

## 4. Cook'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 (markedly 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 =  
fast

— 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.t.  $f(x_0) = 1$   
(i.e. a correct solution).

(Can be interpreted as "database search": Want to  
find a "marked element"  $x_0$  in an un-  
structured 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 any properties  
of  $f$ ).

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

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

Consider  $f: \{0, \dots, N-1\} \rightarrow \{0, 1\}$   
 $\uparrow$   
 $N = 2^n$ : n qubits

Algorithm 1:

Oracle

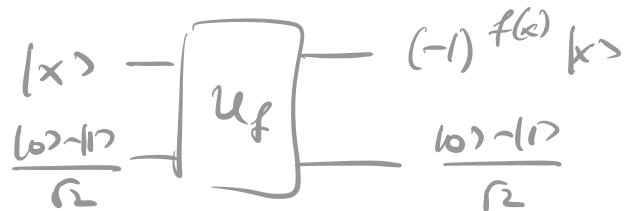
$$O_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle = (-1)^{\delta_{x,x_0}} |x\rangle$$

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

Can also write as

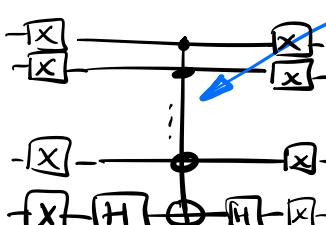
$$\boxed{O_f = I - 2|x_0\rangle\langle x_0|}$$

(Note: Can build  $O_f$  from  $U_f$  via  
phase kick-back technique:



Ingredient 2:

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

Corresponds to 

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

→ can be realized efficiently.

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

Define

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

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

Grover's algorithm:

① Start from  $|y_0\rangle = |\omega\rangle = H^{\otimes n} |0\rangle$

② Repeat: Apply Grover iteration

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

$$|\psi_k\rangle \xrightarrow{C} |\psi_{k+1}\rangle = C|\psi_k\rangle = (-D_\omega) O_f |\psi_k\rangle.$$

(How many times? — Soon!)

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

Recall:  $O_f = I - 2 |\psi_0\rangle\langle\psi_0|$

$$-D_\omega = 2(\omega X_\omega) - I$$

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

$\Rightarrow$  Only two special vectors in  $|\psi_0\rangle, O_f, -D_\omega$ :

$|\psi_0\rangle$  and  $|\omega\rangle$ . The identity  $I$  will

not change those vectors.

$\Rightarrow$  The dynamics  $|\psi_0\rangle \rightarrow |\psi_1\rangle \rightarrow |\psi_2\rangle \rightarrow \dots$

takes place in  $\text{span} \{ |\psi_0\rangle, |\omega\rangle \}$ , i.e.,  
a two-dimensional space!

Two natural ONSs for Heis space:

$$|x_0\rangle$$

$$|x_0^\perp\rangle := \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$$

$$\propto |\omega\rangle - |x_0\rangle \underbrace{\langle x_0|\omega\rangle}_{=\frac{1}{\sqrt{N}}}$$

$$\langle x_0|x_0^\perp\rangle = 0$$

And another basis

$$|\omega\rangle \quad \text{with} \quad \langle \omega|\omega^\perp\rangle = 0$$

$$|\omega^\perp\rangle$$

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

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

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

$$O_f |\psi\rangle = O_f (a|x_0\rangle + b|\omega^\perp\rangle) = \underbrace{-a|x_0\rangle + b|x_0^\perp\rangle}_{\{}$$

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

$\Rightarrow \underline{O_f \text{ reflects } |\psi\rangle \text{ about } |x_0^\perp\rangle!}$

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

$$\stackrel{\vec{\jmath}}{=} -(-x|\omega\rangle + y|\omega^\perp\rangle) = x|\omega\rangle - y|\omega^\perp\rangle.$$

$$O_\omega = I - 2(\omega X\omega)$$

$\Rightarrow \underline{(-O_\omega) \text{ reflects } |\psi\rangle \text{ about } |\omega\rangle!}$

Thus: each Grover iteration consists of two steps:

