QCQI: CHAPTER 5 SUMMARY

A PREPRINT

Krishna N Agaram

December 28, 2022

ABSTRACT

The Fourier Transform and applications.

1 The Fourier Transform

2 The Phase estimation algorithm

Consider a unitary operator U. Say $|u\rangle$ is an eigenvector with eigenvalue $e^{2\pi i\varphi}$. We would like to find (approximately) φ. We assume that we can query a blackbox to apply U^{2^j} for any $j \in \mathbb{Z}_{\geq 0}$. The key idea is to **encode φ into the phase space and then compute the inverse Fourier Transform**.

The key chain of events reads as follows (subscripts on the operator describe the qubit(s) it was applied to):

$$|0\rangle|u\rangle \xrightarrow{H_{[n]}^{\otimes n}} \left(\frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}|j\rangle\right)|u\rangle \xrightarrow[0\leq i\leq n-1]{U_{n-i}^{2^i}} \frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}|j\rangle U^j|u\rangle = \left(\frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}e^{2\pi ij\varphi}|j\rangle\right)|u\rangle \xrightarrow{\mathrm{IFT}_{[n]}} \approx |\tilde{\varphi}\rangle|u\rangle$$

whereupon measuring the first register gives us the estimate $0.\tilde{\varphi}$ for φ. The $\approx$ is for two reasons. One, that φ is possibly more than n bits long, in which case φ is an n-bit approximation to φ. The other reason is that the pther statevectors $|j\rangle$ could also be received in the measurement with a small probability - their amplitudes are non-zero if φ is longer than n bits (in which case we say that the algorithm failed). Nevertheless, the algorithm is one of most vital importance and use in what follows.

Finally, another note: Preparing the eigenvector $|u\rangle$ may not be easy. But it may be easy to prepare a superposition of some eigenvectors (for example, in the order-finding algorithm below). In this case, we receive $\tilde{\varphi}$ with high probability for **one of the eigenvectors in the superposition**.

3 Order-finding and Shor's algorithm

Given integers $x, N > 0$ with $\gcd(x, N) = 1$, we would like to find the order r of x modulo N. Classically, this is hard. Here we show that with high probability we can find it