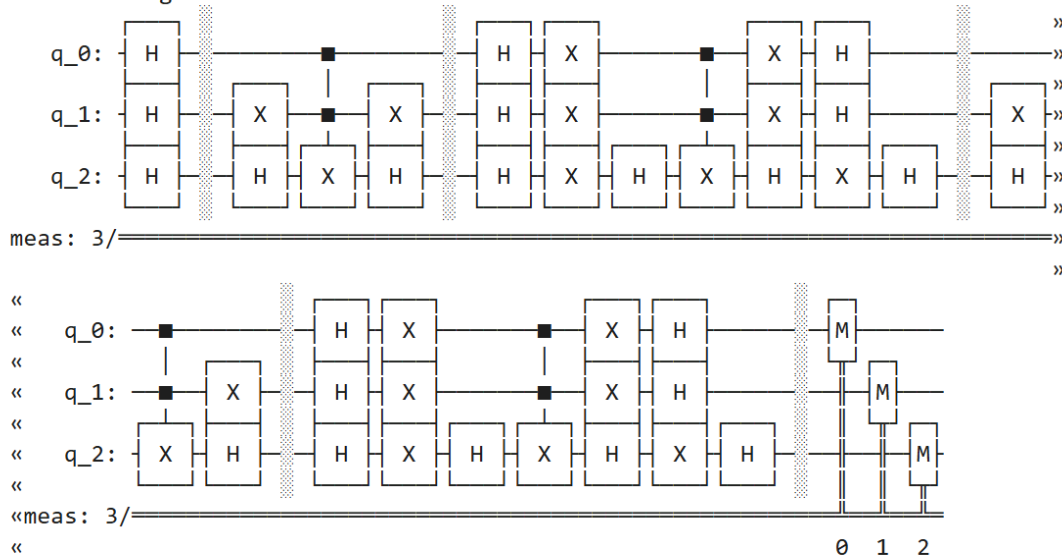


Circuit Diagram:



Circuit diagram for 3 qubits.

Target state = $|101\rangle$

In the explanation below I sometimes refer to 2 qubit grover with target state as $|11\rangle$ for simplicity.

1. Initialization:

First apply Hadamard gate on all input qubits. Same as the math.

Now we have a superposition of all possible 8 states. That's what Hadamard does.

Current state of the system: $|s\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ (This is 2-bit state, apply to 3-bit similarly).

2. Oracle function circuit:

2a. Aim of the Oracle is to change the sign(phase) of the target state in $|s\rangle$

So that the new state is: $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ (For the 3 bit system all positive except $|101\rangle$)

2b. Note that the black dots(controls) on q0 and q1 are activating Z gate(HXH) on q2. Z gate is for phase flip. In the math we noticed that we want to change the sign(phase) of the target state. Here target state is $|101\rangle$ so there is an X-gate on q1 so that the Z gate on q2 will activate only when $q_0 = 1$ and $q_1 = 0$.

2c. Phase flip on q2 is as good as phase flip on the entire system $q_0q_1q_2$.

So effectively, all states in the superposition are positive except the target state which is now negative.

So current state = $|s\rangle - |w\rangle$ where w = target state.

3. Diffuser function circuit:

As per the math we wanted to apply this operator:

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

How to convert it to a quantum circuit?

To do that remember that H-gate is inverse of itself.

So $H|000\rangle = |s\rangle$ and $H|s\rangle = |000\rangle$

We will use this to show that:

$2|s\rangle\langle s| - I = H \times (2|0\rangle\langle 0| - I) \times H$ (here \times denotes matrix multiplication).

Ok, so here is the proof:

We know that $|s\rangle = H|0\rangle$

For 2 qubit system H is a 4x4 matrix and $|0\rangle$ is a 4x1 column vector.

So $|s\rangle$ will be a 4x1 matrix(or column vector) resulting by multiplication of 4x4 and 4x1 matrices.

Similarly:

$\langle s| = \langle 0|H$ (it follows from the fact that H is symmetric and its own conjugate transpose.

Again LHS is $1 \times 4 = 1 \times 4$ mult 4×4

So:

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

$$= 2(H|0\rangle)(\langle 0|H) - I$$

$$= 2(H)(|0\rangle\langle 0|)(H) - I$$

I can be written as $H.I.H$ (. means matrix mult). Since H^*H is also I. H is its own inverse.

$$= 2(H)(|0\rangle\langle 0|)(H) - H.I.H$$

$$= H.(2|0\rangle\langle 0| - I).H$$

So this can be implemented easily as a quantum circuit.

In the circuit diagram you can see H gates at beginning at end, they directly map to this.

Now focus on the part in-between:

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

Let's see what happens when we apply it on any state.

When it is applied on all zeroes, i.e. $|000\rangle$, we get:

$$2|0\rangle - |0\rangle = |0\rangle$$

So it remains unchanged.

But on any other state, e.g. $|100\rangle$ the first part of multiplication will become all zeroes since there is no overlap in $|000\rangle$ and $|100\rangle$ so effectively the result will be $-|100\rangle$

So for $|000\rangle$ (all zeroes), the output is same as input, for every other state the sign gets flipped.

Now look at the circuit.

We have X-gate columns adjacent to H-gates.

And in between we have Z-gate(phase-flip, H.X.H) which gets activated only if all 3 inputs are 0s(the X-gates ensure that).

And X-gates at the end undo this.

So this is how diffuser is implemented as a quantum circuit.