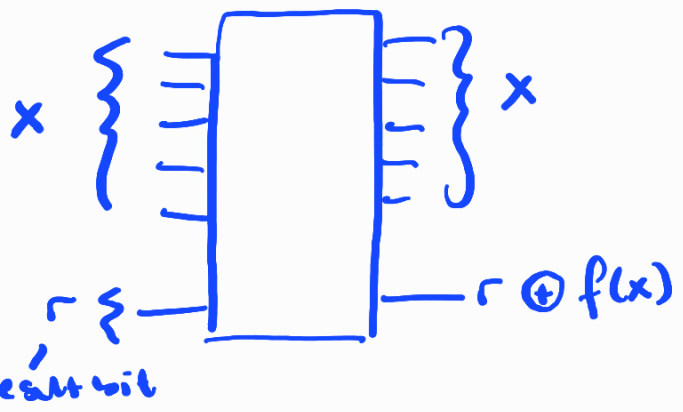
GROVER SEARCH ALGORITHM

Problem: There is a black-box that computes an unknown function f.



is known, the function f is known to take value 1 for one of the inputs x_0, and it is 0 otherwise

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{if } x \neq x_0 \end{cases}$$

Problem: Find x_0

Examples ① Searching an unsorted database

x	words
0	PQA
1	QUA
2	VENI
x_0	SCHÖN
⋮	⋮
N-1	XAV

sorted data base

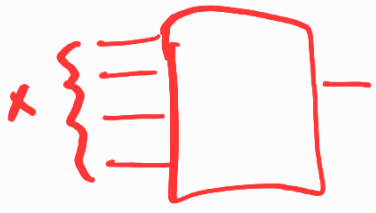
Find the place of x_0 at which the word SCHÖN appears

$f(x) =$ { does the word in x^{th} place equal to SCHÖN? }

$= \begin{cases} 1 & \text{if yes} \\ 0 & \text{no} \end{cases}$

② Password cracking (by brute force)

Chip tests if the input x is the correct password.



$$f(x) = \begin{cases} 1 & \text{if } x \text{ is the correct password} \\ 0 & \text{otherwise} \end{cases}$$

N = number of possible inputs

* Classical algorithm is brute force.
  Try all x values one-by-one and see if $f(x)$ gives 1.

  . On the average you need to evaluate f $\frac{N}{2}$ times.

  . At the worst case N evaluation

  Ex $N = (50)^8$ for password case

  $$\left(\frac{100}{2}\right)^8 \sim \frac{10^{16}}{2^8} \sim 10^{14}$$

→ classical complexity = $O(N)$

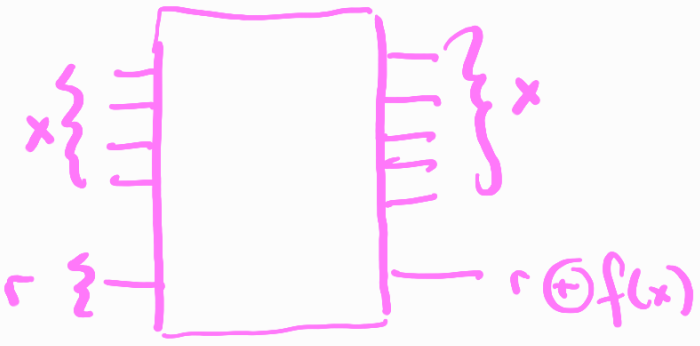
Grover shows that for quantum computes the complexity is $O(\sqrt{N})$ if $N \sim 10^{14}$, $\sqrt{N} = 10^7$ ← database lookup

* $X = \{0, 1, \cdots, N-1\}$ an N-element set

$$f: X \longrightarrow \{0,1\}$$

$$f(x) = \delta_{x,x_0}$$

Find x_0



$$U_f |x\rangle_I \otimes |r\rangle_R = |x\rangle_I \otimes |r \oplus f(x)\rangle_R$$

$|x\rangle_I$ ← input; $|r\rangle_R$ ← result

* $|-\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$U_f |x\rangle_I \otimes |-\rangle_R = (-)^{f(x)} |x\rangle_I \otimes |-\rangle_R$$

$\{|0\rangle_I, |1\rangle_I, \cdots, |N-1\rangle_I\}$ = An orthonormal basis of an

N dimensional Hilbert Space

↓ eigenvalue equation

eigenvalues → + + + + + + ⊙ + + + + + + +

Note: Result qubit R is always in $|-\rangle$ state.

For this reason, we supress it in the notation.

$$U_f |x\rangle = (-)^{f(x)} |x\rangle$$

* Consider the state

$$|\psi\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + |1\rangle + \cdots\cdots + |N-1\rangle \right)$$

= superposition of all possible input values.

