QUANTUM COMPUTATION AND QUANTUM INFORMATION:
THE QUANTUM FOURIER TRANSFORM

1

We consider the linear map in $\mathbb{C}^N$ which acts on the computational basis as

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2i\pi jk}{N}} |k\rangle$$

Let A be the matrix of the transformation in the computational basis.

$$\forall (k,l) \in [\![0, N-1]\!]^2, \quad a_{kl} = \frac{1}{\sqrt{N}} e^{\frac{2i\pi kl}{N}}$$

The adjoint matrix $A^\dagger$ is then

$$\begin{aligned} \forall (k,l) \in [\![0, N-1]\!]^2, \quad b_{kl} &= a^*_{lk} \\ &= \frac{1}{\sqrt{N}} e^{-\frac{2i\pi kl}{N}} \end{aligned}$$

We compute the coefficient k, l of the product $AA^\dagger$:

$$\begin{aligned} \forall (k,l) \in [\![0, N-1]\!]^2, \quad c_{kl} &= \sum_{j=0}^{N-1} a_{kj} b_{jl} \\ &= \frac{1}{N} \sum_{j=0}^{N-1} e^{\frac{2i\pi j}{N}(k-l)} \\ &= \frac{1}{N} \sum_{j=0}^{N-1} (e^{\frac{2i\pi}{N}(k-l)})^j \\ &= \begin{cases} \dfrac{1}{N} \dfrac{1 - (e^{\frac{2i\pi}{N}(k-l)})^N}{1 - e^{\frac{2i\pi}{N}(k-l)}} = 0 & \text{if } e^{\frac{2i\pi}{N}(k-l)} \neq 1, \\ 1 & \text{if } e^{\frac{2i\pi}{N}(k-l)} = 1. \end{cases} \\ &= \begin{cases} 0 & \text{if } k \neq l, \\ 1 & \text{if } k = l. \end{cases} \\ &= \delta_{kl} \end{aligned}$$

which shows that $AA^\dagger = A^\dagger A = I$ i.e. A is unitary.

2

Here the dimension of the state space is $N = 2^n$. The Fourier transform of the n qubit state $|00\ldots 0\rangle$ is

$$A|0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

we can write k in binary $k_{n-1} \ldots k_1 k_0$

$$A|0\rangle = \frac{1}{2^{n/2}} \sum_{k_0, k1, \ldots, k_{n-1}=0}^{1} |k_{n-1} \ldots k_1 k_0\rangle$$

or in product representation,

$$= \frac{1}{2^{n/2}} \underbrace{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \ldots (|0\rangle + |1\rangle)}_{n \text{ qubits}}$$

3

Let $N = 2^n$ and $Y = (y_k)_{k\in[\![0,N-1]\!]}$ be the classical fourier transform of $X = (x_k)_{k\in[\![0,N-1]\!]}$.

$$\forall k \in [\![0, N-1]\!], \quad y_k = \sum_{j=0}^{N-1} e^{\frac{2i\pi kj}{2^n}} x_j$$

The factor $\frac{1}{\sqrt{N}}$ is omitted for clarity. We can write j in binary $j_{n-1}\dots j_1 j_0$

$$\begin{aligned}
y_k &= \sum_{j_0,j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-1}j_{n-1}+\cdots+2j_1+j_0)}{2^n}} x_j \\
&= \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-1}j_{n-1}+\cdots+2j_1)}{2^n}} x_{j_{n-1}\cdots j_1 0} + \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-1}j_{n-1}+\cdots+2j_1+1)}{2^n}} x_{j_{n-1}\cdots j_1 1} \\
&= \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-1}j_{n-1}+\cdots+2j_1)}{2^n}} x_{j_{n-1}\cdots j_1 0} + e^{\frac{2i\pi k}{2^n}} \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-1}j_{n-1}+\cdots+2j_1)}{2^n}} x_{j_{n-1}\cdots j_1 1} \\
&= \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-2}j_{n-1}+\cdots+j_1)}{2^{n-1}}} x_{j_{n-1}\cdots j_1 0} + e^{\frac{2i\pi k}{2^n}} \sum_{j_1,\dots,j_{n-1}=0}^{1} e^{\frac{2i\pi k(2^{n-2}j_{n-1}+\cdots+j_1)}{2^{n-1}}} x_{j_{n-1}\cdots j_1 1}
\end{aligned}$$

