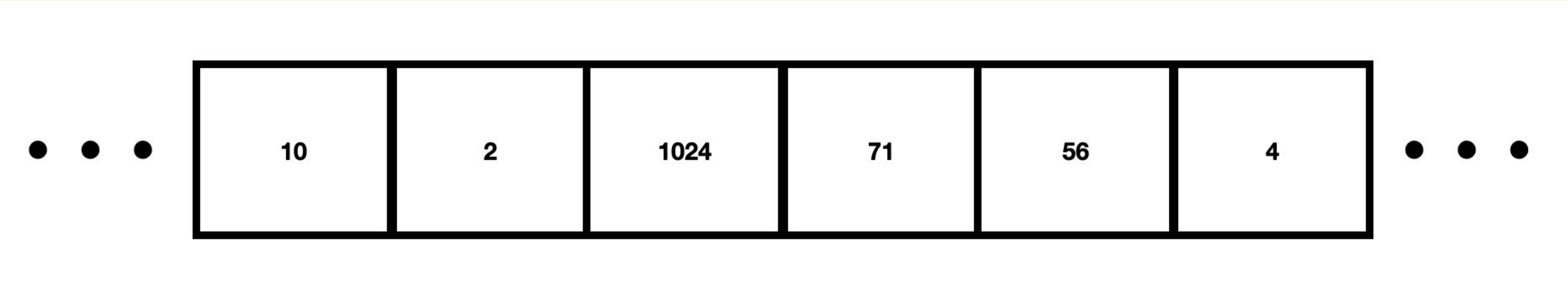
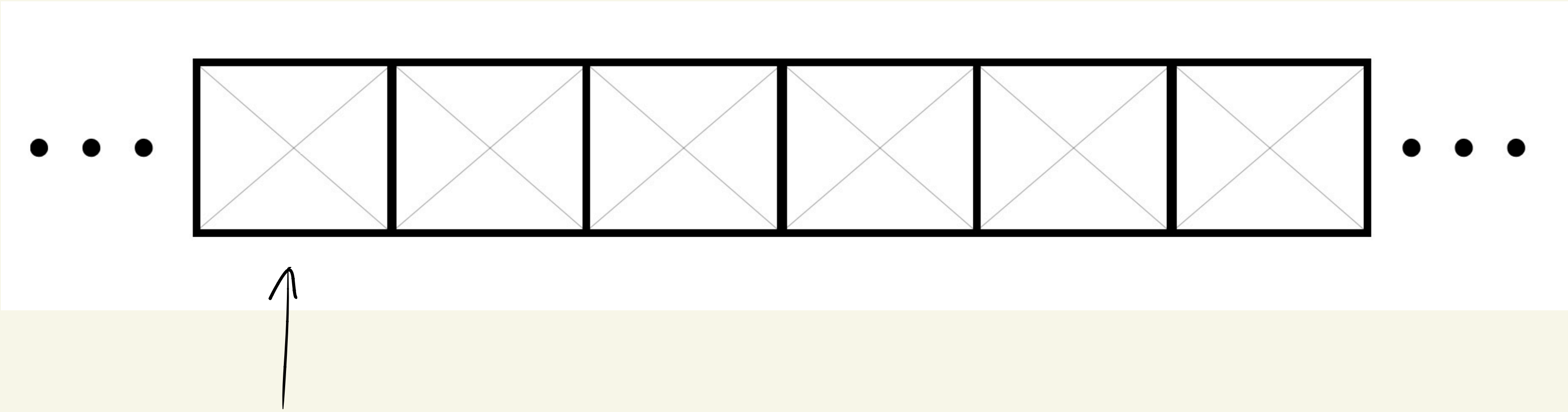
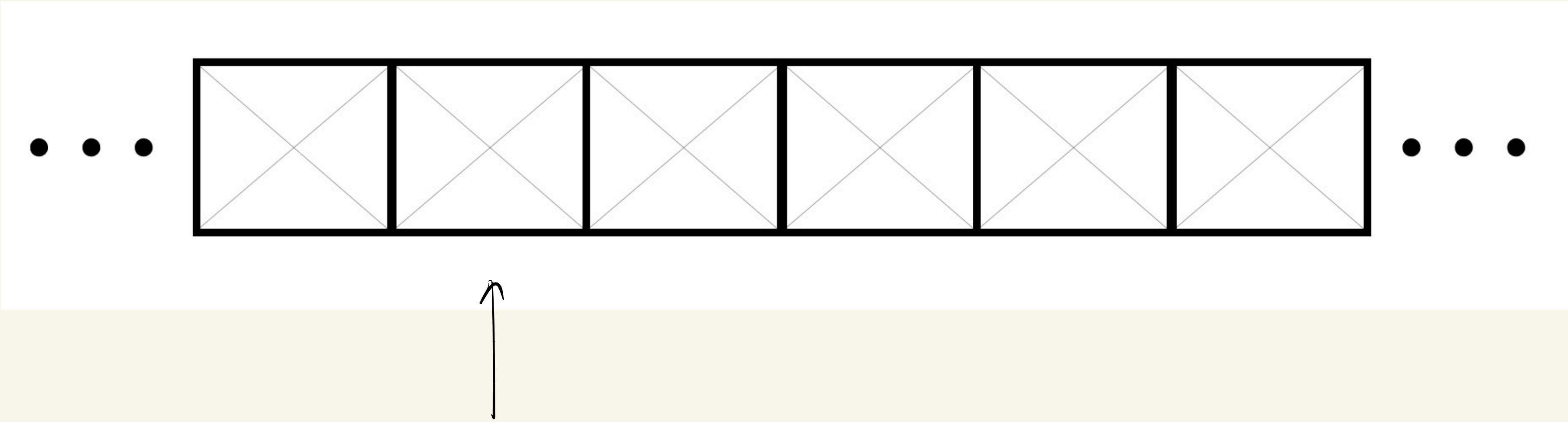
Grover's Algorithm



