Christian B. Mendl, Martina Nibbi, Pedro Hack, Irene López Gutiérrez due: 08 May 2023, 08:00 on Moodle

Tutorial 2 (Discrete logarithms using QFT[1])

Other than order- or period-finding, the Quantum Fourier Transform is applicable to several other interesting problems, one of which is the *discrete logarithm* problem. The problem is phrased as follows; given some large integer N and two integers a, b with $b = a^s \mod N$, find the unknown integer s.

In order to solve this problem using a quantum computer, we introduce the function f:

$$f(x_1, x_2) = b^{x_1} a^{x_2} \mod N = a^{sx_1 + x_2} \mod N.$$

We see that the function is periodic over the tuple $(\ell, -s\ell)$ with $\ell \in \mathbb{Z}$, i.e., $f(x_1 + \ell, x_2 - s\ell) = f(x_1, x_2)$. The following algorithm utilizes two registers with t qubits each and one with $n = \lceil \log_2 N \rceil$ qubits. Moreover, the algorithm requires (a single application of) the unitary operator U defined via:

$$U \left| x_1 \right\rangle \left| x_2 \right\rangle \left| y \right\rangle = \left| x_1 \right\rangle \left| x_2 \right\rangle \left| y \oplus f(x_1, x_2) \right\rangle .$$

We also assume knowledge of the smallest integer $r > 0$ such that $a^r \mod N = 1$. It can be obtained via the order-finding algorithm, which will be discussed in the lecture.

(a) We first introduce a new state, the Fourier transform of f:

$$\left| \hat{f}(\ell_1, \ell_2) \right\rangle = \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} \mathrm{e}^{2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} \left| f(x_1, x_2) \right\rangle .$$

Show that

$$\left| \hat{f}\left(\ell_1, \ell_2\right) \right\rangle = \delta_{\ell_1 - s\ell_2 \mod r, 0} \sum_{j=0}^{r-1} \mathrm{e}^{2\pi i \ell_2 j/r} \left| f(0, j) \right\rangle ,$$

where the δ-function means that the expression is zero unless $\ell_1 - s\ell_2$ is an integer multiple of r.

(b) Next, derive that

$$\frac{1}{r} \sum_{\ell_1=0}^{r-1} \sum_{\ell_2=0}^{r-1} \mathrm{e}^{-2\pi i (\ell_1 x_1 + \ell_2 x_2)/r} \left| \hat{f}(\ell_1, \ell_2) \right\rangle = \left| f(x_1, x_2) \right\rangle .$$

We now provide an overview of the algorithm:

$$\left| 0^{\otimes t} \right\rangle \left| 0^{\otimes t} \right\rangle \left| 0^{\otimes n} \right\rangle \tag{1}$$

$$\xrightarrow{\text{apply } H^{\otimes 2t}} \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} \left| x_1 \right\rangle \left| x_2 \right\rangle \left| 0^{\otimes n} \right\rangle \tag{2}$$

$$\begin{aligned}
\xrightarrow{\text{apply } U} & \frac{1}{2^t} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} \left| x_1 \right\rangle \left| x_2 \right\rangle \left| f(x_1, x_2) \right\rangle \qquad (3) \\
&= \frac{1}{2^t r} \sum_{\ell_2=0}^{r-1} \sum_{x_1=0}^{2^t-1} \sum_{x_2=0}^{2^t-1} \mathrm{e}^{-2\pi i (s\ell_2 x_1 + \ell_2 x_2)/r} \left| x_1 \right\rangle \left| x_2 \right\rangle \left| \hat{f}(s\ell_2, \ell_2) \right\rangle \\
&= \frac{1}{r} \sum_{\ell_2=0}^{r-1} \left[\frac{1}{\sqrt{2^t}} \sum_{x_1=0}^{2^t-1} \mathrm{e}^{-2\pi i (s\ell_2 x_1)/r} \left| x_1 \right\rangle \right] \left[\frac{1}{\sqrt{2^t}} \sum_{x_2=0}^{2^t-1} \mathrm{e}^{-2\pi i (\ell_2 x_2)/r} \left| x_2 \right\rangle \right] \left| \hat{f}(s\ell_2, \ell_2) \right\rangle
\end{aligned}$$

$$\xrightarrow{\text{apply inverse QFT}} \frac{1}{r} \sum_{\ell_2=0}^{r-1} \left| \widetilde{s\ell_2/r} \right\rangle \left| \widetilde{\ell_2/r} \right\rangle \left| \hat{f}\left(s\ell_2, \ell_2\right) \right\rangle \tag{4}$$

$$\xrightarrow{\text{measure first two registers}} \left(\frac{\widetilde{s\ell_2}}{r}, \frac{\widetilde{\ell_2}}{r} \right) \tag{5}$$

(c) Finally, describe the process to determine s from the estimates of $\frac{s\ell_2}{r}$ and $\frac{\ell_2}{r}$.