We see the first sum is the k^{th} coefficient of the FT of the sequence $(x_{2k})_{k\in[\![0,N/2-1]\!]}$ and the second is the k^{th} coefficient of the FT of $(x_{2k+1})_{k\in[\![0,N/2-1]\!]}$. This shows that to compute FT of sequence of length N, we have to compute 2 FT of sequence of length $\frac{N}{2}$ and do $2N$ complex additions/multiplications. The complexity of the operation $T(N)$ follows the recurrence:

$$T(N) = 2T(\frac{N}{2}) + 2N$$

We can use the Master theorem [1]:

Theorem. Let $a \geqslant 1$ and $b > 1$ be constants, let $f(n)$ be a function, and let $T(n)$ be defined on the non negative integers by the recurrence

$$T(n) = aT(\frac{n}{b}) + f(n)$$

where we interpret $\frac{n}{b}$ to mean either $\lfloor \frac{n}{b} \rfloor$ or $\lceil \frac{n}{b} \rceil$. Then $T(n)$ has the following asymptotic bounds:

(1) If $f(n) = O(n^{\log_b a-\epsilon})$ for some constant $\epsilon > 0$, then $T(n) = \Theta(n^{\log_b a})$.
(2) If $f(n) = \Theta(n^{\log_b a})$, then $T(n) = \Theta(n^{\log_b a}\log n)$.
(3) If $f(n) = \Omega(n^{\log_b a+\epsilon})$ for some constant $\epsilon > 0$, and if $af(\frac{n}{b}) \leqslant cf(n)$ for some constant $c < 1$ and n sufficiently large, then $T(n) = \Theta(f(n))$.

Here we are in the second case of the theorem, so $T(N) = \Theta(N\log(N)) = \Theta(n2^n)$.

5

The inverse Fourier Transform

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-\frac{2i\pi jk}{N}} |k\rangle$$

is the adjoint of the Fourier Transform. The quantum circuit of figure 1 is obtained from the FT's circuit, replacing each R_k gate by its adjoint

$$R_k^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-\frac{2i\pi}{2^k}} \end{bmatrix}$$

[1]Thomas H. Cormen and Charles E. Leiserson : *Introduction to algorithms*, MIT Press (2009)

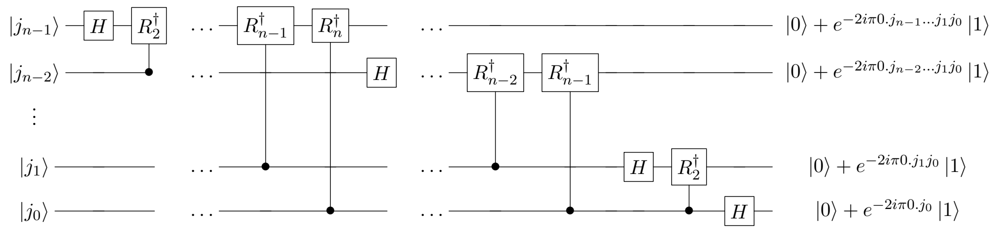

Figure 1. Quantum circuit for IFT.

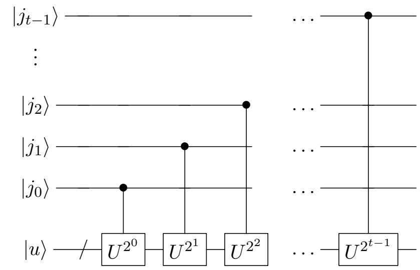

Figure 2. Sequence of controlled U.

