# GROVER SEARCH

# Problem 3

The Grover search algorithm is a Quantum Search Algorithm which finds a given required state from a database by the means of superposition and Amplitude Amplification

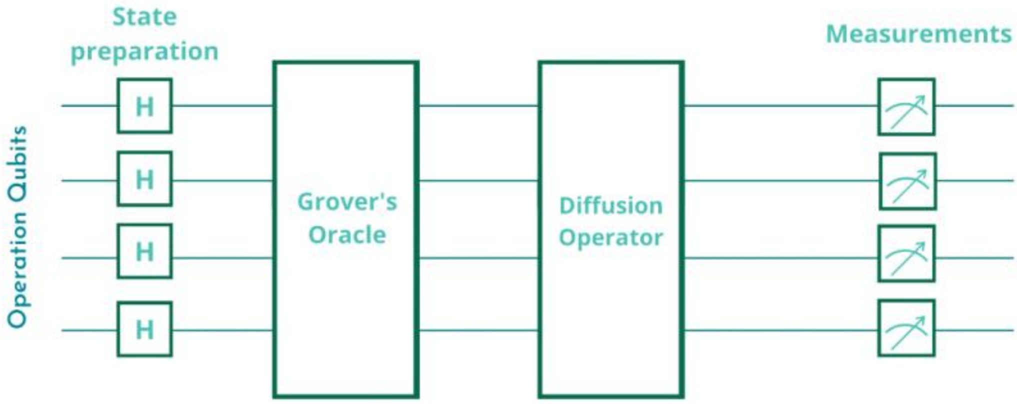
Here we discuss and instance of Grover Search which finds a marked state from a 3 qubit database

Overview of Algorithm:
The Grover Algorithm happens in 3 broad stages

Stage 1
Creating a superposition of states in the search space

Stage 2
Amplitude inversion of the state to be searched (marked state)
This step is done by and ORACLE

Stage 3
Amplitude Amplification of the marked state in the search space
This step is done by an Diffusion Operator.



## Stage 1: Superposition

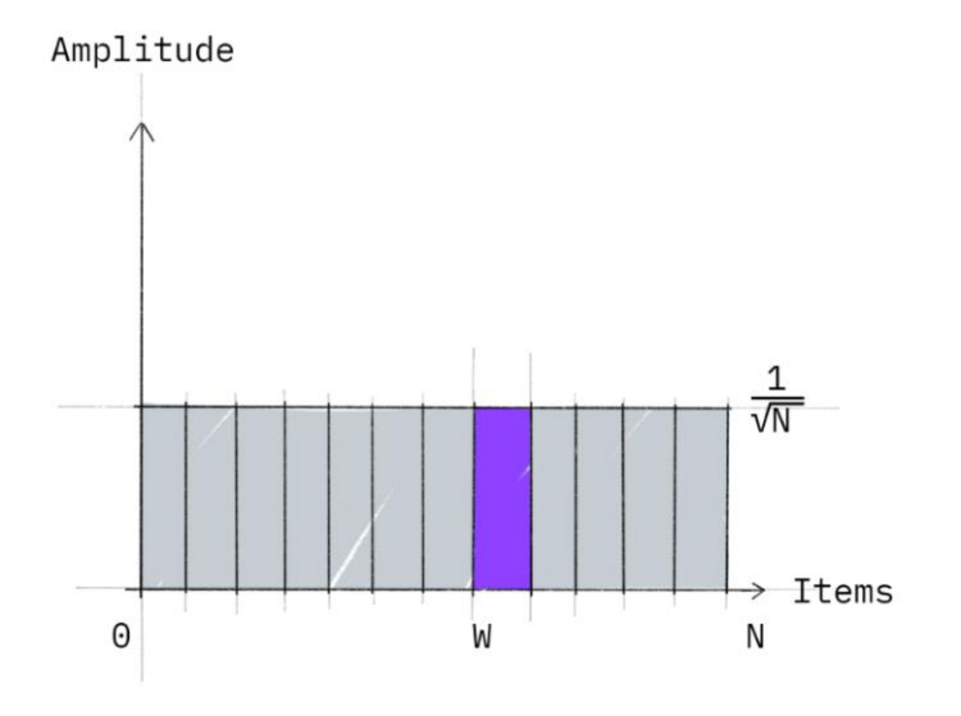
For N qubits taking the value of 0/1 we can have a total of 2^n different input states in the computational basis.

