Grover's Search Algorithm

Learning Goals

- Practice analyzing a new (2nd most famous) q. algorithm w/ geometric technique
- Learn an important q. algorithmic subroutine

Search Problem

Input: $f: \{0,1,2,\ldots,N-1\} \to \{0,1\}$ s.t.

- $\exists\ s: f(s)=1$
- for all other $x \neq s$, $f(s)=0$

Output: s

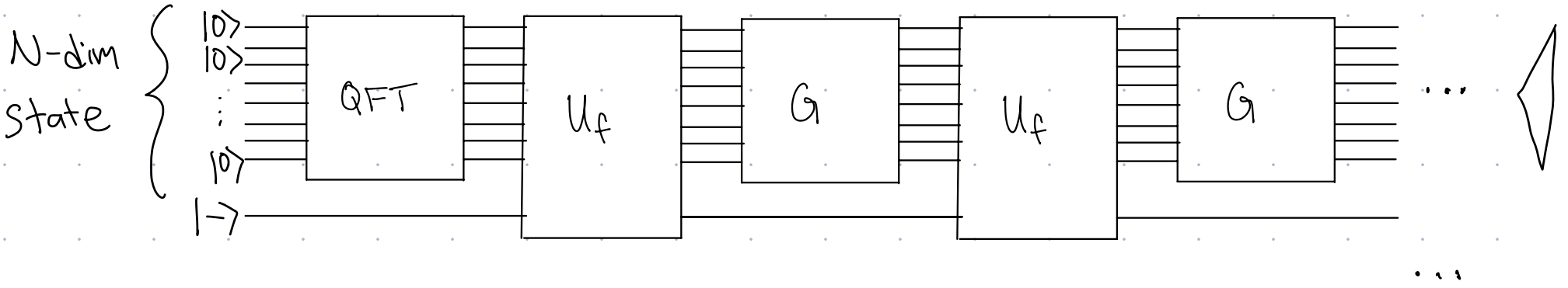
What is the classical query complexity (deterministic)?

A) $O(1)$ B) $O(\log N)$ C) $O(N)$ D) $O(2^N)$

What is the classical query complexity (probabilistic)?

A) $O(1)$ B) $O(\log N)$ C) $O(N)$ D) $O(2^N)$

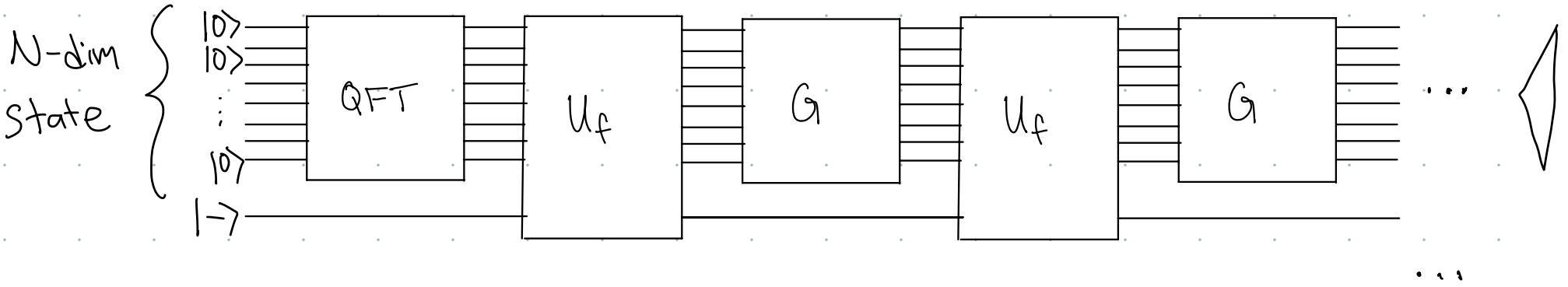
Grover's Algorithm (Quantum Search Alg)



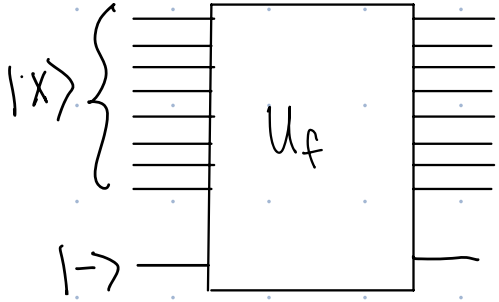
How many qubits are needed to search N possible inputs to f?