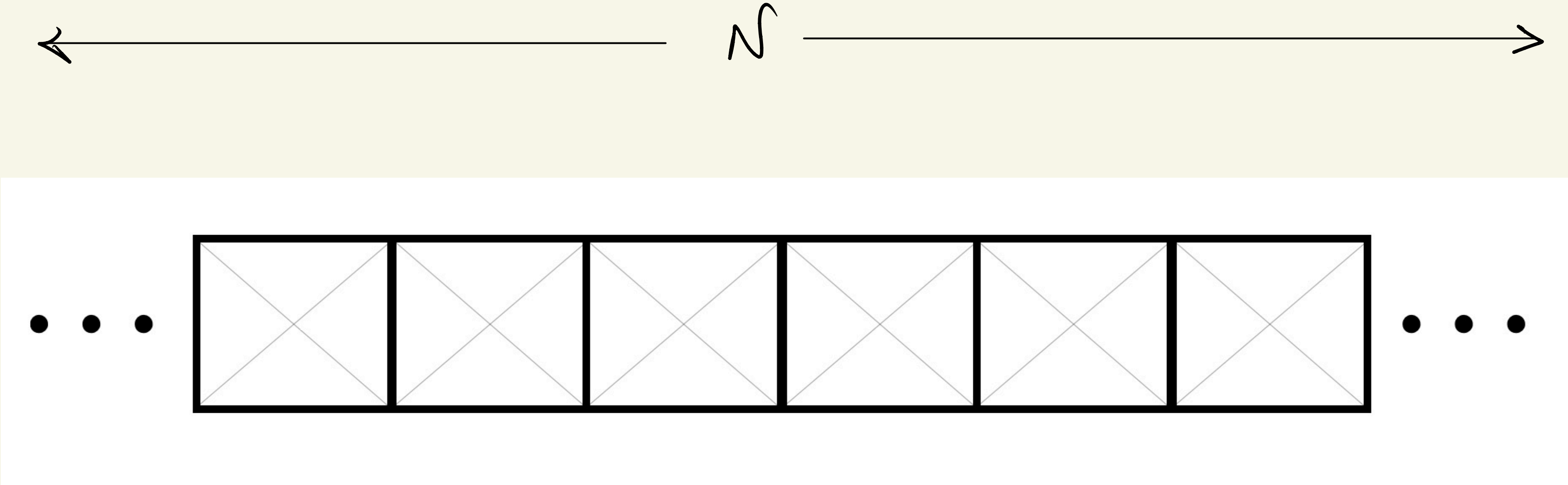
unstructured database . find 56



Are you
56?
No, ok!



Are you 56?



classically $\Rightarrow O(N)$

GROVER $\Rightarrow O(\sqrt{N})$

Let's imagine we have a Boolean function f.

Boolean functions $f : \{0,1\}^n \longmapsto \{0,1\}$

input binary strings

$x_n x_{n-1} \cdots x_1$

$x_1 \rightarrow$
$x_2 \rightarrow$
$\vdots$
$x_k \rightarrow$ $\boxed{f(x)}$ $\longrightarrow$ $0,1$

⊛ Guaranteed that a single binary string satisfies f.

How many calls (queries) to f do we need to find x?

How many calls (queries) to $\mathcal{F}$ do we need to find x?