We initialize all qubits to state
|000000.....⟩

We apply a Hadamard gate to get to a superposition state |++++++.....⟩

Where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$

This way we get an equal superposition of all 2^n input states

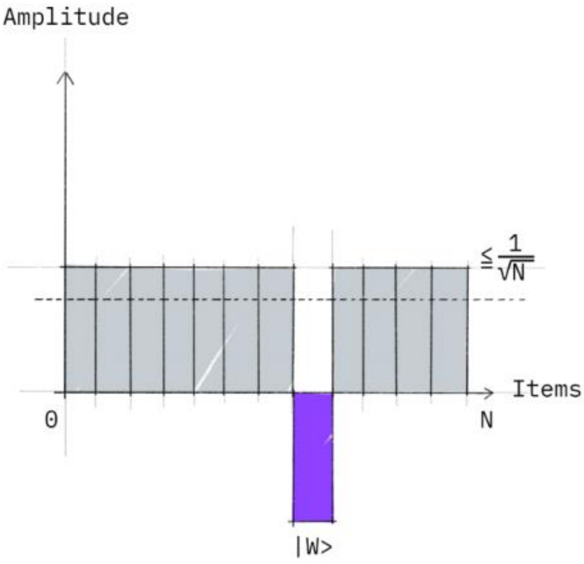


The state W is the state we want to search for but right now it has the same probability as everything else

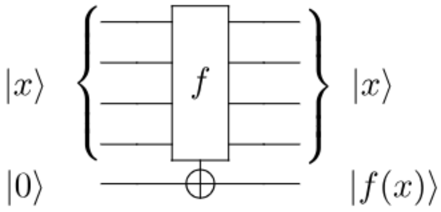
## Stage 2: ORACLE

The ORACLE is the part of the circuit which introduces a exp{iπ/2} to The marked state. i.e. It multiplies the marked state in the superposition state vector by -1

This is done by a phase kickback method through a ancilla qubit

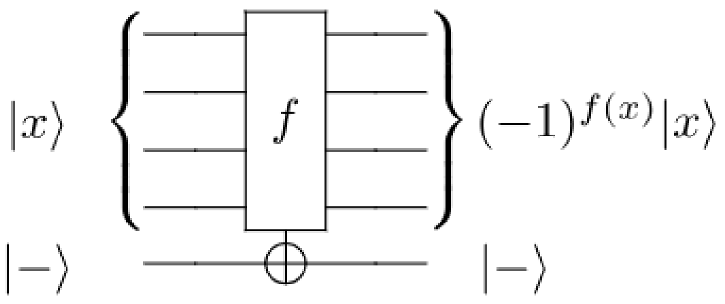


General idea for designing the ORACLE:
The oracle implements a function f(x)
Such that:
f(x) = 1 if |x⟩ =|w⟩
f(x) =0 if |x⟩ !=|w⟩



We first consider the following circuit

Then we initialize the ancilla qubit to |-⟩ state to get a phase kickback non the state |x⟩



