Comp Sci 880 HW1

Hongtao Zhang

March 23, 2023

Contents

1 Question 1

What we want to do is to split the real part and the imaginary part, and then do calculation with only real entry but resulting complex effect.

Firstly we need to split the amplitude into two part. It is easy to check that the RHS also have 2-norm 1.

$$\begin{pmatrix} a+ci \\ b+di \\ 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \tag{1}$$

(Based on Piazza post, we can assume this transformation is given)

Then we can do the calculation with only real entry, and then combine the result back.

For any Complex Unitary $U_c = A + Bi$, we can represent it with a real unitary matrix U as

$$U = \begin{pmatrix} A & -B \\ B & A \end{pmatrix}$$

Then its action on the state vector $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ is exactly the same as the action of U on the state vector $\begin{pmatrix} a+ci \\ b+di \\ 0 \\ 0 \end{pmatrix}$ with the transformation (1).

The thing left to check is that the matrix U is unitary.

Proof.

$$\begin{aligned} UU^* &= \begin{pmatrix} A & -B \\ B & A \end{pmatrix} \begin{pmatrix} A^* & B^* \\ -B^* & A^* \end{pmatrix} \\ &= \begin{pmatrix} AA^* + BB^* & AB^* - BA^* \\ BA^* - AB^* & AA^* + BB^* \end{pmatrix} \end{aligned}$$

We know that matrix $U_c = A + Bi$ is unitary, so $U_c U_c^* = I = (A + Bi)(A + Bi)^T$

$$\begin{aligned} (A + Bi)(A + Bi)^* &= (A + Bi)(A^* - B^* i) \\ &= AA^* - AB^* i + BA^* i - B^* iBi \\ &= AA^* + BB^* - AB^* i + BA^* i \\ &= I \end{aligned}$$

Because I doesn't have complex entries, so $AB^* i + BA^* i = 0$, which means $AA^* + BB^*$. Therefore, $UU^* = I$. Therefore, $AA^* + BB^* = I$, which means U is unitary. □

Finally, if we do a measurement on the first m qubits, we will get the same result for the complex gates on the first m qubits, because the amplitude of the real and complex entries will be superposed given the last qubit is not measured.

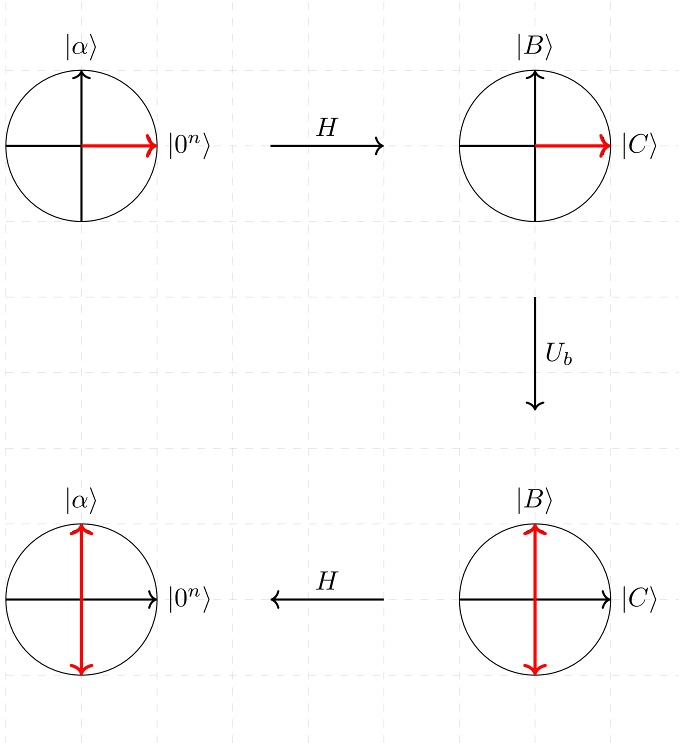
2 Question 2

For Deutsch-Jozsa, we firstly apply the Hadamard gate on all qubits, then apply the oracle, and then apply the Hadamard gate on the first qubit.

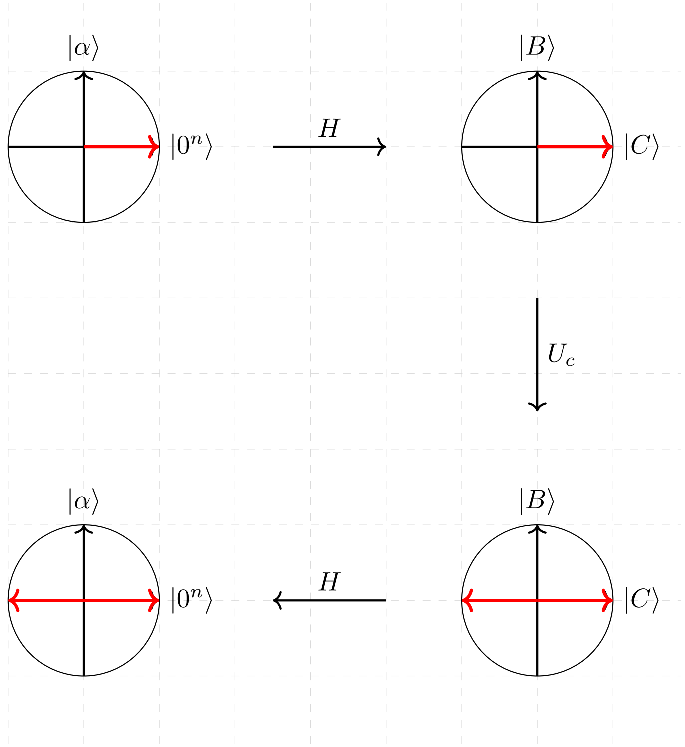
Then we can view the Hadamard gate as the transformation to the amplitude axis, and the phase kickback as the the Oracle and Reflection in Grover, and the other Hadamard gate as the transformation back to original basis.

