Script for Video

Hey guys. Today we will be talking about Grovers algorithm and how YOU can use a quantum computer to your advantage.

First, for some background. Here is Lov Grover, creator of Grover’s search algorithm. Grover invented Grover’s Algorithm in 1996 and it is one of the most famous and most widely used quantum algorithms that exist today.

First, let’s talk about a computational problem that you might run into. Let’s say you have some list of items, and you want to find the position of one item in particular. In this case, we are looking for the position of 5 in the list.

The main method computers have to look for an item in a list like this is by going item by item. Start from the first item in the list and check if it is 5. If not, continue on. We call the component that looks at each element the oracle.This algorithm has a runtime on the order of the number of elements in the list, or as computer scientists say, it is order N.

Instead, we can use a quantum computer. Now, a classical computer uses bits of information; either something is 1 or 0. CLICK Quantum computers, on the other hand, can have individual qubits that are a combination of 0 and 1. This is a quantum computer in a nutshell. This might seem complicated, but try to think of a qubit as a vector in the x, y plane. Instead of x,y however, imagine it is the 0,1 plane. A vector in this plane has both a 0 component and a 1 component.

For a quantum computer, we first put all qubits into a superposition of 0 and 1.CLICK Our goal is that our state vector will be 1 for the item that has 5 in it, and 0 everywhere else. We obtain this by applying the quantum version of the oracle, which negates all states that are 5, and then our diffuser, which applies a reflection in the vector space. The oracle and the diffuser together get our state vector closer to w, or it amplifies its likelihood of being measured, since quantum computers work probabilistically. We call the oracle and the diffuser together the amplifier, and we apply multiple amplifiers depending on the size of our list. The order of this algorithm is of order sqrtN,which is significantly faster than the classical counterpart.

Moving on to our implementation. We implemented a 2 qubit Grover’s Algorithm on a Jupyter Notebook. This a very simple example of Grover’s Algorithm, but it still serves to demonstrate each component of the algorithm we want to show.

Here we have the main three components of the Grover’s Algorithm circuit that we are implementing. We begin with a Hadamard gate on each qubit to set them into the desired superposition. Next, we apply the Oracle matrix which, as mentioned previously, gives a negative phase to the desired state, separating it from the other possible states. In our case, the Oracle matrix is simply a controlled z gate. Last, we add the Diffuser. This reflects the state across its original position, bringing it much closer to the desired state. The diffuser consists of a Hadamard gate, z gate, controlled z gate, and then another Hadamard gate on each qubit. Finally, we add the measurement gates in order to, as the name would entail, measure our circuit. This circuit is designed so that |11> is the desired outcome that we are searching for.

After running our circuit on one of the open source IBM quantum computers, we obtain a histogram of the outcomes. As we can see, the desired state of |11> was found the vast majority of the time, meaning that our algorithm was a success. We see small amounts of incorrect results due to the decoherence associated with quantum computers. For our two qubit circuit, one application of the amplifier was enough to recover the desired state. However, you may need to pass many times through the amplifier in order to obtain the desired state. We implemented a convenient way to add multiple amplifiers onto our circuit. Shown here is a three-amplifier circuit, as well as the results from running it. As mentioned before, this triple amplification is not needed in our case, so the results are not particularly interesting, but it is useful to have the capability for this nonetheless.

The applications for Grover’s algorithm are extremely wide ranging. For example, in 2020, a group in cornell used Grover’s algorithm to search through data at the Large Hadron Collider to find rare instances of 4 lepton Higgs Boson production events. Grover’s algorithm can also be used in applications in cryptography for both breaking and securing encryptions along with translating random walk algorithms into their quantum counterparts, both of which are extremely important in physics, computer science and data science.

And this is how you use a Grovers algorithm on a quantum computer. Further information about any part of this presentation can be found in these references. Be sure to check them, and our repository out to test yourself.

Thanks for watching. Remember, keep calm and Grovers on.