for n-bit bitstrings there are $O(2^n)$ possible bitstrings

classically $\Rightarrow$ $O(2^n)$

Grover $\Rightarrow$ $O(\sqrt{2^n})$

Satisfiability problems

E.g: scheduling problem

Determin when a meeting can occur given contraints on people's availability

$\{\text{Monday}, \dots, \text{Friday}\} \mapsto \{x_1, x_2, \dots, x_5\}$

João $\to$ Monday, Tuesday, Friday

Carlos $\to$ not friday

Diana $\to$ Monday or wednesday

⋮

$$f(x_1, x_2, x_3, x_4, x_5) = (x_1 \vee x_2 \vee x_5) \qquad \text{João}$$

$$\wedge$$

$$(\neg x_5) \qquad \text{Carlos}$$

$$\wedge$$

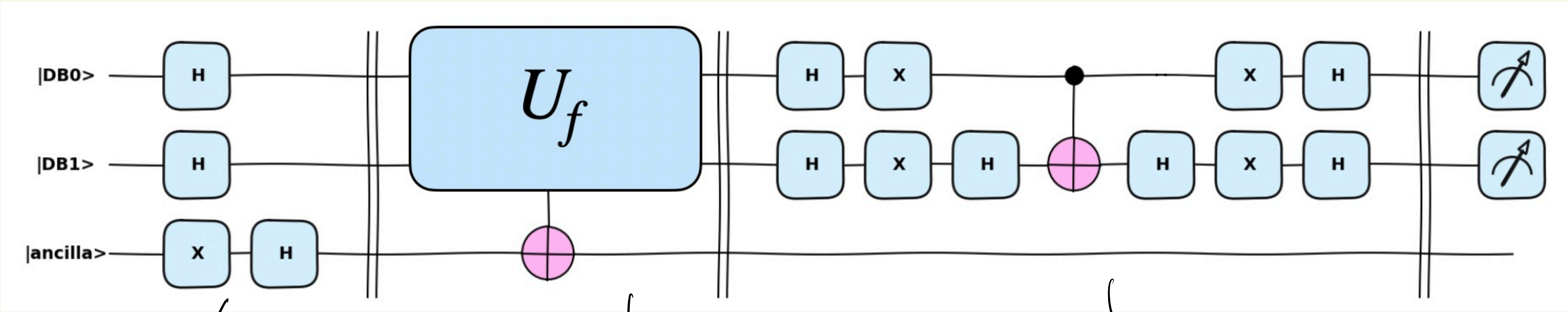
$$(x_1 \vee x_3) \qquad \text{Diana}$$

$$\wedge$$

$$\dots$$

Find $(x_1, x_2, x_3, x_4, x_5)$ that satisfies f.

Grover's Algorithm



Database superposition + ancilla |->

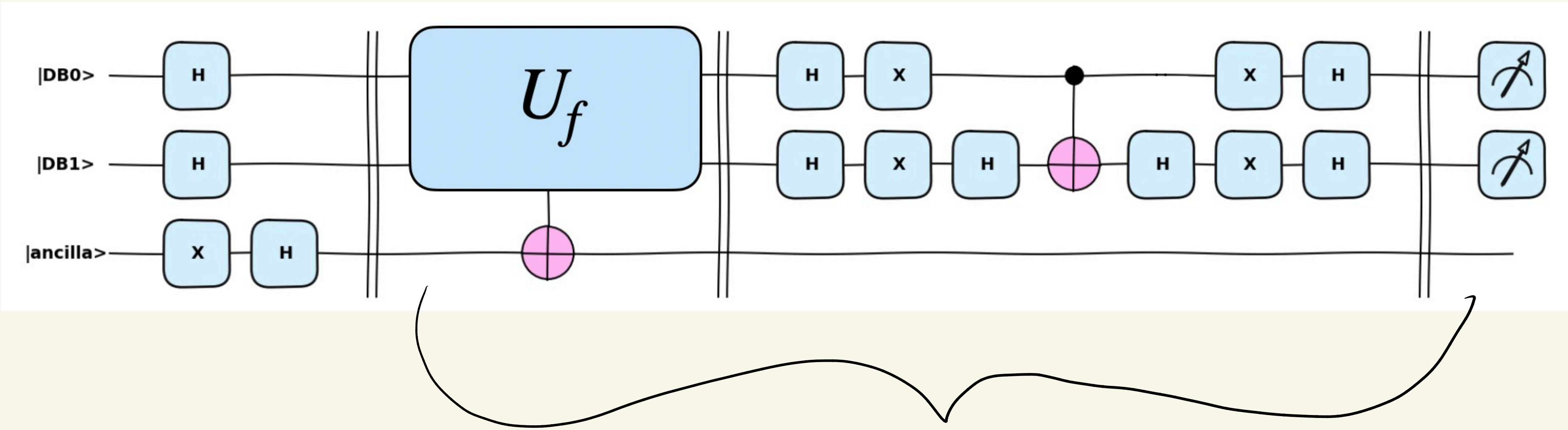
Oracle

function evaluates every possible input

Diffusion operator

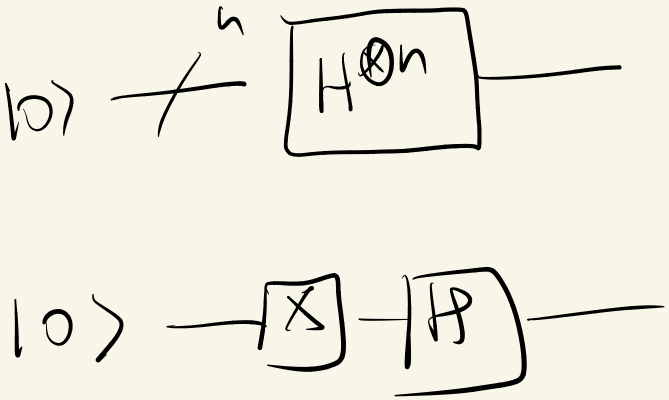
Amplifies probability of measuring solution

Grover's Algorithm



Repeat $O(\sqrt{N})$ times

Initial states

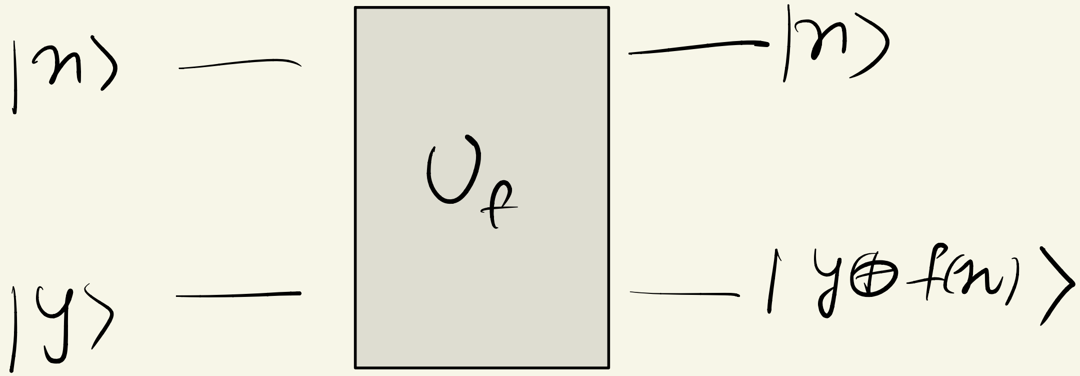


$$\left(H^{\otimes n} \otimes HX\right)\left(|0\rangle^{n} \otimes |0\rangle\right)$$