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

* Consider a unitary W defined as

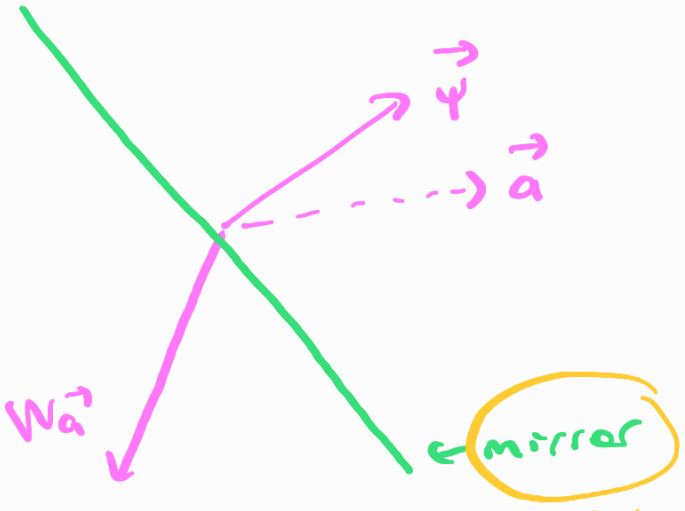
$$W = 1 - 2|\psi\rangle\langle\psi|$$

= reflection along the vector $|\psi\rangle$

* U_f is also a reflection (along $|x_0\rangle$)

$$U_f|x\rangle = (-)^{f(x)}|x\rangle$$

$$U_f = 1 - 2|x_0\rangle\langle x_0| \quad \text{(Alternative expression)}$$

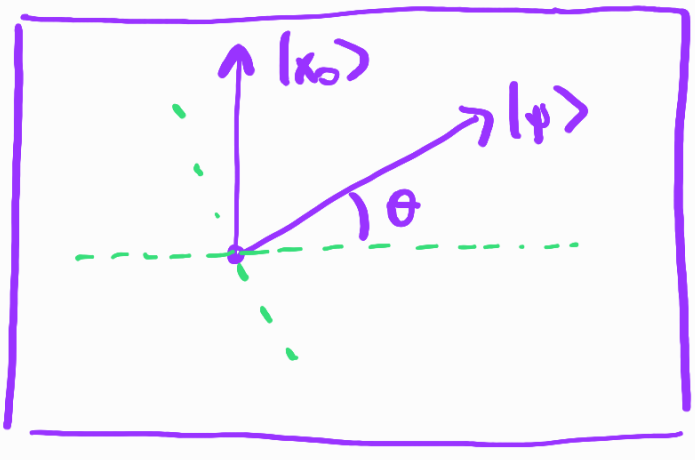


$W|\psi\rangle = -|\psi\rangle$

$W|\phi\rangle = |\phi\rangle$ for any $|\phi\rangle$ perpendicular to $|\psi\rangle$

Mirror plane / subspace = All vectors perp. to $|\psi\rangle$

Claim: The 2D subspace spanned by $|x_0\rangle$ and $|\psi\rangle$ is invariant under the actions of U_f and W.



WU_f is a rotation by angle 2θ

$$\star\quad |\psi\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + \dots + |x_0\rangle + \dots + |N-1\rangle\right)$$

↳ separate out

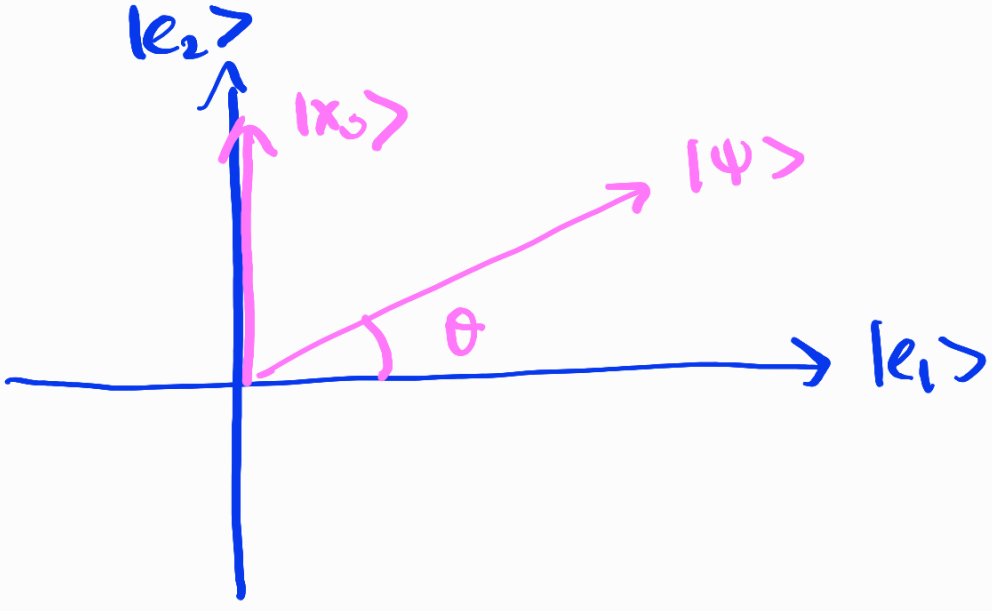
$$= \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |x_0-1\rangle + |x_0+1\rangle + \dots + |N-1\rangle\right) + \frac{1}{\sqrt{N}}|x_0\rangle$$

vector with norm $\sqrt{\frac{N-1}{N}}$

$$|e_1\rangle \equiv \frac{1}{\sqrt{N-1}} \sum_{x(\neq x_0)} |x\rangle$$ = superposition of all non-solutions

$$|\psi\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|e_1\rangle + \frac{1}{\sqrt{N}}|x_0\rangle \rightsquigarrow |e_2\rangle$$

$\{|e_1\rangle, |e_2\rangle\}$ forms an orthonormal basis of the 2D subspace spanned by $|x_0\rangle$ and $|\psi\rangle$?