A) $\log_2 N$ B) $\log_2 N + 1$ C) N D) $N + 1$

Grover's Algorithm (Quantum Search Alg)



U_f:

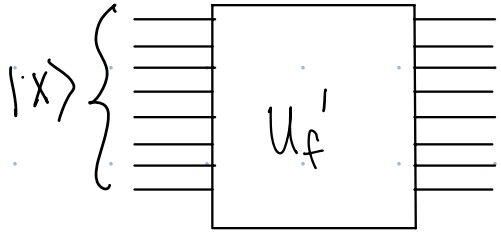


Phase Kickback: (If $|x\rangle$ is standard basis.)

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

$$U_f|x\rangle|-\rangle =$$

⇕ effective



$$U_f' =$$

$$U_f'|s\rangle = (I - 2|s\rangle\langle s|)|s\rangle$$

$$U_f'|x \neq s\rangle =$$

$$=$$

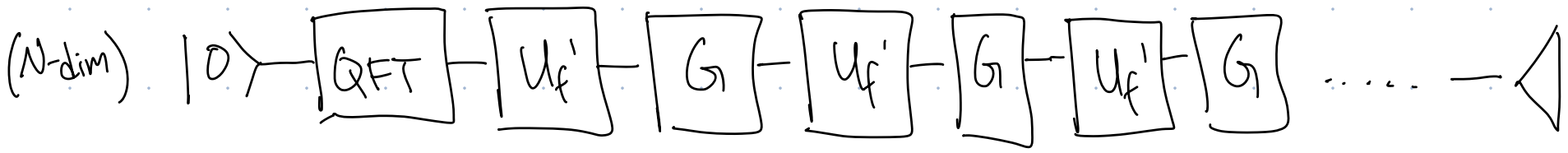
$$=$$

G (Grover Diffusion Operator)

$$G =$$

$$G|\gamma\rangle =$$

Grovers Alg: (Effective)



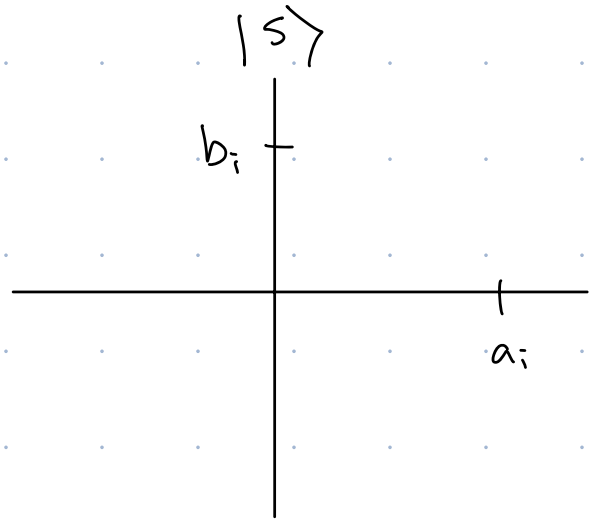
While the state is 2N-Dimensional, throughout the alg, state only stays in 2 of those 2N dimensions.

In other words, we can describe the state as a superposition of 2 states instead of N.

