15-459: Undergraduate Quantum Computation	September 20, 2022

Lecture 7 : Biased or balanced

Lecturer: Ryan O'Donnell

Scribe: Rajeev Godse

1 Quantum programs and analysis

Recall:

1. If $F : \{0,1\}^n \to \{0,1\}$ is easy to compute classically, then "If $F(X_1, \ldots, X_n)$ Then Minus" is easy to compute quantumly in a trash-free way.

2. The operations Hadamard: $\frac{1}{\sqrt{2}}\begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$, Add&Diff: $\begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$, and Aug&Disp: $\frac{1}{2}\begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$ are all the same operation when we allow "unnormalized states."

   To compute Hadamard on the ith bit, we can pair up all states that differ on the ith bit and perform A&D on the two states (if a state is not present, it has 0 amplitude) to get the resulting amplitudes for the associated states.

2 Preparing "Uniform Superposition"

Recipe: Starting from n qubits initialized to 0, do H.A.T.! : H on each qubit, sometimes called the "Hadamard Transform."

Example: Say we start with amplitude 1 on 000. We want to know what is the result of H on A, H on B, and H on C.

Via Add&Diff, we get 1 on 000, 1 on 100. Then, we get 1 on 000, 1 on 010, 1 on 100, and 1 on 110[1]. Finally, we get 1 on all possible quantum states. The result is a quantum state with **uniform amplitudes**. It should be clear that this holds for all n.

Conclusion: After H.A.T.!, the final unnormalized state has amplitude 1 on all states, giving normalized state of amplitude $\sqrt{\frac{1}{\sqrt{2^n}}}$.

Upshot: Say $n = 3$, we H.A.T!, and we now initialize a new qubit called "Ans". Then suppose we "Add Maj(A, B, C) to Ans". We get uniform superposition on all states $ABCD$ such that $D = \mathrm{Maj}(A, B, C)$.

However, say instead we don't care about "Ans" and we instead do "If Maj(A, B, C) Then Minus". The resulting amplitudes are the "truth table" (-1 if the majority is 1, otherwise 1). The behavior if we do "Print All", we just get a uniformly random three bit string.

We can see something cool happen if we instead H.A.T.! on the sign-computed version of some F[2]. For the above example, we'll illustrate this by using Avg&Disp.

After H on A, we get amplitude 1 on 000, 0 on 100, 0 on 001, 1 on 101, 0 on 010, 1 on 110, -1 on 011, 0 on 111. Computing the rest of the transformation is a bit tedious, let's just figure out the final amplitude on 000. After H on B, we have amplitude $\frac{1}{2}$ on 000 and amplitude $-\frac{1}{2}$ on 001. Finally, after H on C, we get amplitude 0 on 000. This amplitude corresponds to the average of the initial amplitudes of all starting states.

[1]We can visualize this as a cube where there is an edge between states if they differ by 1 bit.

[2]This is the biggest, and perhaps only trick in all of quantum computing.

Theorem: After preparing the uniform superposition and sign-computing $F : \{0,1\}^n \to \{0,1\}$ and doing Hademard Transform, the final normalized amplitude on **0** is the **average** of F's 2^n $\pm$ values.

For general F, the final amplitude of **0** is 0 when F is **balanced**, i.e. it maps half of all n-bit strings to 1, and the other half to 0. If a function is not balanced, we say it is **biased**.

If F is balanced, then the amplitude on **0** is 0, so the probability of printing **0** is 0.

Otherwise, if F is biased, then the amplitude on **0** is non-zero, so the probability of printing **0** is strictly positive.

Call the above quantum program C_F. If F is easy in classical computation, then C_F is easy in quantum computation.

This is really cool! **Theorem (Deustch-Tozsa)**: If we had the same thing in the setting of classical computation, then $P^{\Sigma_2} = NP^{\Sigma_2}$.

But what about the other states? Let's return to the tedium and take for granted that we get:

- 0 on 000
- +1/2 on 001
- +1/2 on 010
- 0 on 011
- +1/2 on 100
- 0 on 101
- 0 on 110
- -1/2 on 111

Using our fancy notation, we could also say that the final state is $+\frac{1}{2}|001\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|100\rangle - \frac{1}{2}|111\rangle$.