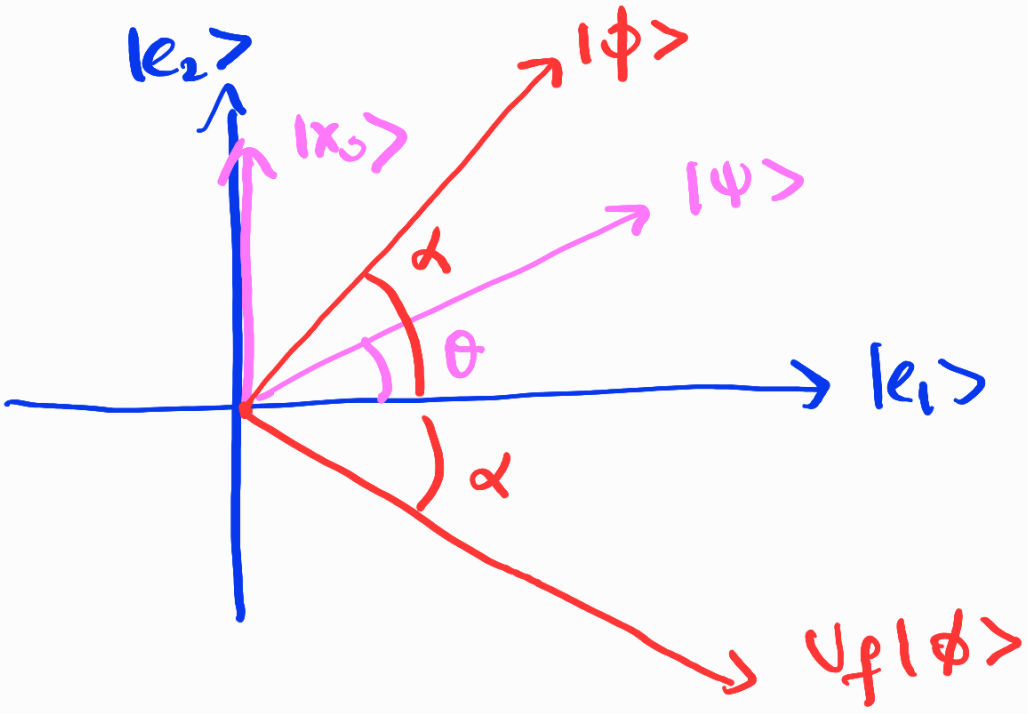
$$|\psi\rangle = \sqrt{\frac{N-1}{N}}\,|e_1\rangle + \frac{1}{\sqrt{N}}\,|e_2\rangle$$

$\cos\theta$ ← $\qquad$ → $\sin\theta$

$$\downarrow$$

$$\theta = \arcsin\left(\frac{1}{\sqrt{N}}\right)$$

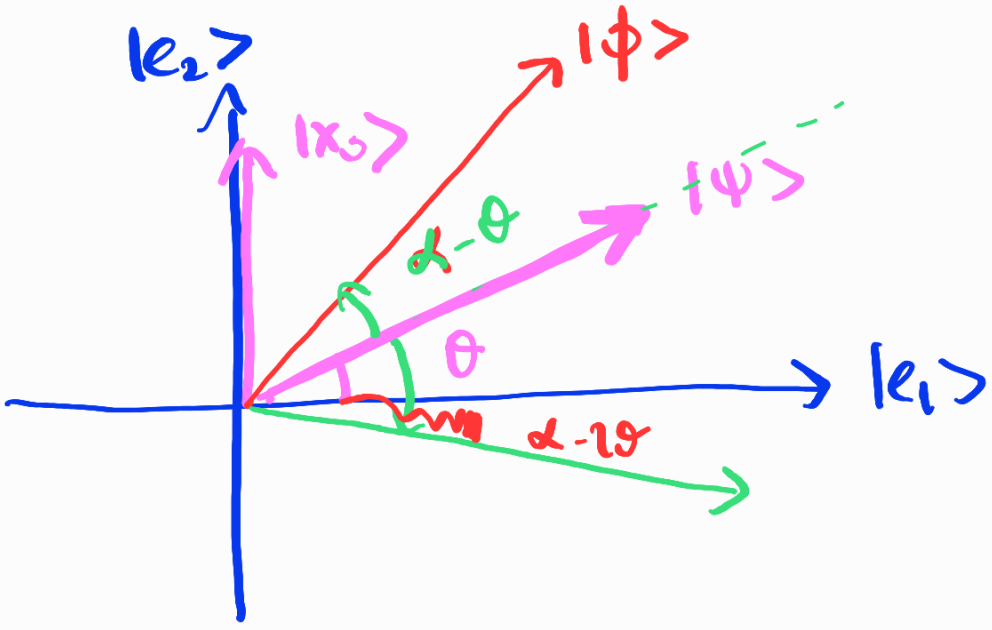
if $N \gg 1$, $\quad \theta \simeq \frac{1}{\sqrt{N}}$



