Quantum Computing CO484

Tutorial*

Sheet 5 – Solutions

Exercise 1 *What is the matrix for the quantum Fourier transform* $\mathbf{F}$ *when* $n = 1$ *and* $n = 2$*? Show that* $\mathbf{F}$ *is unitary for any* n*.*

Solution In general for $N = 2^n$ we have $(\mathbf{F}_{kj}) = \frac{1}{\sqrt{N}} e^{2\pi ijk/N}$. For $n = 1$ we get:

$$\mathbf{F} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

For $n = 2$, we have:

$$\mathbf{F} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

The circuit in the Lecture Notes shows that $\mathbf{F}$ is unitary as it has is the composition of unitary matrices (Hadamard and controlled phase). Alternatively, we can show that the columns of the matrix $(\mathbf{F}_{kj})$ form an orthonormal set of vectors.

Exercise 2 *More on Quantum Fourier Transformation (QFT).*

(i) Work out the matrix for the quantum Fourier transform F *and the network which implements it for* $n = 3$.

(ii) Show that the inverse quantum Fourier transform is given by:

$$\mathbf{F}^\dagger : |j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{-2\pi ijk/2^n} |k\rangle . \tag{1}$$

(iii) Work out the circuit for the inverse of the Fourier transform.

*Partly based on the tutorials by Abbas Edalat and Herbert Wiklicky.

Solution

(i) $(\mathbf{F})_{kj} = \frac{1}{\sqrt{8}} e^{2\pi i kj/8}$. Let $a = e^{\pi i/4} = (1+i)/2$, then $a^2 = i$, $a^3 = ia = (-1+i)/2$, $a^4 = -1$, $a^5 = -a$, $a^6 = -i$, $a^7 = -ia$ and we have:

$$\mathbf{F} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & i & ia & -1 & -a & -i & -ia \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & ia & -i & a & -1 & -ia & i & -a \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -a & i & -ia & -1 & a & -i & ia \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -ia & -i & -a & -1 & ia & i & a \end{pmatrix}$$

(ii) Since $\mathbf{F}$ is a symmetric matrix its adjoint is simply the complex conjugate of $\mathbf{F}$. Hence $(\mathbf{F}^{-1})_{kj} = (\mathbf{F}^\dagger)_{kj} = (\mathbf{F}^*)_{jk} = (\mathbf{F}^*)_{kj} = \frac{1}{\sqrt{2^n}} e^{-2\pi i jk/2^n}$.

(iii) Since $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$, the circuit is the same as the circuit for $\mathbf{F}$ but reversed with all the gates replaced by their adjoints. We have $\mathbf{H}^\dagger = H$ and $\mathbf{R}_k^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i/2^k} \end{pmatrix}$.

Exercise 3 *Quantum Phase Estimation. Let be* $\mathbf{U} : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ *an unitary operator acting on* $\mathbb{C}^{2^n}$ *and let* $|u\rangle \in \mathbb{C}^{2^n}$ *an eigenstate of* $\mathbf{U}$ *and let* $\lambda_{|u\rangle} \in \mathbb{C}$ *its associated eigenvalue:*

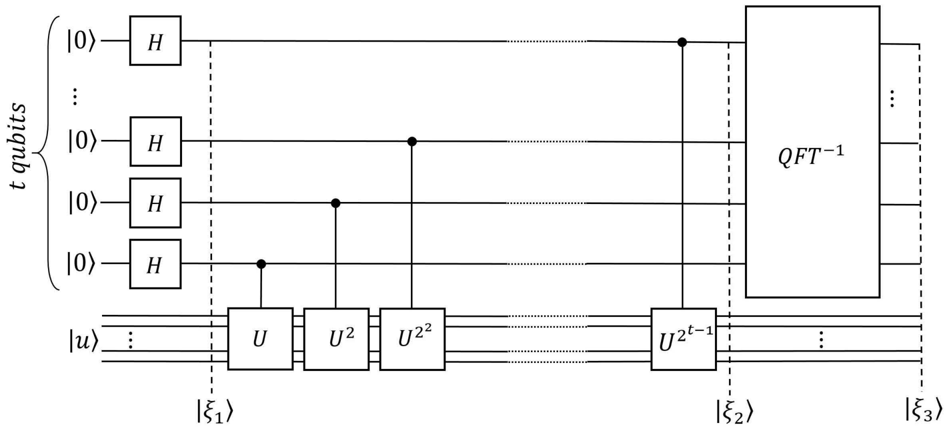
(i) Show that $\exists \phi \in [0, 1[$ *such that* $\lambda_{|u\rangle} = e^{2\pi i \phi}$.

(ii) Let t *be a non-zero natural number. Write the form of the states* $|\xi_1\rangle, |\xi_2\rangle$ *as depicted in the quantum circuit below.*

(iii) Suppose that ϕ *is an exact multiple of* $\frac{1}{2^t}$, *write then the form of* $|\xi_3\rangle$. *What does this tell you about* ϕ?

