Exercise Set 5: Solution
Quantum Computation

Exercise 1 *Upper bound on the period of* $f(x) = a^x \,(mod\ N)$

(a) To check that G is a group, we need to check:
- The multiplication modulo N is an internal operation in G: indeed, if $\gcd(n, N) = 1$ and $\gcd(m, N) = 1$, then it also holds that $\gcd(n \cdot m \,(\text{mod } N), N) = 1$.
- It is associative: this follows form the associativity of the multiplication modulo N.
- The neutral element 1 belongs to G: clear.
- Each element in G has an inverse in G: indeed, if $\gcd(n, N) = 1$, then Bézout's theorem implies there exist integers x, y such that $xn + yN = 1$, i.e., $xn \,(\text{mod } N) = 1$, which is exactly saying that x is the inverse of n modulo N, and the same equation also implies that $\gcd(x, N) = 1$, so x also belongs to G.

(b) The number of elements in G is equal to

$$(p-1) \cdot (q-1) = pq - p - q + 1 = N - p - q + 1 = (N-1) - (p-1) - (q-1)$$

Indeed, the set G contains all the elements between 1 and $N-1$, except the $q-1$ multiples of p and the $p-1$ multiples of q.

(c) H is a subgroup of G because:
- For any two elements a^ℓ and a^m in H, it is clear that $a^\ell \cdot a^m \,(\text{mod } N) = a^{\ell+m} \,(\text{mod } N)$ also belongs to H (note that if $\ell + m \geq k$, then $a^{\ell+m} \,(\text{mod } N) = a^{\ell+m-k} \,(\text{mod } N)$).
- Also, each element a^ℓ in H has an inverse $a^{k-\ell}$ which belongs also to H.

(d) Lagrange's theorem states that $|H| = k$ divides $|G| = (p-1)\,(q-1)$. But by definition, k is the smallest integer such that $a^k (\text{mod } N) = 1$, which is nothing but the period of the function f defined as $f(x) = a^x \,(\text{mod } N)$. This implies inequality (1).

Remark: The above also implies that if $\gcd(a, N) = 1$, then $a^{(p-1)\,(q-1)} \,(\text{mod } N) = 1$, which is known as (a particular instance of) *Euler's theorem.*

Exercise 2 *Quantum Fourier Transform*

(a) When $M = 2$,

$$QFT = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

is simply the Hadamard transform.

(b) When $M = 4$,

$$QFT = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad \text{so} \quad QFT^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}$$

and one can check indeed that $QFT \cdot QFT^\dagger = I$.

(c) By definition, it holds that

$$QFT\,|x\rangle = \frac{1}{2}\left(|0\rangle + i^x\,|1\rangle + (-1)^x\,|2\rangle + (-i)^x\,|3\rangle\right)$$

which can be rewritten as

$$QFT\,|x\rangle = \frac{1}{2}\left(|00\rangle + i^x\,|01\rangle + (-1)^x\,|10\rangle + (-i)^x\,|11\rangle\right) = \frac{1}{2}\left(|0\rangle + (-1)^x\,|1\rangle\right)\otimes\left(|0\rangle + i^x\,|1\rangle\right)$$

(d) Even though one may be tempted to deduce from the last expression that QFT can be written as a tensor product, this is not the case! The reason is that x here is a number between 0 and 3 and not a single bit. Formally, one can check by contradiction that there exist no 2×2 matrices A and B such that $QFT = A \otimes B$: the elements of the first row and column of QFT are all equal: this implies that both $a_{11} = a_{12} = a_{21}$ and $b_{11} = b_{12} = b_{21}$; then it becomes impossible to recover $QFT = A \otimes B$.

Exercise 3 *Another algorithm involving the QFT*

(a) The matrix elements of V_f are

$$\langle y|\,V_f\,|x\rangle = e^{-\frac{2\pi i}{M}f(x)}\,\langle y|x\rangle = \begin{cases} e^{-\frac{2\pi i}{M}f(x)} & \text{if } x = y \\ 0 & \text{fi } x \neq y \end{cases}$$

i.e., the matrix is diagonal and one checks trivially that $V_f V_f^\dagger = V^\dagger V_f = I$. For the QFT matrix, we have

$$\langle y|\,QFT\,|x\rangle = \frac{1}{\sqrt{M}}\sum_{y'=0}^{M-1} e^{\frac{2\pi i}{M}xy'}\,\langle y|y'\rangle = \frac{1}{\sqrt{M}}e^{\frac{2\pi i}{M}xy} \quad \text{since } \langle y|y'\rangle = \delta_{y,y'}$$

The inner product between two lines is given by

$$\frac{1}{M}\sum_{y=0}^{M-1} e^{\frac{2\pi i}{M}(x-x')y} = \begin{cases} 1 & \text{if } x = x' \\ 0 & \text{otherwise} \end{cases}$$

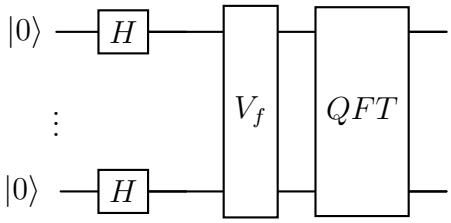
so $(QFT)(QFT)^\dagger = (QFT)^\dagger(QFT) = I$.

(b) A state $|x\rangle$ is represented by

$$|x\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{m-1}\rangle$$

where $x = x_0 + 2x_1 + \cdots + 2^{m-1}x_{m-1}, x_i \in \{0, 1\}$ is represented in base 2. The Hilbert space is $(\mathbb{C}^2)^{\otimes m}$. The initial state is $|x = 0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$.

The circuit is



(c) After the Hadamard gates, the state is

$$\frac{1}{2^{m/2}} \sum_{b_1 \ldots b_M} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_M\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle$$

After the V_f gate, the state is

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} |x\rangle$$

After the QFT gate, the state is

$$|\Psi\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} xy} |y\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \left\{ \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} e^{\frac{2\pi i}{M} xy} \right\} |y\rangle$$

(d) For $f(x) = Ax + B$, the coefficients of $|\Psi\rangle$ in the computational basis are

$$\frac{1}{M} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} Ax} e^{-\frac{2\pi i}{M} B} e^{\frac{2\pi i}{M} xy} = e^{-\frac{2\pi i}{M} B} \frac{1}{M} \sum_{x=0}^{M-1} e^{\frac{2\pi i}{M} (y-A)x}.$$

The probability to observe a given state $|y\rangle$ after the measurement is

$$\mathbb{P}(y) = \frac{1}{M^2} \left| \sum_{x=0}^{M-1} e^{\frac{2\pi i}{M} (y-A)x} \right|^2$$

For $y = A$, $\mathbb{P}(y) = 1$ and for $y \neq A$, $\mathbb{P}(y) = 0$. Therefore, a single measurement suffices to retrieve the value of A. On the other hand, B only appears as a global phase and cannot therefore be determined.