In particular:

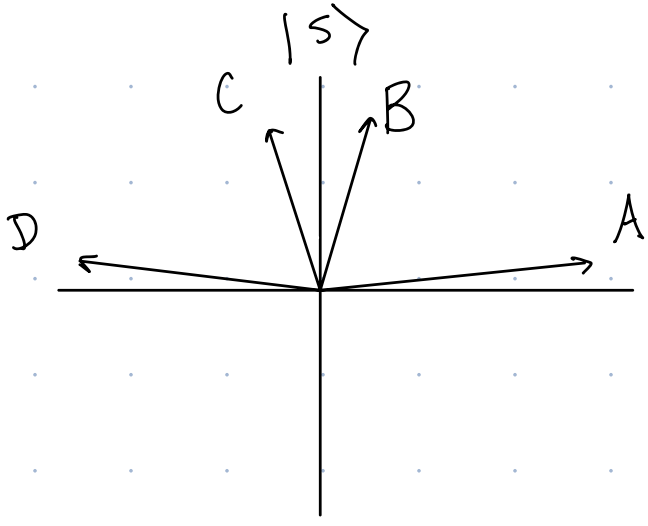
$$|\psi_i\rangle =$$

We can express $|\psi_i\rangle = a_i|\beta\rangle + b_i|s\rangle$ as a vector in 2D:



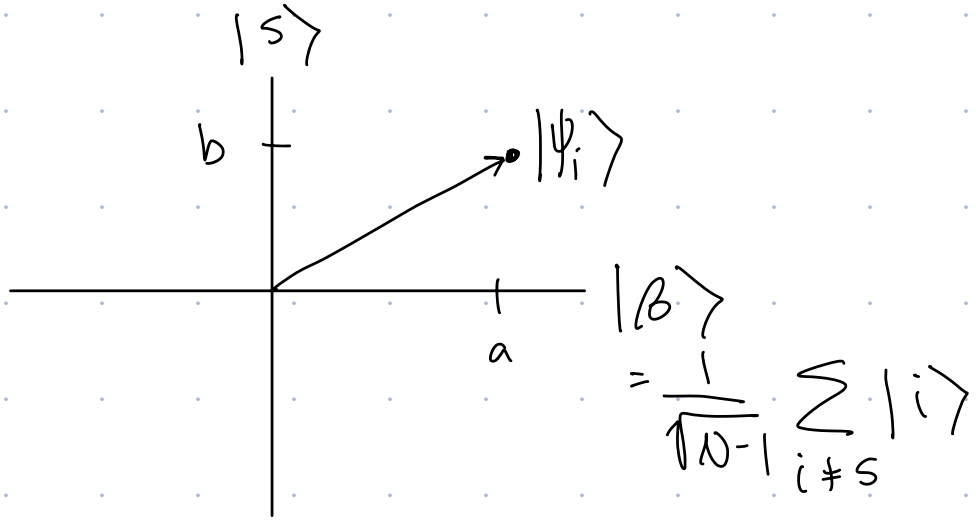
$$|\beta\rangle = \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

Where is $|\alpha\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$? (assume N is big)



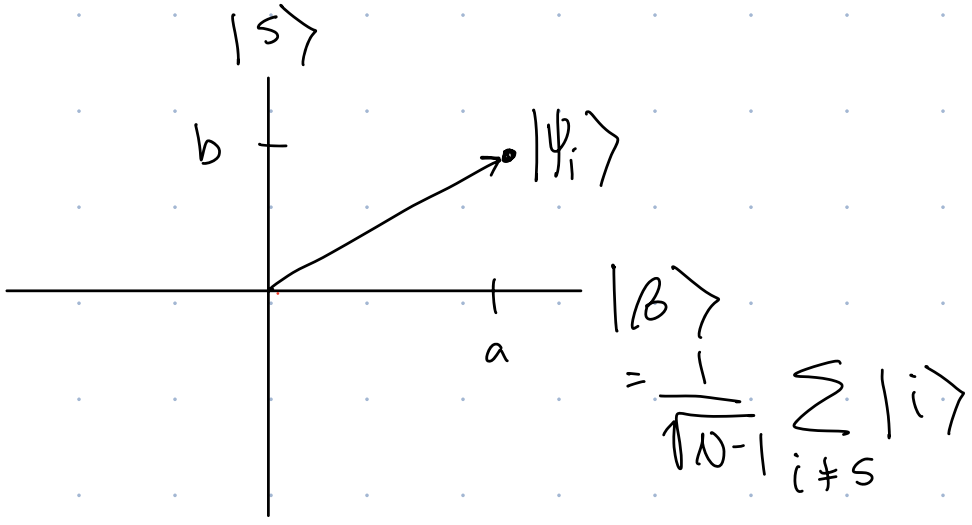
$$|\beta\rangle = \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