Solution (i) Since $\mathbf{U}$ is Unitary then its spectrum is formed by all the complex numbers with modulus 1 which means $\lambda_{|u\rangle}$ can be parametrized as in (i) for an appropriate value of ϕ.
(ii) It's clear that:

$$|\xi_1\rangle = |u\rangle \otimes \frac{1}{\sqrt{2^t}} (|0\rangle + |1\rangle)^{\otimes t}.$$



By definition $\mathbf{U}\left|u\right\rangle = \lambda_{\left|u\right\rangle}\left|u\right\rangle = e^{2\pi i\phi}\left|u\right\rangle$ so for every $j \in \{0, \dots, t-1\}$ we have:

$$\mathbf{U}^{2^j}\left|u\right\rangle = e^{2\pi i(2^j\phi)}\left|u\right\rangle.$$

Before the application of the controlled $\mathbf{U}^{2^j}$ the state of the $j-th$ qubit of the first register (enumerating them from below and starting from 0) will be simply the output of the Hadamard gate on the $j-th$ qubit of the first register. Since the initial state of that qubit was $\left|0\right\rangle$ then immediately after the Hadamard gate its state will be $\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$. It's then clear that the effect of applying the controlled $\mathbf{U}^{2^j}$ is to encode the angle $2\pi(2^j\phi)$ in the relative phase of the state of the $j-th$ qubit. Then we can conclude that:

$$\left|\xi_2\right\rangle = \left|u\right\rangle \otimes \frac{(\left|0\right\rangle + e^{2\pi i(2^0\phi)}\left|1\right\rangle) \otimes \dots \otimes (\left|0\right\rangle + e^{2\pi i(2^{t-1}\phi)}\left|1\right\rangle)}{\sqrt{2^t}}.$$

(iii) Relabelling the Hilbert spaces starting from the above we can write $\left|\xi_2\right\rangle$ as:

$$\frac{(\left|0\right\rangle + e^{2\pi i(2^{t-1}\phi)}\left|1\right\rangle) \otimes \dots \otimes (\left|0\right\rangle + e^{2\pi i(2^0\phi)}\left|1\right\rangle)}{\sqrt{2^t}} \otimes \left|u\right\rangle.$$

Since ϕ is an exact multiple of $\frac{1}{2^t}$ then we can find a collection of t bits $\phi_1, \dots, \phi_t$ such that:

$$\phi = 0.\phi_1 \dots \phi_t.$$

Consider now the expression $e^{2\pi i(2^j\phi)}$ for $j \in \{2, \dots, t-2\}$, we have:

$$\begin{aligned} e^{2\pi i(2^j\phi)} &= e^{2\pi i(2^j 0.\phi_1 \dots \phi_t)} = e^{2\pi i\phi_1 \dots \phi_j.\phi_{j+1} \dots \phi_t} = e^{2\pi i((\phi_1 2^{j-1} + \dots + \phi_j 2^0) + 0.\phi_{j+1} \dots \phi_t)} \\ &= e^{2\pi i(\phi_1 2^{j-1} + \dots + \phi_j 2^0)} e^{2\pi i 0.\phi_{j+1} \dots \phi_t} = e^{2\pi i 0.\phi_{j+1} \dots \phi_t}, \end{aligned}$$

with the obvious extension for $j \in \{0, 1, t-1\}$. Then using this relation we can rewrite the above quantum state as:

$$\frac{(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.\phi_1 \ldots \phi_t}|1\rangle)}{\sqrt{2^t}} \otimes |u\rangle \, .$$

We then recognize that the state of the first register is exactly the output of the Quantum Fourier Transform applied to the computational basis state $|\phi_1\rangle \otimes \ldots |\phi_t\rangle$. This implies that, applying the inverse Quantum Fourier Transform to the first register we get the state:

$$|\xi_3\rangle = |\phi_1\rangle \otimes \ldots |\phi_t\rangle \otimes |u\rangle \, .$$

Measuring the first register with respect to the computational basis we then find the t bits $\phi_1, \ldots, \phi_t$ which will allow us to retrieve he phase ϕ using the formula $\phi = 0.\phi_1 \ldots \phi_t$. This is why this procedure is called Quantum Phase Estimation.

Exercise 4 **Prime factorization. Show that any $n \in \mathbb{N}$ greater than one can be written as a unique product (up to ordering of the factors) of prime numbers.*

Solution We do a proof by contradiction to show the existence, i.e. we assume that there exist numbers that do not have a prime factorization. Call the smallest one of these n. We have that $n \neq 1$ and n is not prime. Hence $n = ab$ for $a, b \in \mathbb{N}$ and $a < n$, $b < n$. But a, b can be written in a prime factorization, since we assumed that n is the smallest number that can not be written in a prime factorization. This gives us a prime factorization of n — a contradiction. To prove uniqueness, we need Euclid's Lemma: Let $p, a, b \in \mathbb{N}$ with p prime. Then if p divides ab, p divides a or p divides b or p divides a and b. This is proven as follows: Assume that p does not divide a (the proof for this case is sufficient). Since p is prime we have that $\gcd(p, a) = 1$. Lemma 8 of the script gives us that there exist $x, y \in \mathbb{Z}$ such that $p \cdot x + a \cdot y = 1$. This implies that $pxb + aby = b$. Since p divides pxb and aby, it also divides b.

Now, let $s \in \mathbb{N}$ be the smallest number that can be written as (at least) two different products of prime numbers, i.e. $s = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$. By Euclid's Lemma p_1 divides q_1 or $q_2 \cdot \ldots \cdot q_n$ (or both). But q_1 and $q_2 \cdot \ldots \cdot q_n$ both have a unique prime factorization (since they are both smaller than s) and hence $p_1 = q_j$ for some j. It follow that $p_2 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_n < s$. But this number has to have a unique prime factorization (since it is smaller than s) and hence the p- and the q-factorization are identical.