if $|\psi\rangle = \cos\alpha\,|e_1\rangle + \sin\alpha\,|e_2\rangle$

then $\quad U_f|\psi\rangle = \cos\alpha\,|e_1\rangle - \sin\alpha\,|e_2\rangle$

$\alpha \xrightarrow{U_f} -\alpha$ ($\alpha=0$ is mirror plane)



The action of w

$(-w)\,|\phi\rangle = ?$

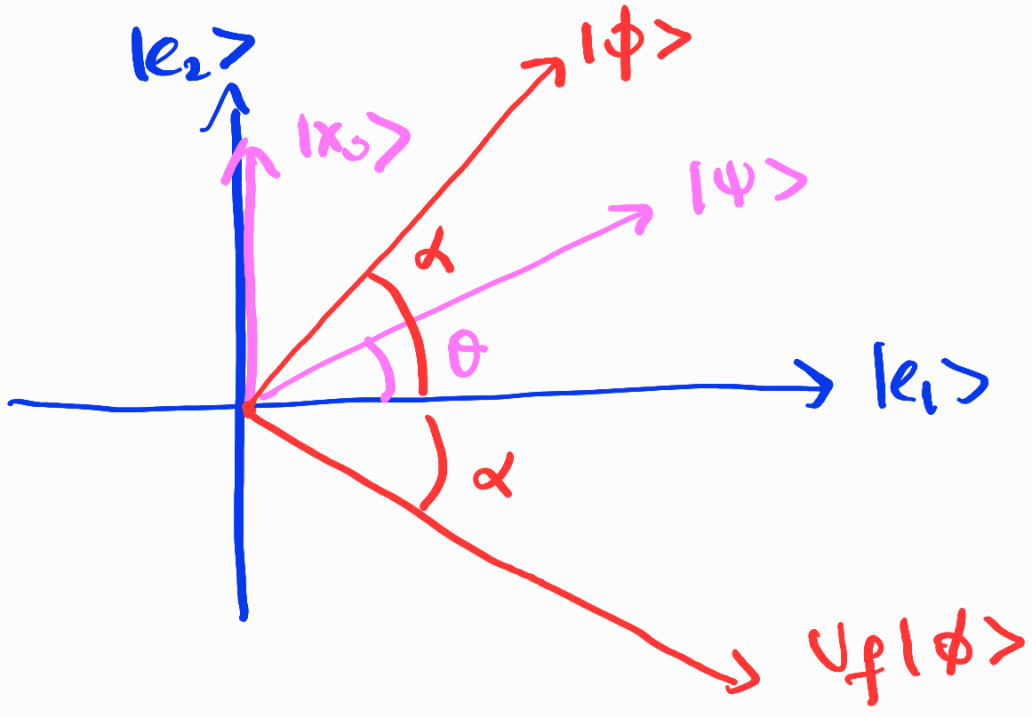
if $|\phi\rangle = \cos\alpha\,|e_1\rangle + \sin\alpha\,|e_2\rangle$

then $(-w)|\phi\rangle = \cos(\alpha-2\theta)\,|e_1\rangle - \sin(\alpha-2\theta)\,|e_2\rangle$

$$\alpha \xrightarrow{(-w)} -(\alpha-2\theta)$$

$$\theta \longrightarrow \theta$$

$\alpha=\theta$ is the mirror plane



What is the action of $-WU_f$

$$\alpha \xrightarrow{U_f} -\alpha \xrightarrow{(-W)} -((-\alpha)-2\theta)$$

$$= \alpha + 2\theta$$

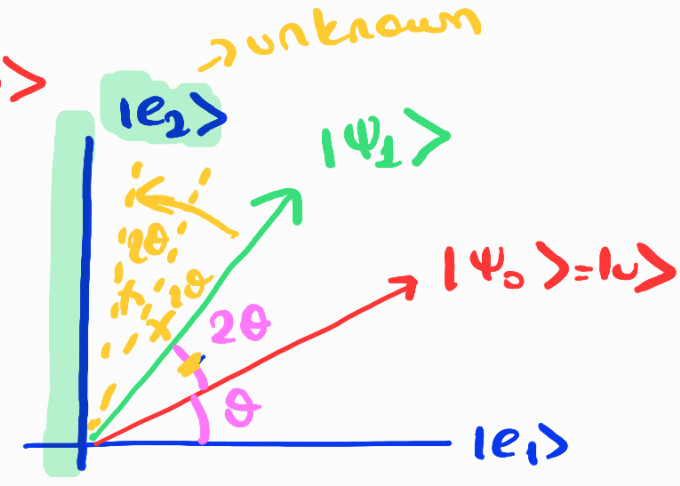
if $|\phi\rangle = \cos\alpha\,|e_1\rangle + \sin\alpha\,|e_2\rangle$

then $-WU_f|\psi\rangle = \cos(\alpha+2\theta)\,|e_1\rangle + \sin(\alpha+2\theta)\,|e_2\rangle$