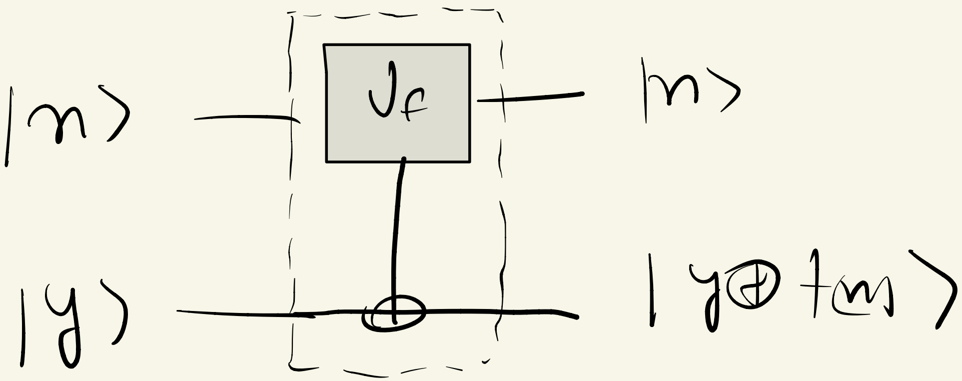
$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |x_0\rangle \; |-\rangle$$

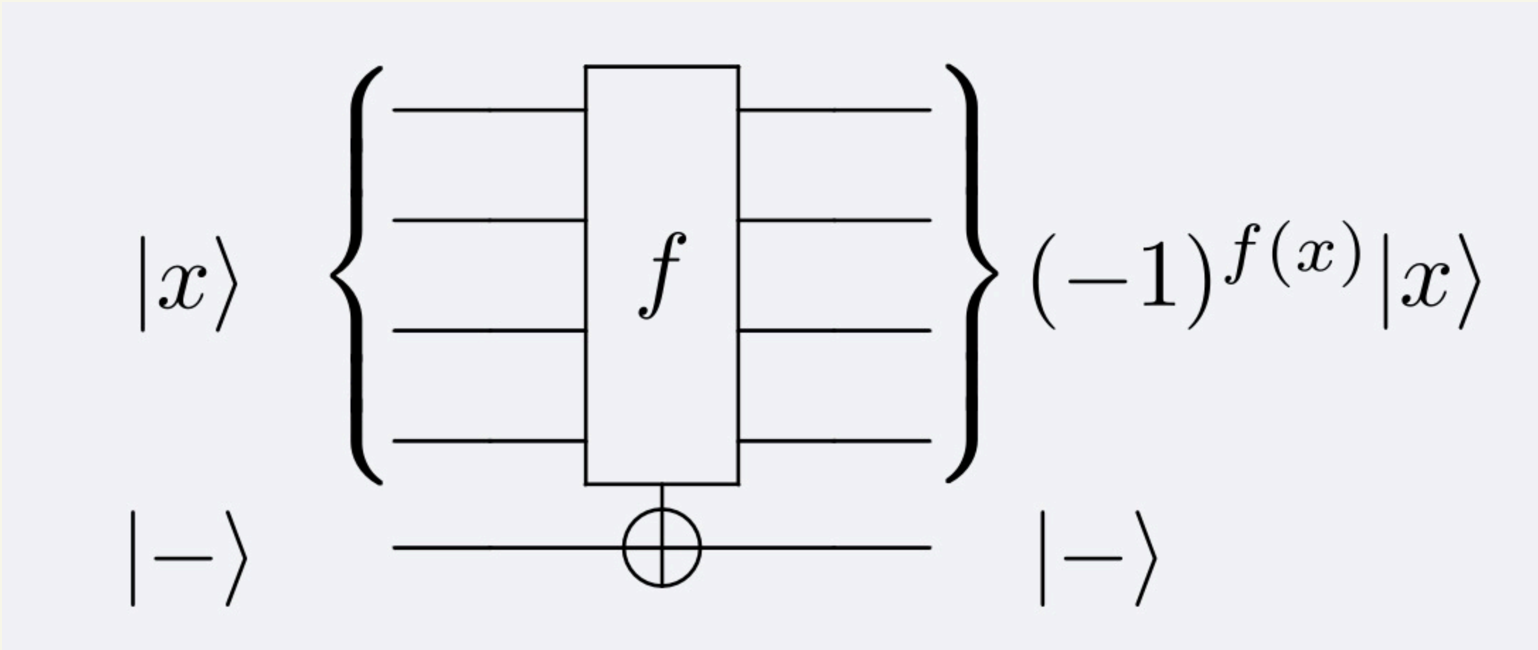
ORACLE

Quantum query gates



U_f makes bitflip on $|y\rangle$:





$|x\rangle$ satisfies F. then, from phase kickback:

$$F\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle$$

$$= |x\rangle|1\rangle - |x\rangle|0\rangle$$

$$= -|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |x_i\rangle \; |-\rangle \right)$$