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), section 5.4.2

Exercise 2.1 (Binary phase estimation)

(a) Specify the quantum circuits performing the forward and inverse Fourier transform for vectors of length 2 (i.e., acting on a single qubit), and verify your circuits based on the definition of the Fourier transform.

Hint: Each of your circuits should consist of a single gate.

(b) Let U be a unitary operator with eigenvalues ± 1, which acts on a state $|\psi\rangle$. Using the phase estimation procedure, construct a quantum circuit to collapse $|\psi\rangle$ into one or the other of the two eigenspaces of U, giving also a classical indicator as to which space the final state is in. Compare your result with "measuring an operator" (see also exercise 4.34 in the Nielsen and Chuang book).

Exercise 2.2 (Numerical simulation of the phase estimation algorithm)
The Moodle page contains a Python/NumPy code template with a simple statevector simulator of quantum circuits (see the subfolder `circuit_sim/`). Familiarize yourself with the implementation in `gates.py` first, which defines common quantum gates, and functionality for applying these gates to a statevector stored as NumPy array.

(a) Revisit the quantum Fourier transform circuit from the lecture, and complete the TODOs in `fourier.py`. To test your solution, `cd` to the parent folder of `circuit_sim/` and run "`python3 test/test_fourier.py`" in a terminal. (Depending on your local installation, the command to start the Python 3 interpreter might be slightly different. The tests require the `unittest` package.)

(b) Fill the missing code sections in `phase_estimation.py`. As before, you can test your implementation by calling "`python3 test/test_phase_estimation.py`".

(c) Finally, run the Jupyter notebook `phase_estimation_sim.ipynb` and submit the notebook with the generated plots.

2.1.

a) Forward Fourier transform on a single bit:

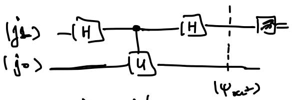
$|j\rangle \ -\boxed{H}- \ \mathcal{F}(|j\rangle)$

Backward Fourier transform of a single bit

since $H \cdot H^{-1} = \mathbb{1} \Rightarrow$

$\mathcal{F}(|j\rangle) -\boxed{H}- \ |j\rangle$

b) Phase estimation on one bit:



$|j_1\rangle = |0\rangle$ initial state

$|j_0\rangle = |u_x\rangle$ or $|u_y\rangle$ (eigenvectors of $\hat{U}$)

$U|u_x\rangle = a|u_x\rangle$

$U|u_y\rangle = b|u_y\rangle$

$\Rightarrow \quad |\psi_{out}\rangle = (H \otimes \mathbb{1})\left(\frac{1}{\sqrt{2}}|0, j_0\rangle + |1\rangle \otimes U|j_0\rangle\right) \longrightarrow$

$|j_0\rangle \to u_a, \ u_b \qquad U|j_0\rangle \to a, \ b$

$\longrightarrow$

$(H \otimes \mathbb{1})\left(\frac{1}{\sqrt{2}}|0, a\rangle + |1\rangle \otimes |a\rangle\right) =$

$\frac{1}{\sqrt{2}}\left((|0\rangle + |1\rangle)\frac{1}{\sqrt{2}} \otimes |a\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle \otimes |a\rangle\right) =$

$\frac{1}{2}|0, a\rangle + \frac{1}{2}|0, a\rangle = |0, a\rangle$; measurement $= 0 \Rightarrow$ eigenvector $|a\rangle$

$(H \otimes \mathbb{1})\left(\frac{1}{\sqrt{2}}|0, b\rangle + |1\rangle \otimes |b\rangle\right)$

$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |b\rangle + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |b\rangle\right)$

Since H4 second eigenvalue is negative

$\frac{1}{2}|1, b\rangle + \frac{1}{2}|1, b\rangle = |1, b\rangle$ measurement $= 1$ eigenvector $|b\rangle$