ΦΦ

Grover algorithm

① Prepare the input qubits I in the state $|u\rangle$ $\quad |\psi_0\rangle = |u\rangle$



② Evaluate f and then apply W operation (in short, apply $-WU_f$)

$$|\psi_1\rangle = -WU_f|\psi_0\rangle$$

②' Apply the step ② k times

$$|\psi_k\rangle = (-WU_f)^k|\psi_0\rangle$$

$$= \cos(2k+1)\vartheta\,|e_1\rangle + \sin(2k+1)\vartheta\,|e_2\rangle$$

②'' Choose k such that $(2k+1)\vartheta \approx \frac{\pi}{2}$ rad

$$k = \left[\frac{\pi}{4\vartheta} - \frac{1}{2}\right] \quad \text{integer part}$$

$$\vartheta = \arcsin\frac{1}{\sqrt{N}} \sim \frac{1}{\sqrt{N}}$$

$$k \sim \frac{\pi}{4}\sqrt{N} = \#\text{ of function evaluations}$$

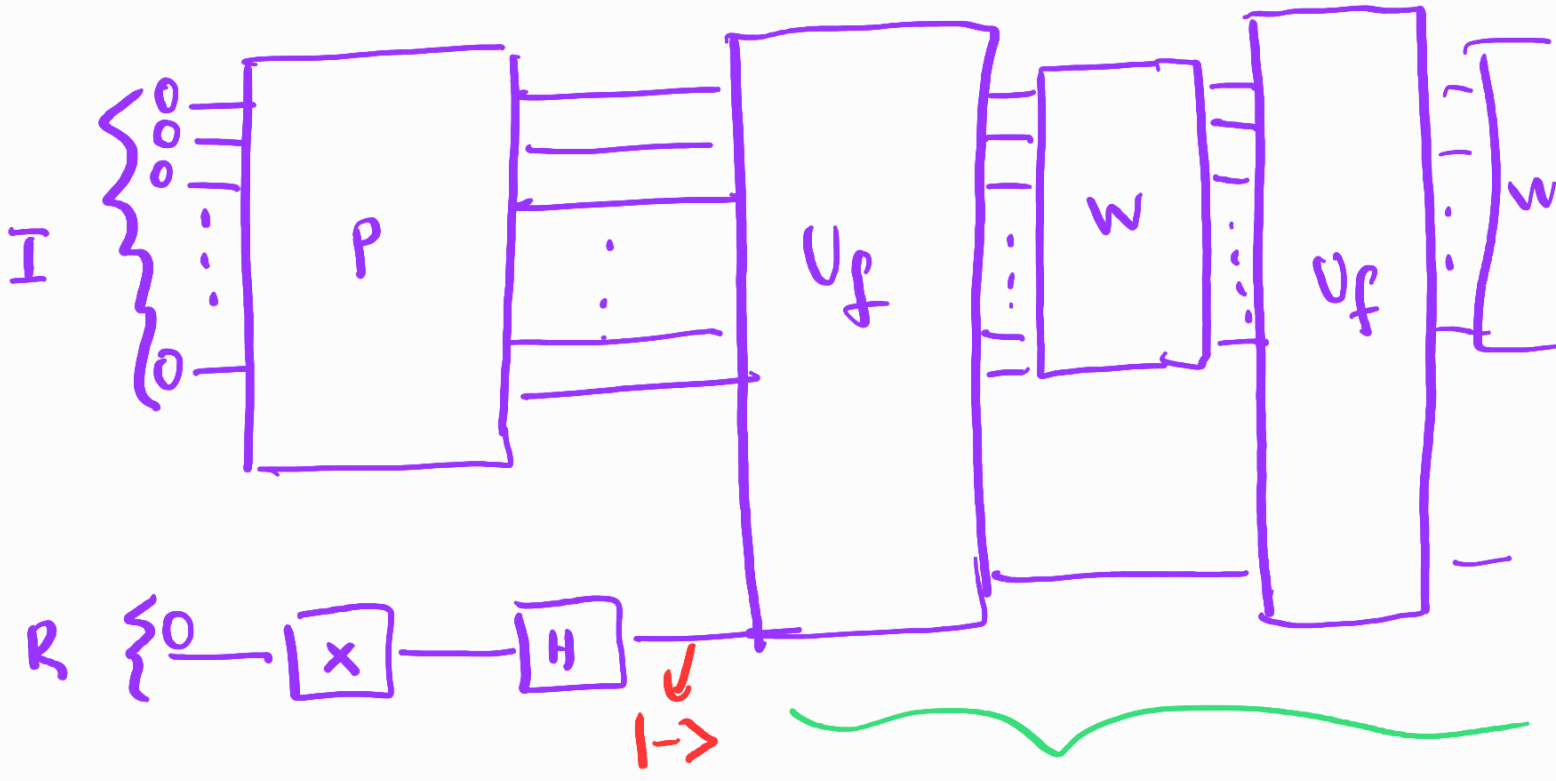
(3) Measure the input qubits I.