Let's assume a single solution $|w\rangle$

$$\left(\frac{2^n-1}{\sqrt{2^n}} \sum_{n \neq w} |n\rangle - \frac{1}{\sqrt{2^n}} |w\rangle \right) |-\rangle$$

* If we measure at this stage then we get $|w\rangle$ with $\frac{1}{2^n}$ probability

→ Diffusion operator amplifies probability of $|w\rangle$

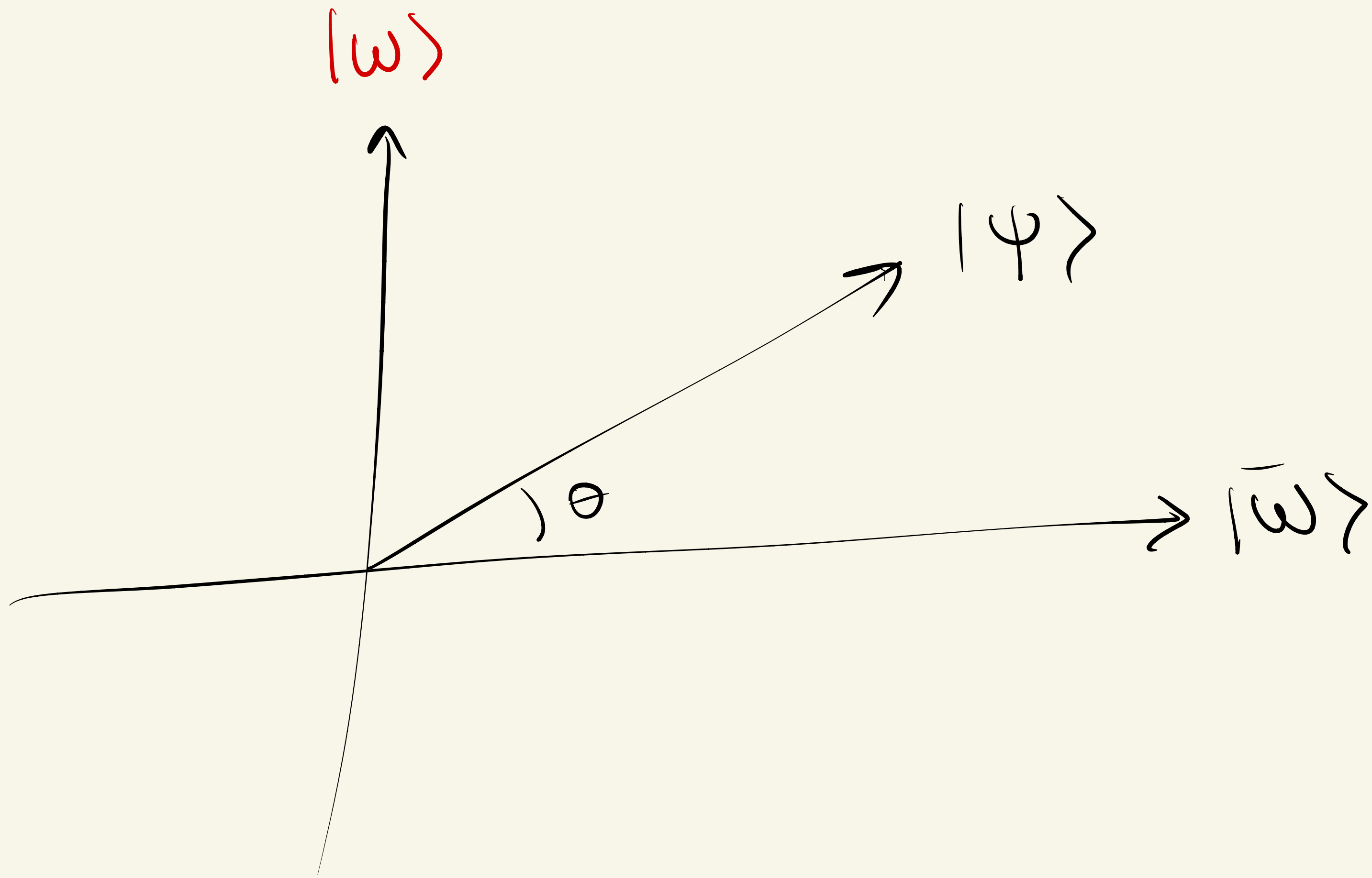
Diffusion operator

Before oracle (ignoring ancilla)

