rangle$$

$$|x_0^\perp\rangle := \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle \propto |\omega\rangle - |x_0\rangle \underbrace{\langle x_0|\omega\rangle}_{=1/\sqrt{N}}$$

$$\left.\right\} \langle x_0|x_0^\perp\rangle = 0$$

And another basis

$|\omega\rangle$

$|\omega^\perp\rangle$ with $\langle\omega|\omega^\perp\rangle = 0$

Of course, any vector in span$\{|x_0\rangle, |\omega\rangle\}$ can be expanded in either basis:

$$|\psi\rangle = a|x_0\rangle + b|x_0^\perp\rangle = x|\omega\rangle + y|\omega^\perp\rangle$$

What is the effect of O_f and $(-O_\omega)$ on $|\psi\rangle$?

$$O_f|\psi\rangle = O_f\left(a|x_0\rangle + b|x_0^\perp\rangle\right) \overset{?}{=} -a|x_0\rangle + b|x_0^\perp\rangle$$

$$O_f = I - 2|x_0\rangle\langle x_0|$$

$\Rightarrow$ <u>O_f reflects $|\psi\rangle$ about $|x_0^\perp\rangle$!</u>

$$(-O_\omega)|\psi\rangle = (-O_\omega)\left(x|\omega\rangle + y|\omega^\perp\rangle\right)$$

$$= -\left(-x|\omega\rangle + y|\omega^\perp\rangle\right) = x|\omega\rangle - y|\omega^\perp\rangle.$$

$O_\omega = I - 2|\omega\rangle\langle\omega|$

$\Rightarrow$ <u>$(-O_\omega)$ reflects $|\psi\rangle$ about $|\omega\rangle$!</u>

<u>Thus</u>: each Grover iteration consists of two steps:

(i) reflect about $|x_0^\perp\rangle$

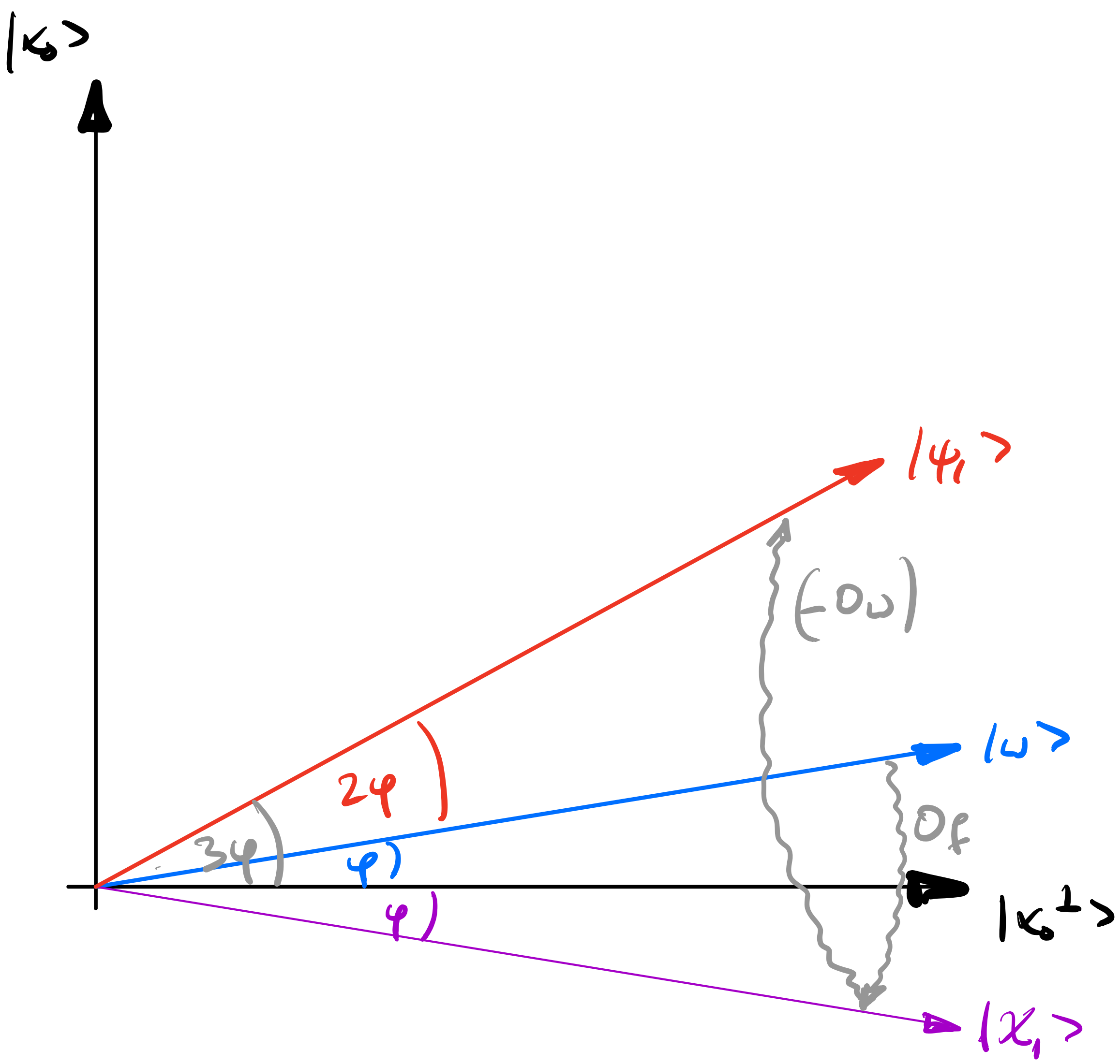
(ii) reflect about $|\omega\rangle$

What happens now if we start with $|\psi_0\rangle = |\omega\rangle$ and apply one iteration?

$$|\omega\rangle = \sin\varphi\,|x_0\rangle + \cos\varphi\,|x_0^\perp\rangle.$$

$$|\chi_1\rangle = O_f\,|\omega\rangle$$

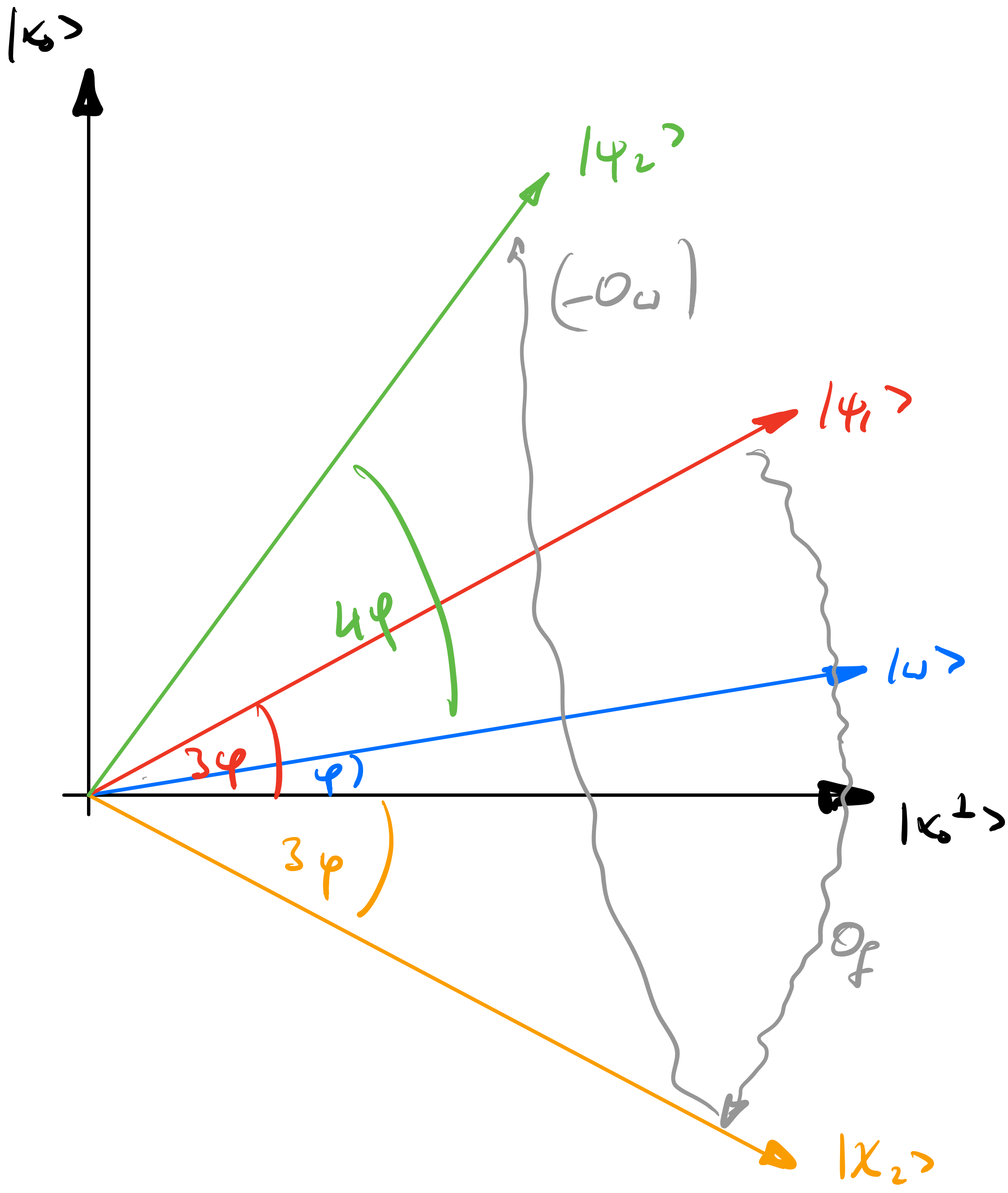
$$|\psi_1\rangle = (-O_\omega)\,|\chi_1\rangle = (-O_\omega)\,O_f\,|\omega\rangle$$