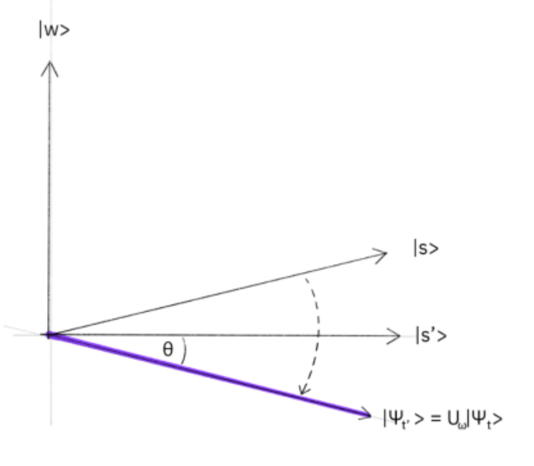
Hence :
|x⟩ =   |x⟩  if |x⟩ ! =|w⟩
|x⟩ = -|x⟩  if |x⟩ =|w⟩

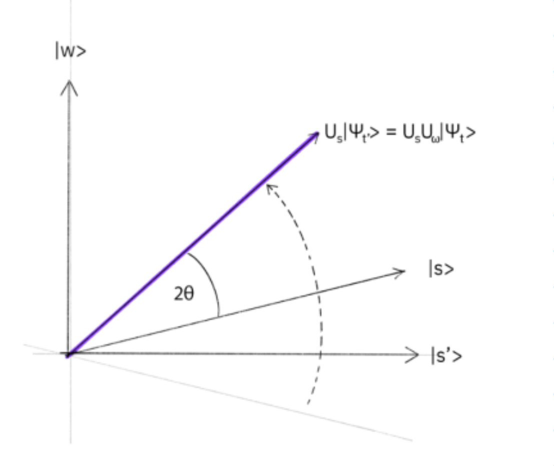
For a given state to search for we can make the oracle using x gates and multiqubit controlled x gates as shown in the jupyter notebook

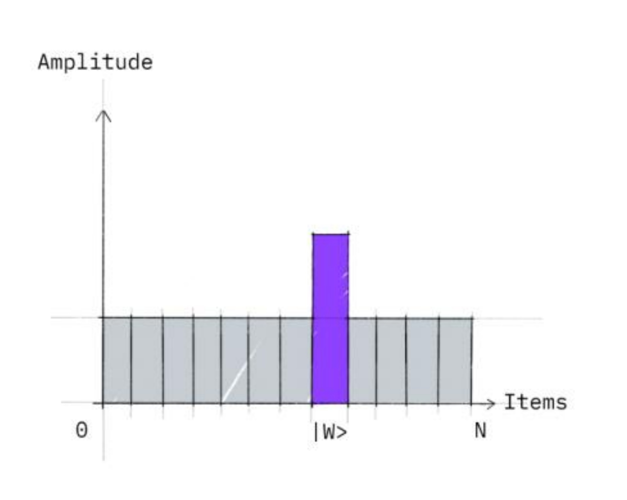
Stage 3: DIFFUSION
After the ORACLE we have a state vector  |Ψ⟩

The diffuser reflects the this state vector w.r.t to the superposition state vector. This in turn increases the amplitude of the marked state and reduces that of unmarked states.