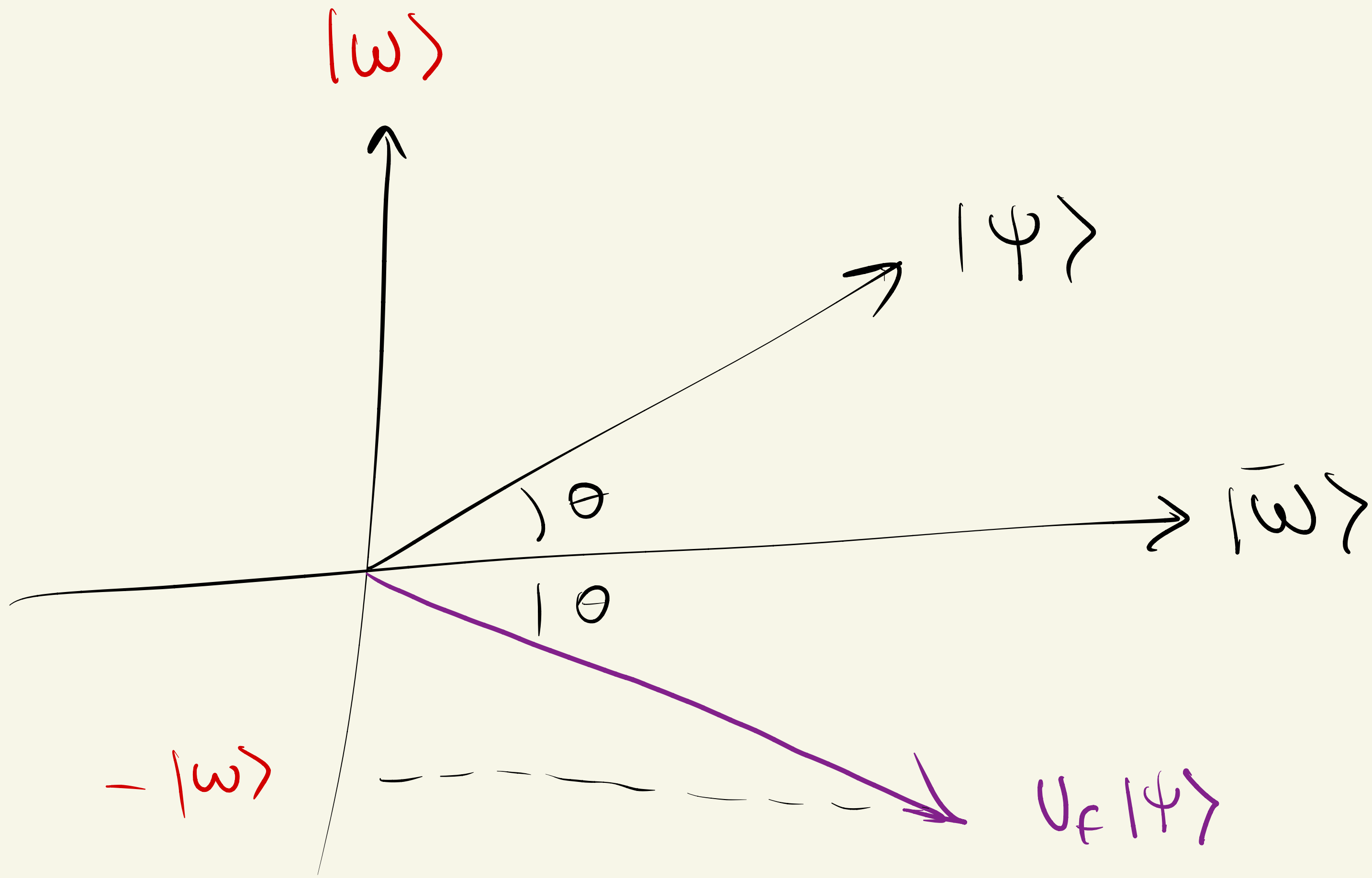
$$\frac{2^n-1}{\sqrt{2^n}} \sum_{n \neq w} |n\rangle + \frac{1}{\sqrt{2^n}} |w\rangle = |\psi\rangle$$