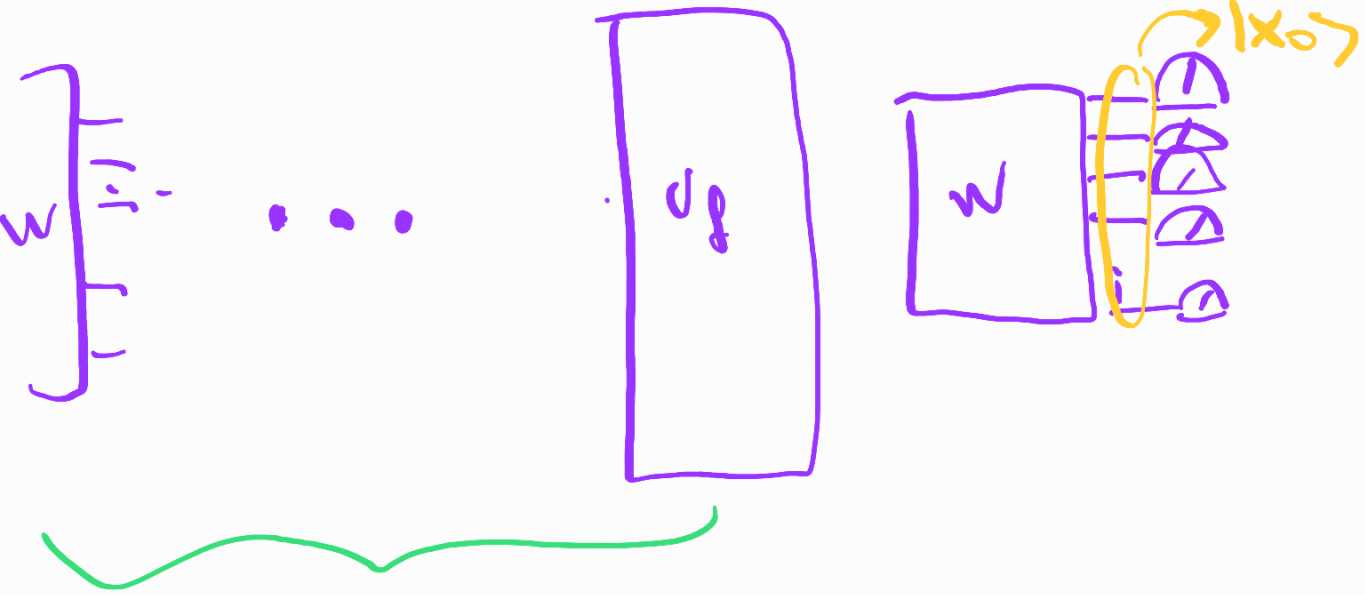
Since $|\psi_k\rangle \simeq \cos\frac{\pi}{2}|e_1\rangle + \sin\frac{\pi}{2}|e_2\rangle$

then with pros ~ 1 we $= |e_2\rangle = |x\rangle$ ← solution

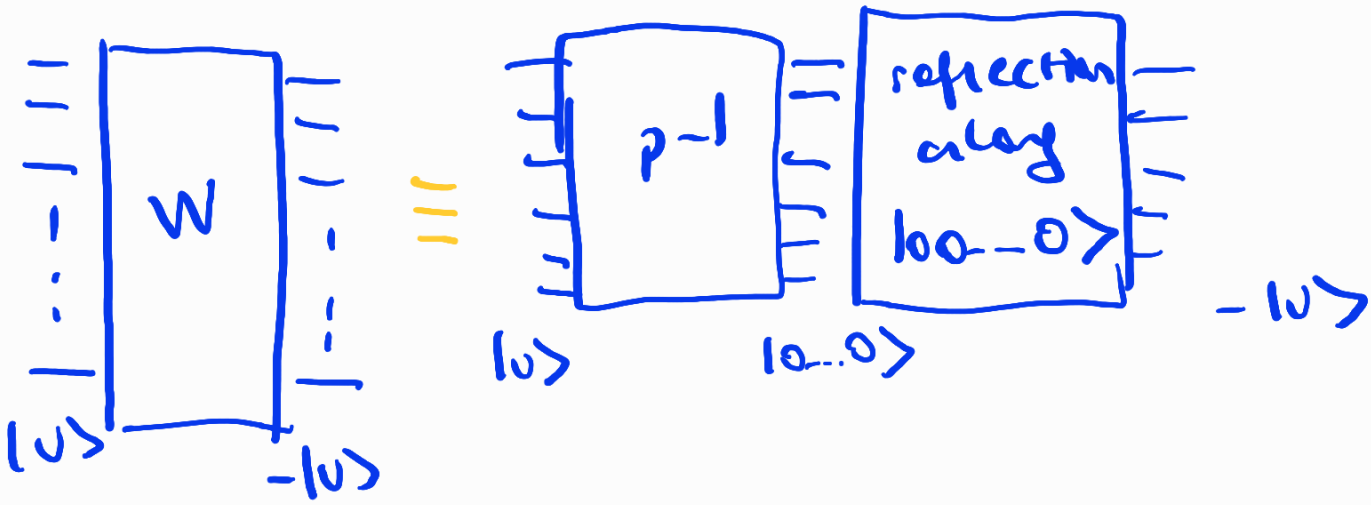
get the value of x_0.