7

In figure 2, the t qubits of the first register are prepared with $|j\rangle = |j_{t-1}\dots j_1 j_0\rangle$, the second register is prepared with some state $|u\rangle$. After the first controlled-U operation, the state is $|j\rangle\,|U^{j_0 2^0}u\rangle$. After the second controlled-U, the state is $|j\rangle\,|U^{j_1 2^1}U^{j_0 2^0}u\rangle = |j\rangle\,|U^{j_0 2^0 + j_1 2^1}u\rangle$ and so on. The final state is $|j\rangle\,|U^{j_0 2^0 + j_1 2^1 + \dots + j_{t-1}2^{t-1}}u\rangle = |j\rangle\,|U^j u\rangle$.

8

By linearity, the phase estimation algorithm takes input $|0\rangle\,|\Sigma_{u\in A} c_u\,|u\rangle\rangle$, where A is some orthonormal basis of eigenstates of U, to output $\sum_{u\in A} c_u\,|\widetilde{\varphi_u}\rangle\,|u\rangle$, where $\widetilde{\varphi_u}$ is an estimation of the phase of the eigenvalue associated with eigenstate u. If we fix $u_0 \in A$ beforehand, the probability to measure $\widetilde{\varphi_{u_0}}$ when measuring the first register in the computational basis is

$$
\begin{aligned}
(\sum_{u\in A} c_u^*\,\langle\widetilde{\varphi_u}|\,\langle u|)P_{\widetilde{\varphi_{u_0}}}\otimes I(\sum_{u\in A} c_u\,|\widetilde{\varphi_u}\rangle\,|u\rangle) &= (\sum_{u\in A} c_u^*\,\langle\widetilde{\varphi_u}|\,\langle u|)(\sum_{\substack{u\in A\\ \widetilde{\varphi_u}=\widetilde{\varphi_{u_0}}}} c_u\,|\widetilde{\varphi_u}\rangle\,|u\rangle)\\
&= (\sum_{u\in A} c_u^*\,\langle\widetilde{\varphi_u}|\,\langle u|)(\sum_{\substack{u\in A\\ \widetilde{\varphi_u}=\widetilde{\varphi_{u_0}}}} c_u\,|\widetilde{\varphi_{u_0}}\rangle\,|u\rangle)\\
&= \sum_{\substack{v\in A\\ u\in A\\ \widetilde{\varphi_u}=\widetilde{\varphi_{u_0}}}} c_v^* c_u\,\langle\widetilde{\varphi_v}|\widetilde{\varphi_u}\rangle\,\langle v|u\rangle\\
&= \sum_{\substack{v\in A\\ u\in A\\ \widetilde{\varphi_u}=\widetilde{\varphi_{u_0}}}} c_v^* c_u\,\langle\widetilde{\varphi_v}|\widetilde{\varphi_u}\rangle\,\delta_{vu}\\
&= \sum_{\substack{u\in A\\ \widetilde{\varphi_u}=\widetilde{\varphi_{u_0}}}} |c_u|^2\\
&\geqslant |c_{u_0}|^2
\end{aligned}
$$

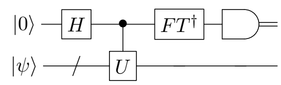

FIGURE 3. Phase estimation circuit with $t = 1$.

I is the identity operator of whatever state space U operates on, while $P_{\widetilde{\varphi_{u_0}}}$ is the orthonormal projector onto the space generated by the vector $|\widetilde{\varphi_{u_0}}\rangle$ of the computational basis. Besides, following the analysis of the book, $\widetilde{\varphi_{u_0}}$ is an approximation to φ_{u_0} to an accuracy 2^{-n} with probability at least $1-\epsilon$ if we make use of $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ bits in the first register. We conclude we get the desired approximation of φ_{u_0} at the end of the phase estimation algorithm with probability at least $|c_{u_0}|^2(1-\epsilon)$.