$$\Rightarrow \quad |\psi_1\rangle = \sin(3\varphi)\,|x_0\rangle + \cos(3\varphi)\,|x_0^\perp\rangle$$

Next Grover iteration:

$$|\psi_2\rangle = (-O_\omega)\,\underbrace{O_f\,|\psi_1\rangle}_{=:\,|\chi_2\rangle}$$



$$\Longrightarrow \quad |\psi_2\rangle = \sin(5\varphi)\,|x_0\rangle + \cos(5\varphi)\,|x_0^\perp\rangle$$

Can continue … !

$$\longrightarrow \quad |\psi_k\rangle = \sin\big((2k+1)\varphi\big)|x_0\rangle + \cos\big((2k+1)\varphi\big)|x_0^\perp\rangle$$

Want that $(2k+1)\varphi \approx \frac{\pi}{2}$: Then, measurement in comp. basis will return $|x_0\rangle$ with high prob.!

Since $|\omega\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}\,|x_0^\perp\rangle$

$$= \sin\varphi\,|x_0\rangle + \cos\varphi\,|x_0^\perp\rangle$$

$$\Rightarrow \quad \frac{\sin\varphi}{\cos\varphi} = \frac{\sqrt{\frac{1}{N}}}{\sqrt{\frac{N-1}{N}}} = \frac{1}{\sqrt{N-1}}$$

$\Rightarrow$ for large N, $\varphi \approx \frac{1}{\sqrt{N}}$.

$\Rightarrow$ Need $k \approx \frac{\pi}{4}\cdot\sqrt{N}$ Grover iterations.

$\Rightarrow$ $O(\sqrt{N})$ calls to f (for O_f) sufficient!

<u>Quadratic speed-up</u> with respect to classical algorithms for <u>general search problems</u>!

Note:

- If there are $K > 1$ solutions:

  Same method with $O\left(\sqrt{\frac{N}{K}}\right)$ steps works

  (→ homework)

- Can also be adapted to case where number of solutions is unknown.