The overall goal is similar, to transform the final state to a particular state that is either good (Grover), or to a state that we can distinguish from (Deutsch-Jozsa).

2.1 Balanced Function



2.2 Constant function



3 Question 3

We can create a controlled version of the black box so make sure the black box transform to a state that is orthogonal to each other.

In the solution in error elimination, we have learned how to create a controlled version of the phase kick back black box. We can use this to create a controlled version of the black box.

The idea is to have a black box that is controlled by an additional ancilla that has uniform probability between $|0\rangle$ and $|1\rangle$.

Then we can just apply the same analysis as in the Deutsch-Jozsa algorithm.

In this case, the black box will be applied with probability $\frac{1}{3}$.

If the black box is the constant case (i.e. $2^n 0$), then the resulting distribution of the modified black box is identical to the original black box, with up to a global phase change.

If the black box is with 2^{n-2} 0 and 2^{n-1} 1, then the resulting distribution of the modified black box will be

$$P(x=0) = p + \frac{1}{4} \cdot (1-p) = \frac{1}{3} + \frac{1}{4} \cdot (1 - \frac{1}{3}) = \frac{1}{3} + \frac{1}{6} = \frac{1}{2}$$

Therefore, the resulting distribution is uniform, so the black box is balanced.

Therefore, we can follow the same algorithm as in the Deutsch-Jozsa algorithm.

4 Question 4

4.1

If two graph are isomorphic, then there must exist some permutation of the vertices such that $G_1 = G_2$.

On the other hand, it is impossible for two graphs that is not isomorphic to have any permutation of the vertices that is the same. Therefore, $\sigma(G_1) \perp \sigma(G_2) \iff G_1 \cong G_2$

4.2

We know that if two graphs are isomorphic, then there must exist some permutation of the vertices, so there will exist some destructive interference between the two resulting distribution.

However, I am not really sure how to approach the destructive interference. There are a few guesses below.

We know that when we are applying Hadamard twice to state $|0\rangle$, we will get $|0\rangle$ with probability 1 because of the destructive interference during the second Hadamard.

Then I guess if we apply Hadamard to both distribution, then do a complete **CNOT** from one distribution to the other, then apply Hadamard to both distribution again, then do a measurement on the first distribution. I guess it will result in a $|0^m\rangle$ with probability 1.

If the two distribution are orthogonal, I claim that the resulting distribution will only have very small probability of $|0^m\rangle$.

4.3

There exists a way to perform permutation on graph classical doesn't imply that it is possible to perform superposition of permutation on graph to achieve superposition quantumly in polynomial time.

5 Question 5

First Attempt

The idea is very simple and like a binary search, each time we chunk half of the range, and see whether we can find the element in the chunk.

If we found, then the lowest index is in the chunk, otherwise it is in the other chunk.

We will need to do this n time.

Each time Grover search will take $O(\sqrt{N})$ time, so the final query complexity is $O(n\sqrt{N})$.

However, there will be an issue with the error, where the error will be amplified, because each time we apply Grover, there will be some error. Therefore, we actually need to bound the error of every single Grover search to be $\frac{1}{2n}$, which might require additional logarithmic factor of n.

Second Attempt

Notice that we didn't actually exploit the fact of the Grover search, which it might give a uniformly sample from the set of solutions.

Based on Markov inequality, with probability $\frac{1}{2}$, we will be in the bound $2\mathbb{E}[X]$, therefore, as long as we can have the expected runtime be within the required bound, with high probability, we will not exceed some constant times the bound.

Therefore, we will only consider expected bound in the following analysis.

The idea is an improvement of the previous algorithm, where we will use the fact that Grover search will give a uniformly sample from the set of solutions.

On the first round, we will do a uniform sampling of the possible from $[0, N]$ to get a point x_1. Apply f to the sampled value, and set the bound to be the value of $f(x)$. (it is equivalent to do a Grover search that uses the oracle that map everything to 1).

On the second round, we will do a Grover Search with the oracle U_f that only map the value that is within the $[0, f(x_1)]$to 1, and the rest to 0. If we find the result equal to x_1, then we succeed (try a few times) otherwise, we will repeat the process.

We will repeat this process until we find a close enough solution.

For every single run, we expect to remove half of the range, so the expected number of run is n. Each run we will need $\sqrt{\frac{N}{t}}$, where t is the size of the range.

Therefore, on average, we can expect the number of query be the following

$$\begin{aligned} 1 + \sqrt{\frac{N}{\frac{1}{2}N}} + \sqrt{\frac{N}{\frac{1}{4}}N} + \cdots \\ \approx 1 + \sqrt{2} + \sqrt{4} + \cdots \end{aligned}$$

which is a geometric series, which will converge some constant factor with $\sqrt{N}$.

We still might need to take care of the accumulated error, which might contribute to a logarithmic factor.

However, we can smartly avoid this error by checking whether the sample from Grover search is within the range that is actually makes sense. If it is not, then we perform a Grover search again, which by expectation, we might need on average two trials, which is a constant factor.

The probability of getting $x_1 = x_*$ is low, which is $\frac{1}{t}$, where t is the size of the range.

Then, if we just try some constant times, we can have high probability to make sure that we stop early only in some small probability.

The error at the end might not be removed, but it will be bounded by $\frac{1}{2}$ which is in the allowed range.