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

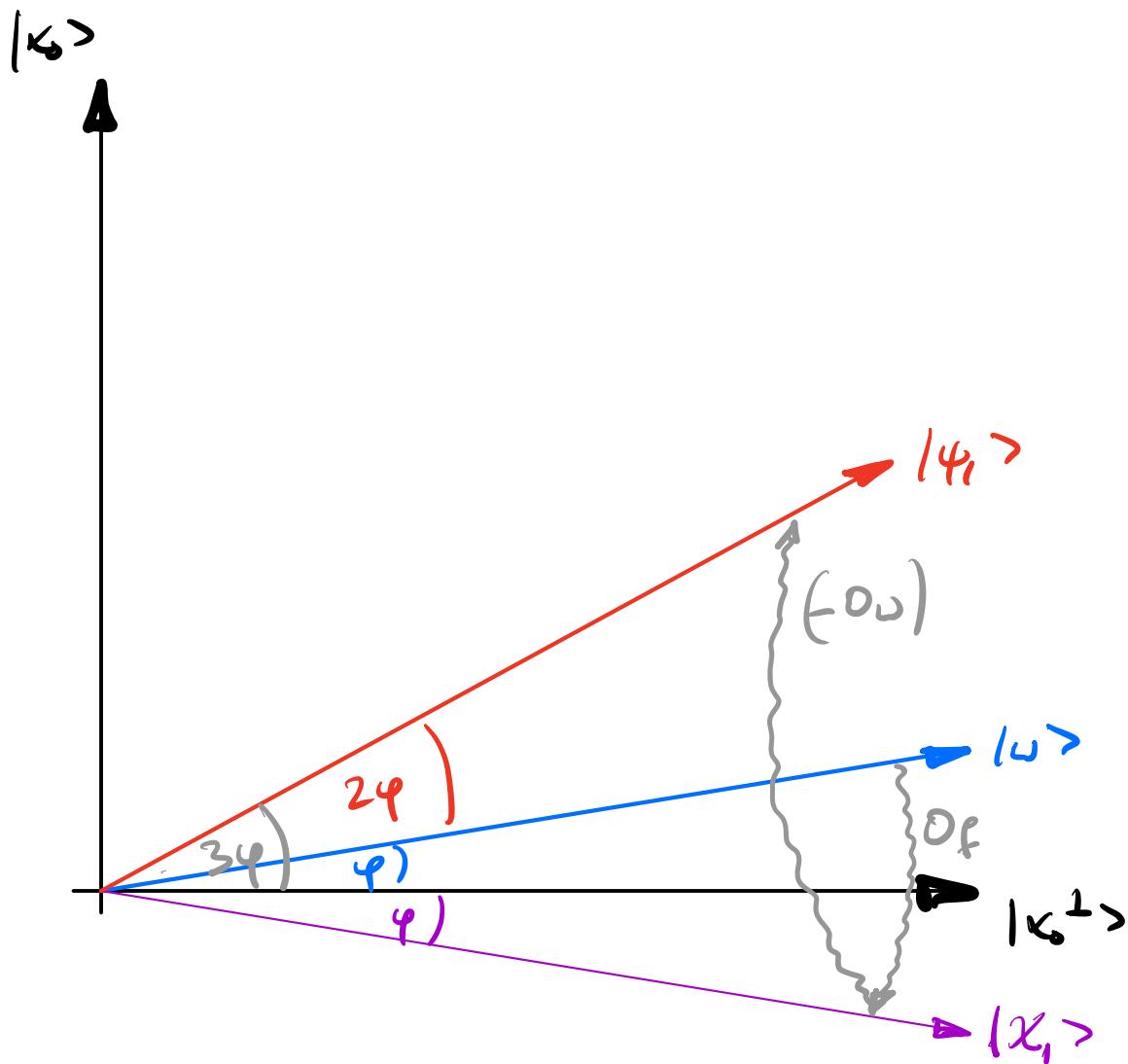
(ii) reflect about  $|\omega\rangle$

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

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

$$|x_1\rangle = O_f |\omega\rangle$$

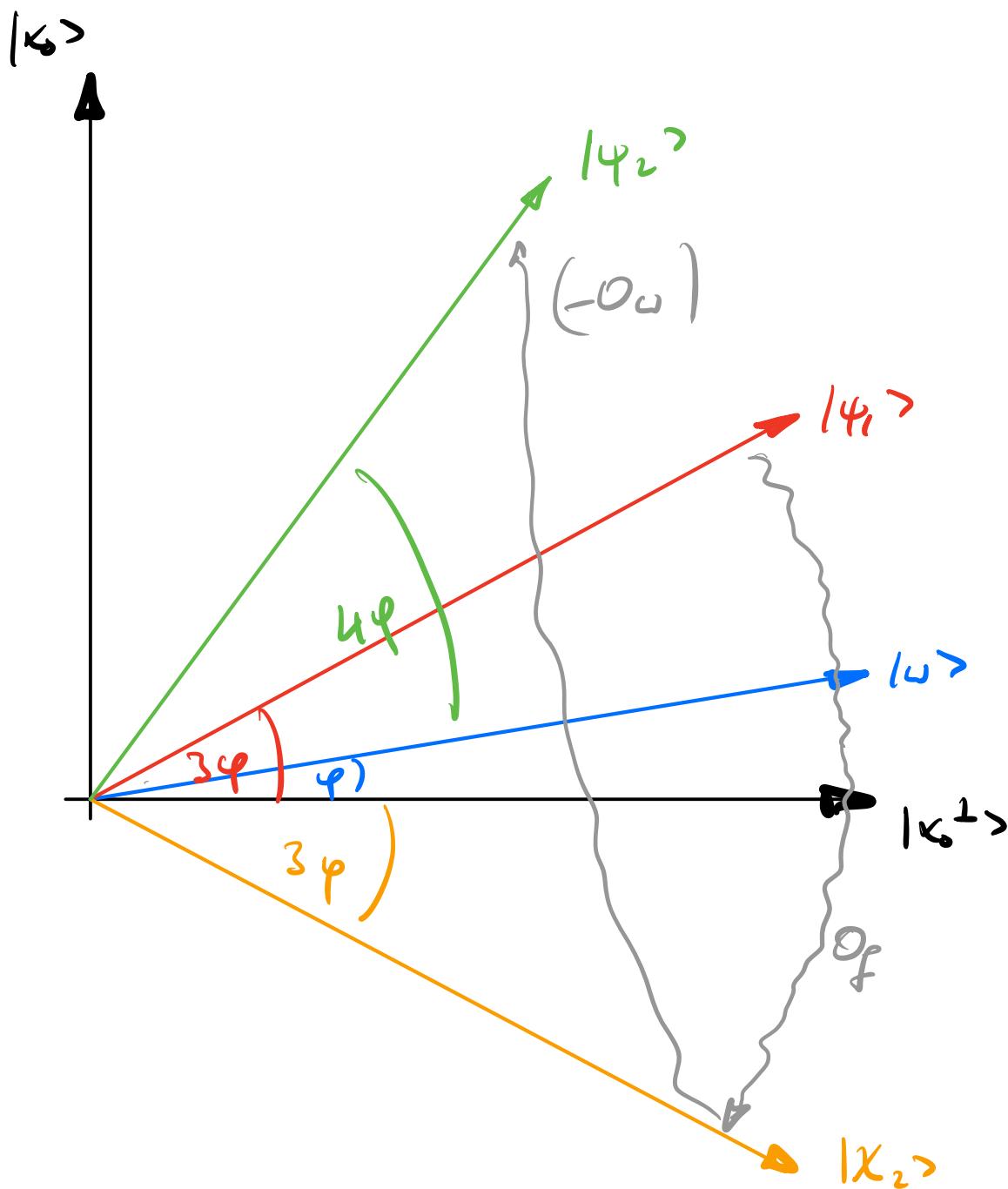
$$|\psi_1\rangle = (-O_\omega)|x_1\rangle = (-O_\omega)O_f |\omega\rangle$$



$$\rightarrow |\psi_1\rangle = \sin(3\varphi) |x_0\rangle + \cos(3\varphi) |x^\perp\rangle$$

Next Grover iteration:

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



$$\Rightarrow |\psi_2\rangle = \sin(\sqrt{\varphi}) |\kappa\rangle + \cos(\sqrt{\varphi}) |\kappa^\perp\rangle$$

Can continue ... :

$$\Rightarrow |\psi_k\rangle = \sin((2k+1)\varphi) |\kappa\rangle + \cos((2k+1)\varphi) |\kappa^\perp\rangle$$

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

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

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

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

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

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

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

Quadratic speed-up with respect to classical  
algorithms for general search problems!

Note:

- If there are  $k > 1$  solutions:

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

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