9

U being unitary with eigenvalues -1 and $+1$, the state space is the direct sum of the two orthogonal eigenspaces $E_{-1} \oplus E_1$. Thus we can uniquely decompose any $|\psi\rangle = |\psi_{-1}\rangle + |\psi_{+1}\rangle$, with $|\psi_{-1}\rangle \in E_{-1}$ ans $|\psi_{+1}\rangle \in E_{+1}$. Then $-1 = e^{i\pi} = e^{2i\pi 0.1}$ and $1 = e^0 = e^{2i\pi 0.0}$ shows that is is sufficient to make use of $t = 1$ wire in the first register in the phase estimation procedure to read directly the phase of any eigenvector. If we use $|0\rangle |\psi\rangle$ as input in the circuit of figure 3, the output before the final measurement will be $|0\rangle |\psi_{+1}\rangle + |1\rangle |\psi_{-1}\rangle$.

When we measure the first register, we obtain 0 with probability

$$\begin{aligned}(\langle 0| \langle\psi_{+1}| + \langle 1| \langle\psi_{-1}|)P_0 \otimes I(|0\rangle |\psi_{+1}\rangle + |1\rangle |\psi_{-1}\rangle) &= (\langle 0| \langle\psi_{+1}| + \langle 1| \langle\psi_{-1}|)(|0\rangle |\psi_{+1}\rangle) \\ &= \langle 0|0\rangle \langle\psi_{+1}|\psi_{+1}\rangle \\ &= \langle\psi_{+1}|\psi_{+1}\rangle\end{aligned}$$

or 1 with probability

$$\begin{aligned}(\langle 0| \langle\psi_{+1}| + \langle 1| \langle\psi_{-1}|)P_1 \otimes I(|0\rangle |\psi_{+1}\rangle + |1\rangle |\psi_{-1}\rangle) &= (\langle 0| \langle\psi_{+1}| + \langle 1| \langle\psi_{-1}|)(|1\rangle |\psi_{-1}\rangle) \\ &= \langle 1|1\rangle \langle\psi_{-1}|\psi_{-1}\rangle \\ &= \langle\psi_{-1}|\psi_{-1}\rangle\end{aligned}$$

The state will collapse respectively into $\frac{1}{\sqrt{\langle\psi_{+1}|\psi_{+1}\rangle}} |0\rangle |\psi_{+1}\rangle$ or $\frac{1}{\sqrt{\langle\psi_{-1}|\psi_{-1}\rangle}} |1\rangle |\psi_{-1}\rangle$. Thus if we read 0 in the first register, that means that we have an eigenvector associated to eigenvalue $+1$ in the second register, and if we read 1 in the first register, that means that we have an eigenvector associated to eigenvalue -1 in the second register.

Once we have noticed that the FT in dimension $N = 2^1$ is just the Hadamard operator, we conclude the phase estimation circuit in this particular case is the just the same as the circuit of exercice 4.34.

10

$$\begin{aligned} x^2 &= \quad 25 &&= 4 \\ x^3 &= \quad 20 &&= -1 \\ x^4 &= \quad 4^2 &&= 16 \\ x^5 &= 16 \times 5 &&= 80 \\ & &&= 17 \\ x^6 &= (-1)^2 &&= 1 \end{aligned}$$

11

Theorem (*Euler*)**.** For $N \in \mathbb{N}^*$, let

$$\varphi(N) = \#\{m \in [\![1, N]\!], m \wedge N = 1\}$$

We have

$$\forall x \in \mathbb{N}^*, \quad x \wedge N = 1 \Rightarrow x^{\varphi(N)} = 1 \mod N$$

Then by definition of the order r, $r \leqslant \varphi(N) \leqslant N$.