# of evaluations $= \frac{\pi}{4}\sqrt{N} \longrightarrow O(\sqrt{N})$ complexity





repeated $k \sim \frac{\pi}{4}\sqrt{N}$ times



* if $N=4$ $\quad \sin\theta = \frac{1}{\sqrt{N}} = \frac{1}{2}$, $\theta = 30^\circ = \frac{\pi}{6}$ rad.

$(2k+1)\theta = \frac{\pi}{2} = 3\theta$ Only $k=1$ evaluation is sufficient

if $N>4$ then $(2k+1)\vartheta$ can never be equal to $\frac{\pi}{2}$.

$$|\psi_k\rangle = \underbrace{\cos\left(\frac{\pi}{2}-\epsilon\right)}_{\sim \epsilon \sim \frac{1}{\sqrt{N}}} |e_1\rangle + \underbrace{\sin\left(\frac{\pi}{2}-\epsilon\right)}_{\sim} |e_2\rangle$$

$\left((2k+1)\vartheta \approx \frac{\pi}{2}$ with a difference of the order of $\vartheta \sim \frac{1}{\sqrt{N}}\right)$

probability of finding a non-solution at the measurement stage is $\sim \frac{1}{N}$

Summary of the algorithm:

① Prepare $\underbrace{\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\right)_I}_{|\phi\rangle} \otimes |-\rangle_R$

② Apply $(-W U_f)$ $k = \frac{\pi}{4}\sqrt{N}$ times

$\swarrow$

$1 - 2|\phi\rangle\langle\phi|$

③ Measure I

At m^{th} step of iteration

$$(-\omega U_f)^m |\psi_{in}\rangle = \cos(2m+1)\vartheta \left(\sqrt{\frac{N-1}{N}} \sum_{x \neq x_0} |x\rangle\right) + \sin(2m+1)\vartheta \cdot |x_0\rangle$$

superposition of non-Selection

* If $f: \{0, 1, \ldots, N-1\} \to \{0, 1\}$ is such that there are M solutions to the equation $f(x) = 1$

$$f(x) = \begin{cases} 1 & \text{if } x = x_1 \text{ or } x_2 \ldots x_M \\ 0 & \text{otherwise} \end{cases}$$

$$1 \leq M < N$$

(You know the value of both M and N)

Problem: Find one of the solutions.

* Two states

$$|S\rangle = \frac{1}{\sqrt{M}} \underbrace{\left(|x_1\rangle + |x_2\rangle + \cdots + |x_m\rangle \right)}_{\text{superposition of solutions}}$$

$$|NS\rangle = \sqrt{\frac{1}{N-M}} \underbrace{\left(\sum_{x \neq x_1, \ldots, x_m} |x\rangle \right)}_{\text{superposition of non-solutions}}$$

$$|\phi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \Big\} \text{superposition of all poss. inputs}$$

$$|\phi\rangle = \underbrace{\sqrt{\frac{N-m}{N}}}_{\cos\theta} |NS\rangle + \underbrace{\sqrt{\frac{M}{N}}}_{\sin\theta} |S\rangle$$

$$\cos^2\theta + \sin^2\theta = 1$$

if $M \ll N$, then $\theta \sim \sqrt{\frac{M}{N}} \ll 1$

$$\star \quad U_f = \mathbb{1} - 2|s\rangle\langle s|$$

$$W = \mathbb{1} - 2|\phi\rangle\langle\phi|$$

$$(-WU_f)^m \left(\cos\alpha|NS\rangle + \sin\alpha|S\rangle\right)$$

(m → m times; $\alpha = \theta$ initially)

$$= \cos(\alpha + 2m\theta)|NS\rangle + \sin(\alpha + 2m\theta)|s$$

After $m = \cdots$ we have $(2m+1)\theta = \frac{\pi}{2}$

$$m \simeq \frac{\pi}{4\theta}$$

$$m \simeq \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

and any measurement of I will yield one of the solutions. (each one is equally likely.)

* If f has N solutions, finding one of the solutions takes $\frac{\pi}{4}\sqrt{\frac{N}{M}}$ steps

* what if ...