Effect of $U_f' = I - 2|s\rangle\langle s|$



$$= \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

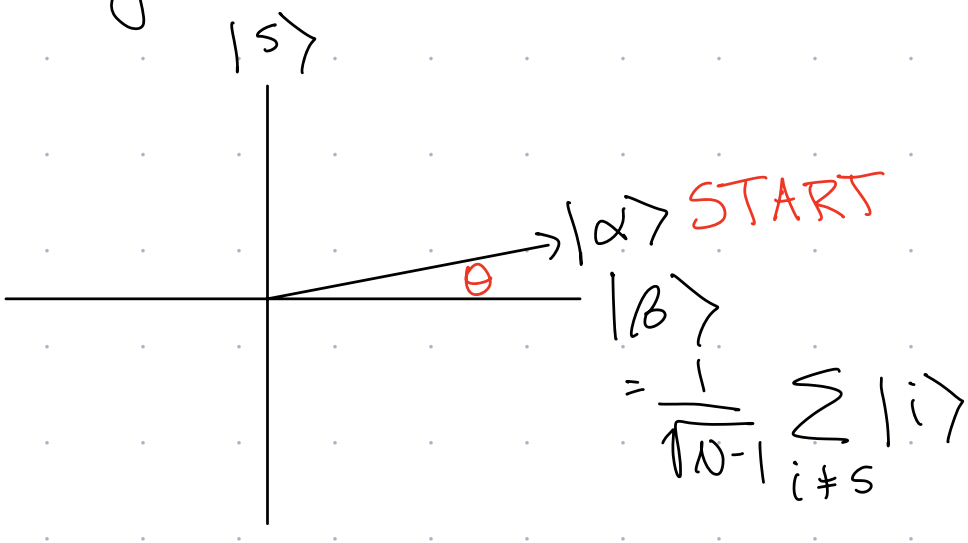
Effect of $G = -I + 2|\alpha\rangle\langle\alpha|$



$$= \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

How many iterations before state becomes $|s\rangle$?

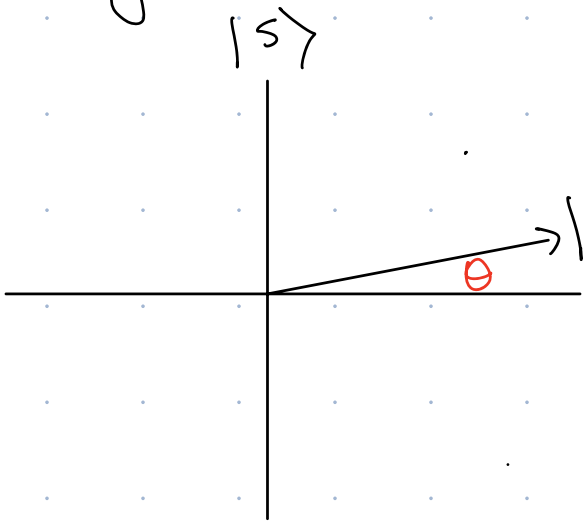
$(U_f', G, U_f', G, \ldots)$



$$= \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

$\tan^{-1}(x) \approx x$ for $x \ll 1$

How many iterations before state becomes $|s\rangle$?



START

$$= \frac{1}{\sqrt{N-1}} \sum_{i \neq s} |i\rangle$$

Note

Searches for input to a function – not a search through data.

Application

Suppose have classical alg that succeeds with prob p.

$$f(c) = \begin{cases} 1 & \text{if coin flips } c \text{ lead to success} \\ 0 & \text{else} \end{cases}$$

Can create a quantum alg that searches for set of random choices that causes alg to succeed.

ex: Best classical 3-SAT alg:

↳ Grover Quant. Alg with runtime:

Can do for any alg. → not that exciting theoretically