QUANTUM INFORMATION

MFF UK

Recall the definitions of the IFT and DFT circuits for $(\mathbb{Z}_{2^m}, +)$:

$$\mathrm{IFT} : |k\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{l=0}^{2^m-1} \omega_{2^m}^{kl} |l\rangle,$$

$$\mathrm{DFT} : |k\rangle \mapsto \frac{1}{\sqrt{2^m}} \sum_{l=0}^{2^m-1} \overline{\omega}_{2^m}^{kl} |l\rangle,$$

where ω_M^N denotes $e^{2\pi i \frac{N}{M}}$.

The following exercises are designed to derive Shor's algorithm as an application of Kitaev's algorithm for phase estimation. We start by solving the following problem: given a unitary operator U with an eigenvector $|\psi\rangle$, find its corresponding eigenvalue. Note that the eigenvalue is of the form $e^{2\pi i\theta}$ for some $\theta \in [0, 1]$, and we will be computing this θ (also known as *phase*).

The idea is simple: we apply different powers of U on $|\psi\rangle$ at the same time to get the distribution of the outputs, which will be almost periodic (i.e., similar to a character). We can then use the DFT to find the corresponding character, which, hopefully, will help us compute θ.

Formally, we pick some $M = 2^m$ large enough and construct the circuit:

$$|k\rangle|\psi\rangle \mapsto |k\rangle U^k|\psi\rangle = e^{2\pi i k\theta}|k\rangle|\psi\rangle, \tag{1}$$

where $|k\rangle \in \mathbb{H}_2^m$.

(1) Implement the above circuit using at most m controlled single-qubit operators.

To apply all the possible powers of U onto $|\psi\rangle$ simultaneously we need to apply the above circuit onto the $(H^{\otimes m}|0\rangle^{\otimes m})|\psi\rangle$.

(2) Write down the result of the application of (1) onto $(H^{\otimes m}|0\rangle^{\otimes m})|\psi\rangle$.

The resulting state is of the form $|\varphi\rangle|\psi\rangle$, and so we can drop the $|\psi\rangle$ part (or recycle it for future usage). So, from now on, we concentrate on the given $|\varphi\rangle$ only.

(3) Assume θ is of the form $\frac{p}{2^m}$ for some natural number p. Show that applying DFT on $|\varphi\rangle$ and measuring the result in the computational basis yields the desired θ (actually $|p\rangle$, however θ can then be easily reconstructed) with probability 1.

Assume now that $2^m\theta = a + 2^m\delta$ for some natural number a so that $|2^m\delta| \leq \frac{1}{2}$. Since it is not possible, in general, to compute an arbitrary θ, from now on we will be interested in computing the natural number a which is a good approximation of $2^m\theta$.

(4) Apply DFT on the general $|\varphi\rangle$ and compute the result. Show that, assuming δ is 0, one arrives at the same conclusion as in the previous exercise.

We now measure the result in the computational basis and ask about the probability of getting $|a\rangle$.

(5) * Show a good (e.g., constant) lower bound on getting $|a\rangle$ after the measurement, assuming $\delta \neq 0$.

This concludes Kitaev's algorithm on phase estimation. We now connect it with Shor's algorithm.

Assume we are given $a \in \mathbb{Z}_N^*$ and U realizing multiplication by a in $\mathbb{Z}_N$. Let r denote the order of a in $\mathbb{Z}_N$.

(6) Show that all eigenvectors of U are of the form $\lambda_p = \omega_r^p = e^{2\pi i \frac{p}{r}}$ for $p = 0, 1, ..., r-1$.

(7) Show that the state $|u_p\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i \frac{pj}{r}} |a^j\rangle$ is an eigenvector corresponding to λ_p.

So, one might pick $|u_1\rangle$ and compute the phase of λ_1, which equals $\frac{1}{r}$, by applying Kitaev's algorithm. This reveals the order of a. However, the problem is that we cannot directly construct $|u_1\rangle$ without the knowledge of r. The corresponding eigenvector, however, is crucial in the application of Kitaev's algorithm.

(8) Assume we use Kitaev's algorithm with $|\psi\rangle = \sum c_p |u_p\rangle$. What do we expect to see after the measurement?

(9) Show that $|1\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |u_p\rangle$. What do we expect to see after applying Kitaev's algorithm to this state?

This almost finishes Shor's algorithm. i.e., finding the order of a in $\mathbb{Z}_N$. The final catch is that we do not get the value $\frac{p}{r}$ precisely but rather its binary approximation. To compute $\frac{p}{r}$, one needs to perform an algorithm related to *continuous fractions*. Number theory then tells us that, assuming m in the application of Kitaev's algorithm is big enough, we are guaranteed to find $\frac{p}{r}$ exactly after a small number of steps. This $\frac{p}{r}$ can then be used to reconstruct r, assuming p and r are coprime.

(10) * Fix r and pick p uniformly at random from the set $\{0, 1, ..., r-1\}$. Give a good lower bound on p and r being coprime.