$$= \frac{2^n-1}{\sqrt{2^n}} |\bar{w}\rangle + \frac{1}{\sqrt{2^n}} |w\rangle$$

$$= \cos(\theta) |\bar{w}\rangle + \sin(\theta) |w\rangle$$

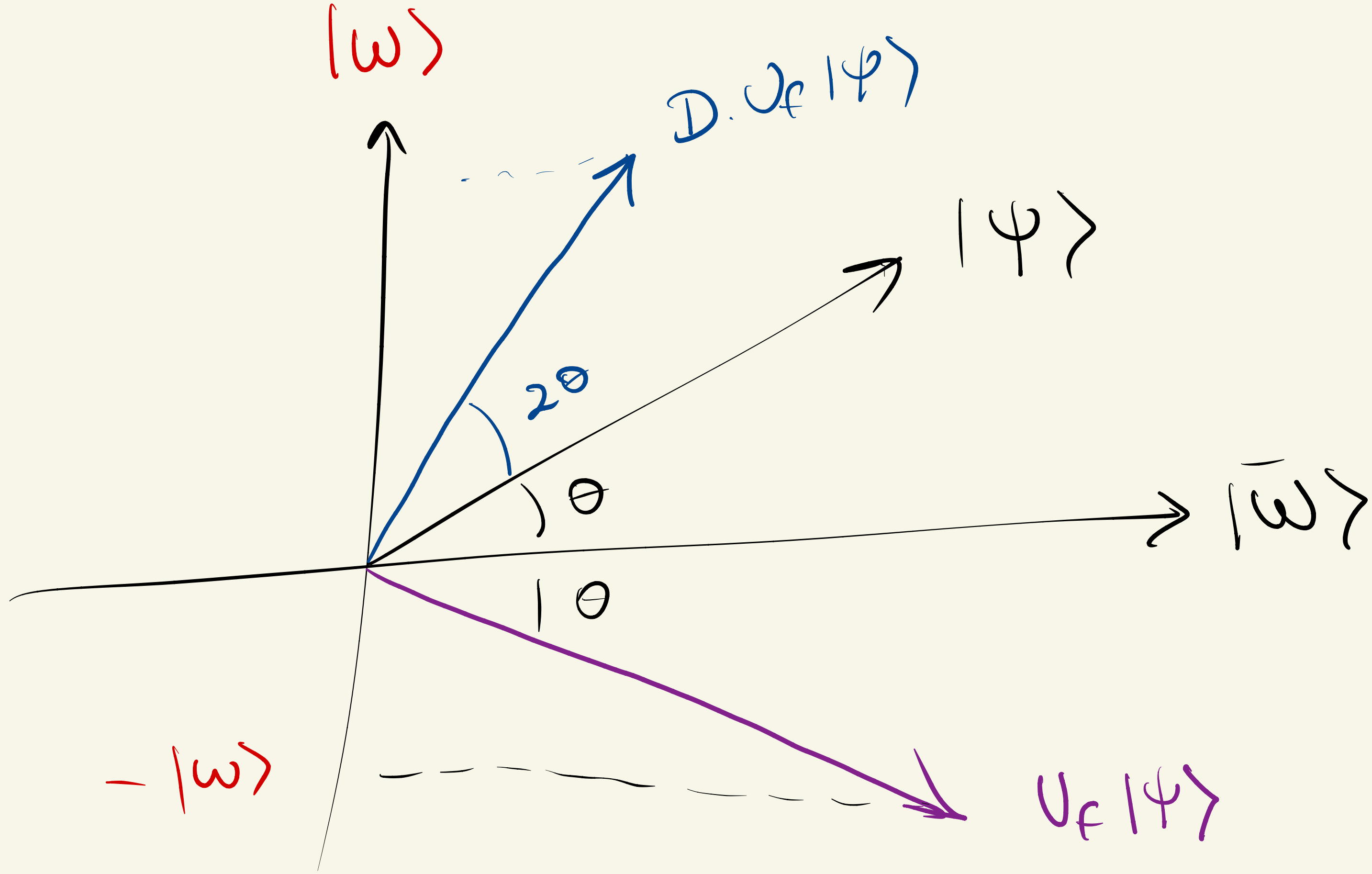


Effect of the oracle on $|\psi\rangle$?



what if we reflected over $|\psi\rangle$?

Probability would increase with an angle of 3θ !



$$\boxed{D = 2|\psi\rangle\langle\psi| - I}$$

$$D = 2|\psi\rangle\langle\psi| - I$$

$$= 2\, H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I$$

$$= 2\, H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - H^{\otimes n}H^{\otimes n}$$

$$= H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n}$$

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & & & \vdots \\ 0 & & 0 & & \vdots \\ 0 & & & & \vdots \\ 0 & \cdots & & & \end{pmatrix}$$

$$2|0\rangle\langle 0| - I$$

$$= \begin{pmatrix} 1 & & & & & \\ & -1 & & & 0 & \\ & & -1 & & & \\ & & & -1 & & \\ & 0 & & & \ddots & \\ & & & & & -1 \end{pmatrix}$$

$\downarrow$

-1 phase in every state except $|0\rangle$.

$$2|0\rangle\langle 0| - I$$

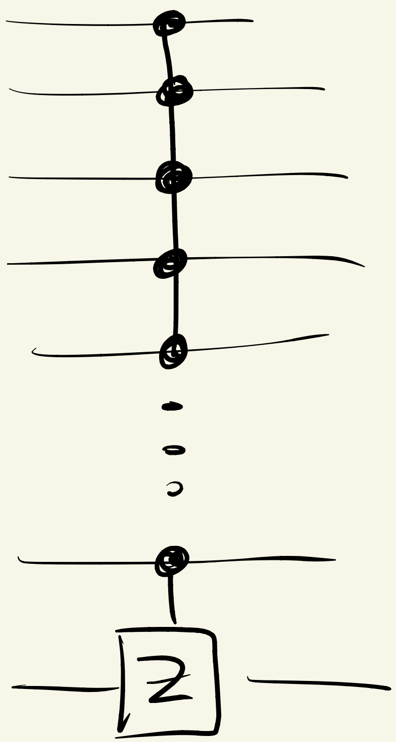
$$= -\begin{pmatrix} -1 & & & & & \\ & +1 & & & 0 & \\ & & +1 & & & \\ & & & +1 & & \\ & 0 & & & \ddots & \\ & & & & & +1 \end{pmatrix}$$

$\downarrow$

-1 phase in state $|0\rangle$

what gate implements this?

multicontrolled Z gate



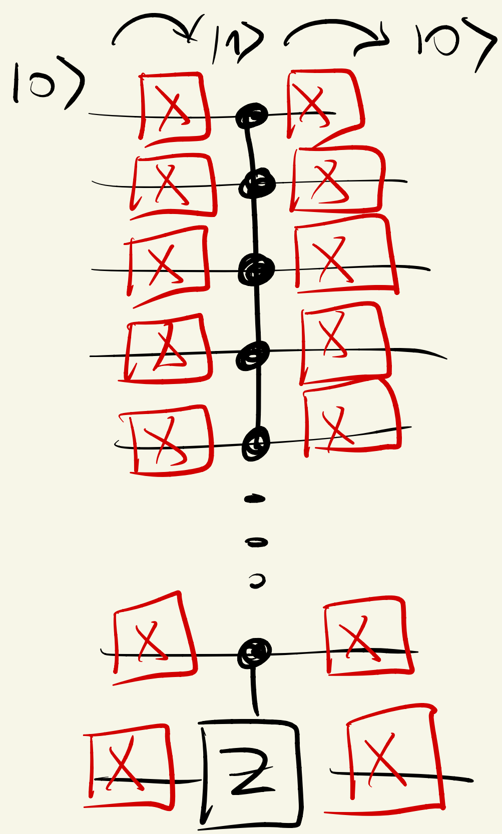
$\rightsquigarrow$ Applies phase (-1)