## Implementation of the diffuser

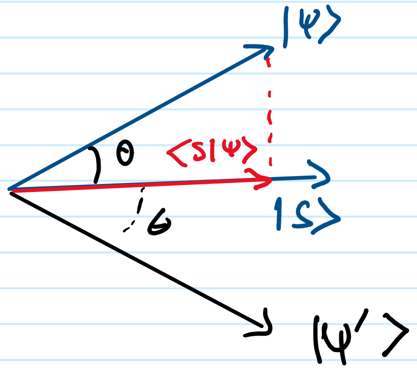






State $|s\rangle = |+\rangle^{n}$

For reflection of a state $|\psi\rangle$ w.r.t som $|s\rangle$



$$\boxed{D\,|\psi\rangle = |\psi'\rangle}$$

Now we can observe that $|\psi\rangle + |\psi'\rangle = 2\psi.s\,|s\rangle$

$\therefore\ |\psi'\rangle = 2(\psi.s)\,|s\rangle - |\psi\rangle$

$$\therefore\ \boxed{D = 2\,|s\rangle\langle s| - I}$$

## Now

$$D = \left(2|+\rangle^n\langle+|^n - \mathbb{I}\right)$$

Consider the operator M

$$\hat{M} = H^n \, D \, H^n$$

$$\therefore \hat{M} = \left(2.|0\rangle^n\langle 0|^n - \mathbb{I}\right)$$

if we observe the effect of M we see that :-

$$M|x\rangle = |x\rangle \quad \text{if } |x\rangle = |0\rangle^n$$

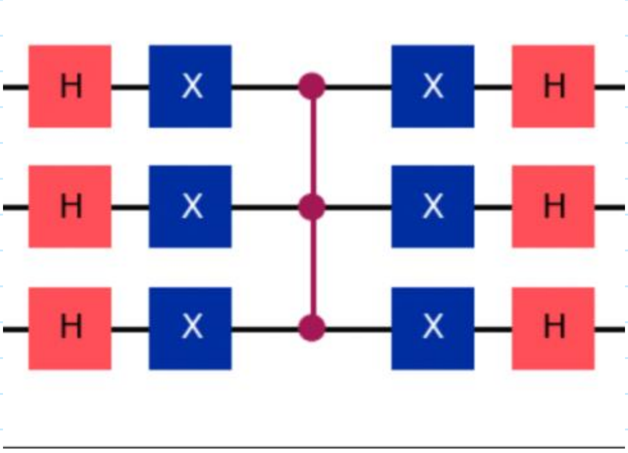
$$M|x\rangle = -|x\rangle \quad \text{if } |x\rangle \neq |0\rangle^n$$

we can implement M as $-\left(X^n (MCZ) X^n\right)$

we can ignore the -ve sign as it is a global phase to the circuit.

$$\therefore \boxed{D = H^n\left(X^n (MCZ) X^n\right) H^n}$$

implemented in notebook.

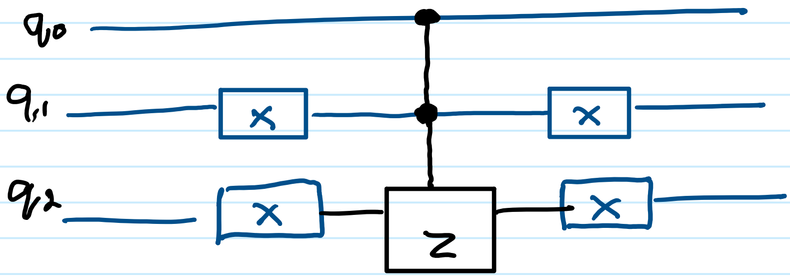


Diffusion operation for 3 qubits

## NO ANCILLA CONSTRAINT

If the marked state is known beforehand we can design an ORACLE which doesn't use an ancilla qubit. This method doesn't rely on phase kickback for state marking.

E.G. For a 3 qubit superposition state oracle to mark the state 100 we can make it as follows:



## NO Z Gate CONSTRAINT

We can design the entire circuit without using the Z gate and replacing it by HXH gates instead

Z = HXH

## NO X Gate CONSTRAINT

We can design the entire circuit without using the X gate and replacing it by HZH gates instead

X = HZH

## Performance

The Grover search algorithm repeatedly uses the oracle and diffuser O(sqrt(N)) times where N = 2^n (n:- no. of qubits)

After floor(sqrt(N)) the oracle and diffuser starts to drive the statevector away from the marked state. Hence the maximum probability of finding the marked state happens after floor(sqrt(N)) repetitions.

**ADVANTAGE OVER CLASSICAL SEARCH**

The Grover algorithms provides a O(sqrtN) time complexity for a Black Box search problem. i.e. it can perform any search (structured or unstructured in O(sqrtN) complexity)

For structured search the classical binary search has a time complexity of O(logN) and hence is faster than Grover

But for unstructured search the best classical time complexity is O(N)

Hence the Grover algorithmn give a quadratic speedup in this case