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

but you don't know the number of solutions to $f(x) = 1$ (you don't know N)

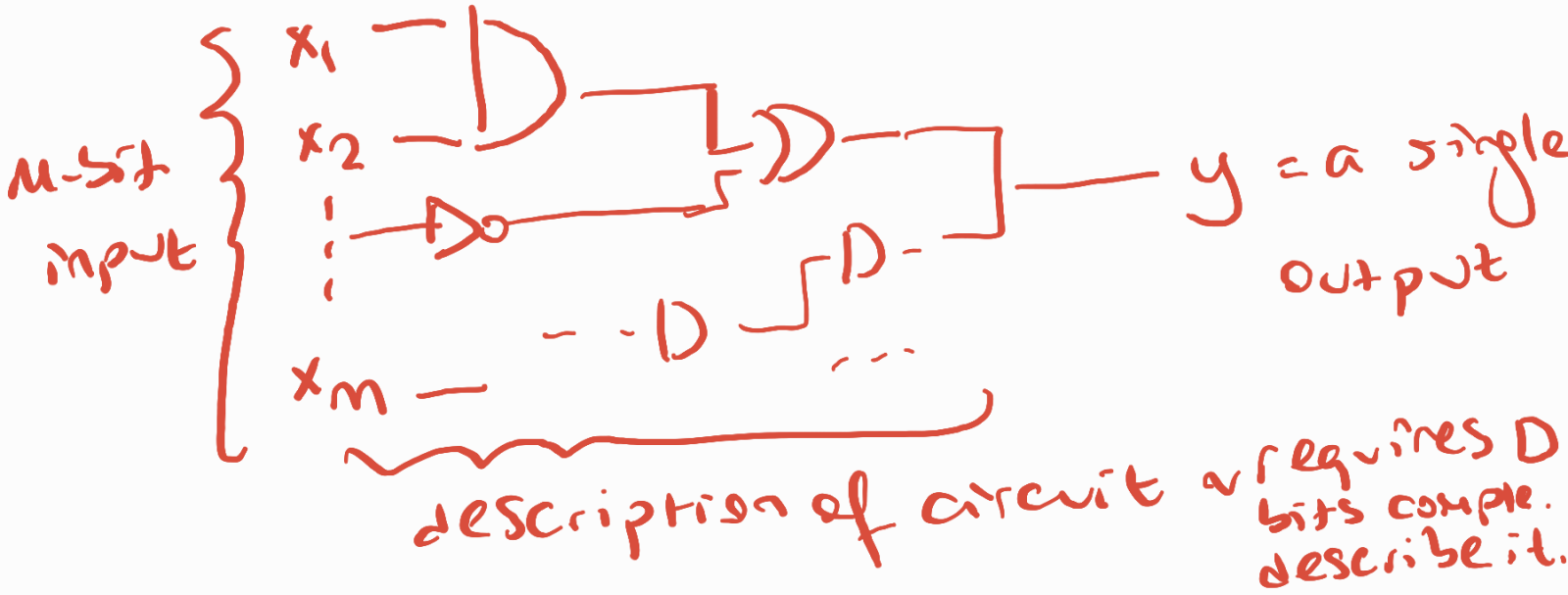
don't know where to find

→ There is an algorithm that prob. finds a solution of order $\sqrt{N}$.

* Some problems:

SAT: Satisfiability

A given logic circuit



Circuit computes a one-bit logical function $y = f(x_1, \ldots, x_n)$

N = the size of the description of the problem. $= D$

Problem: Find an input $x = (x_1, \ldots, x_n)$ which produces an output of $f(x) = 1$

Decision problem: Given the description of the circuit, decide if there is an input that produces the outcome of 1.

Complexity of problem: How many steps of computation is needed to find the answer.

polynomial complexity: if steps $\sim N^{\text{const}}$ } some power

exponential comp: if steps $\sim e^{N}$ } class P

Nobody has found an algorithm that solves SAT in polynomial time steps

↙

we don't know if SAT is in P class or not.

* A problem is NP if a proposed solution is given, then it can be checked that it is the solution in polynomial times

SAT is NP if $x = (x_1, \dots, x_n)$ is given.

in D steps you can compute $y = f(x)$

steps $\sim N$

* Multiplication of two N bit numbers

$x = x_1 \text{ ---- } x_N$

$y = y_1 \text{ ---- } y_N$

---

compute $x.y = z_1 \text{ ---- } z_{2N}$

size $\sim 2N$

steps = time = N^2 multiplication $\sim N^2$

multiplication is P

* Factorization of a number z into its prime factors. If $z = x.y$ find x or find y.

Factorization is NP

* SAT is also NP-complete

every NP problem can be expressed as a SAT.

✡ Millenium problem: $P \stackrel{?}{=} NP$

Grover iteration can speed up the solution of NP problems

if there are N possible solutions, then Grover algorithm converts this problem to $\sqrt{N}$ step problem.

$N \sim e^{cN}$

$\sqrt{N} \sim e^{\frac{c}{2}N}$

} exponentially difficult problems are still exponential, but they are somewhat easier now.