to state $|111\cdots1\rangle$

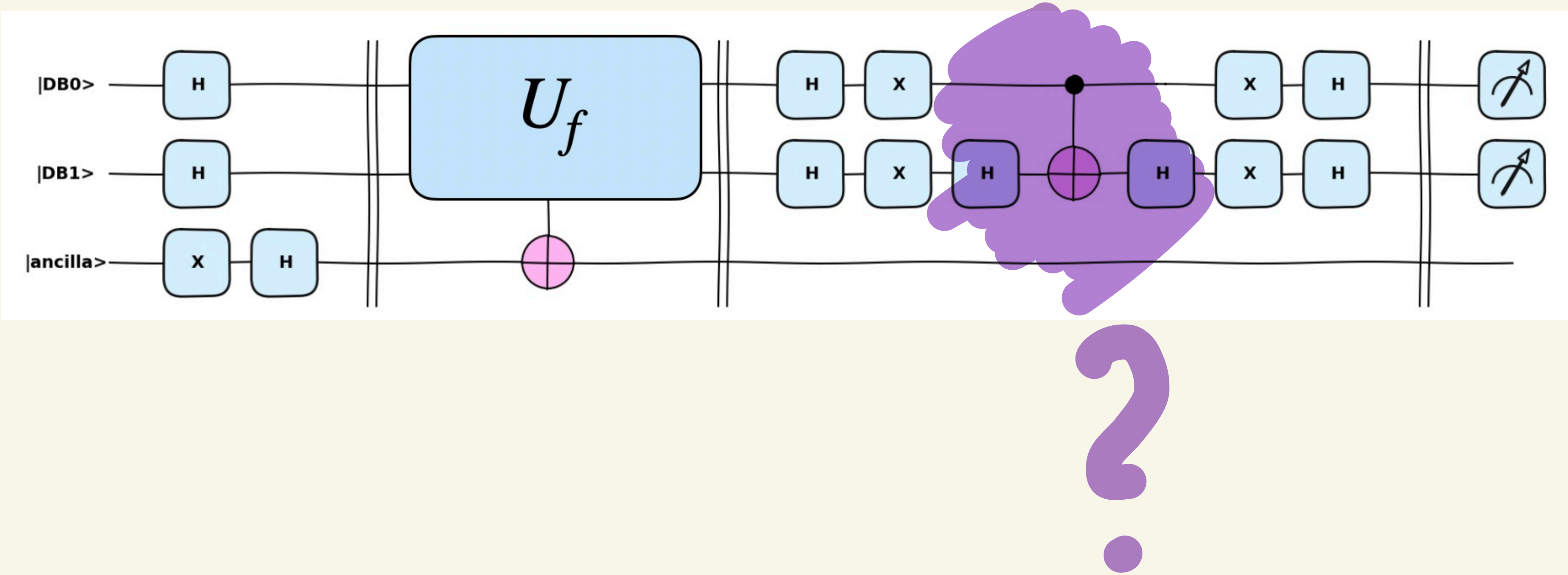
but we want

$|000\cdots0\rangle$

multicontrolled z gate

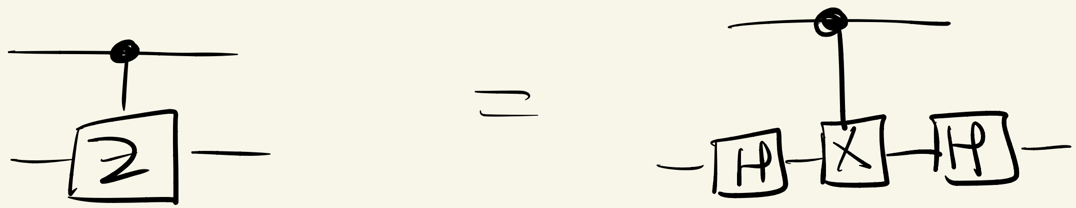


$\rightsquigarrow$ Applies phase (-1) to state $|000\cdots0\rangle$


|DB0>
|DB1>
|ancilla>
X
H
H
H
U_f
H
X
H
X
H
H
X
H
X
H
?

$$Z = HXH$$

Extends to controlled gates



How many times should we apply $U_f + D$?

Each application of D adds 2θ.

for j iterations, the goal is:

$$\operatorname{sen}^2\left((2j+1)\theta\right) \simeq 1$$

$$\Downarrow$$

$$\operatorname{sen}^2(\theta) = \frac{1}{2^n}$$

$$\arcsin(1) = \frac{\pi}{2}$$

$$\theta = \arcsin\left(\frac{1}{\sqrt{2^n}}\right)$$

$$J \simeq \frac{\pi}{4} \frac{1}{\arcsin \frac{1}{\sqrt{2^n}}} - \frac{1}{2}$$

$\arcsin(x) \simeq x$ for $|x| \ll 1$ $\quad N \to \infty$

Asymptotically, $J \in O\left(\sqrt{2^n}\right)$

$\sqrt{2^n}$ calls to the "database" or function to find solution!

Questions:

→ what if $\mathcal{J}$ has more than one solution?

→ what if we do not know the number of solutions?