12

Since $x \wedge N = 1$, from Bezout's Theorem $\exists (u,v) \in \mathbb{Z}^2$ such that $ux + vN = 1$ that is $\exists u$ such that $ux = 1 \mod N$ which shows that x has a multiplicative inverse $x^{-1} = u$ in the ring $(\frac{\mathbb{Z}}{N\mathbb{Z}}, +, \times)$. We define the linear map U' on $(\mathbb{C}^2)^{\otimes L} \cong \mathbb{C}^{2^L}$ that acts on the computational basis as

$$\forall y \in \{0,1\}^L, \quad U' |y\rangle = \begin{cases} |x^{-1}y \mod N\rangle & \text{if } y < N, \\ y & \text{if } y \in [\![N, 2^L - 1]\!]. \end{cases}$$

We have

$$\begin{aligned} \forall y_1, y_2 \in \{0,1\}^L, \quad \langle y_1 | U(y_2) \rangle = 1 &\Leftrightarrow y_1 = y_2 \in [\![N, 2^L - 1]\!] \text{ or } (y_1, y_2 < N \text{ and } xy_2 = y_1 \mod N) \\ &\Leftrightarrow y_1 = y_2 \in [\![N, 2^L - 1]\!] \text{ or } (y_1, y_2 < N \text{ and } \exists k \in \mathbb{Z}, xy_2 = y_1 + kN) \\ &\Leftrightarrow y_1 = y_2 \in [\![N, 2^L - 1]\!] \text{ or } (y_1, y_2 < N \text{ and } \exists k \in \mathbb{Z}, y_2 = x^{-1}y_1 + x^{-1}kN) \\ &\Leftrightarrow y_1 = y_2 \in [\![N, 2^L - 1]\!] \text{ or } (y_1, y_2 < N \text{ and } \exists k' \in \mathbb{Z}, y_2 = x^{-1}y_1 + k'N) \\ &\Leftrightarrow y_1 = y_2 \in [\![N, 2^L - 1]\!] \text{ or } (y_1, y_2 < N \text{ and } x^{-1}y_1 = y_2 \mod N) \\ &\Leftrightarrow \langle U'(y_1) | y_2 \rangle = 1 \end{aligned}$$

so, since $\langle U'(y_1) | y_2 \rangle, \langle y_1 | U(y_2) \rangle \in \{0,1\}$,

$$\forall y_1, y_2 \in \{0,1\}^L, \quad \langle y_1 | U(y_2) \rangle = \langle U'(y_1) | y_2 \rangle$$

This shows that $U' = U^\dagger$. since it is obvious that U is invertible and $U^\dagger = U^{-1}$, we have shown that U is unitary.

13

$(|u_s\rangle)_{s \in [\![0, r-1]\!]}$ is defined to be the IFT of the sequence $(|x^k \mod N\rangle)_{k \in [\![0, r-1]\!]}$:

$$\forall s \in [\![0, r-1]\!], \quad |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2i\pi sk}{r}} |x^k \mod N\rangle$$

Thus the equalities

$$\forall k \in [\![0, r-1]\!], \quad |x^k \mod N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi sk}{r}} |u_s\rangle$$

just express the fact that $(|x^k \mod N\rangle)_{k \in [\![0, r-1]\!]}$ is the FT of the sequence $(|u_s\rangle)_{s \in [\![0, r-1]\!]}$. Let's check this. Let $k \in [\![0, r-1]\!]$,

$$\begin{aligned} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2i\pi sk}{r}} |u_s\rangle &= \frac{1}{r} \sum_{s=0}^{r-1} e^{\frac{2i\pi sk}{r}} \sum_{j=0}^{r-1} e^{-\frac{2i\pi sj}{r}} |x^j \mod N\rangle \\ &= \frac{1}{r} \sum_{j=0}^{r-1} \left(\sum_{s=0}^{r-1} (e^{\frac{2i\pi(k-j)}{r}})^s \right) |x^j \mod N\rangle \\ &= \frac{1}{r} \sum_{j=0}^{r-1} r\delta_{jk} |x^j \mod N\rangle \\ &= |x^k \mod N\rangle \end{aligned}$$