Quantum Computing HW3

Nir Stiassnie and Shay Kricheli

June 2020

Question 1 - Convolution Theorem

Let us recall the convolution of two vectors $e, f \in \mathbb{C}^N$ as:

$$(e * f)_j = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e_i f_{(j-i)(modN)}$$

We also defined the Fourier Transform of a vector $v \in \mathbb{C}^N$ as $\hat{v}$, where:

$$\hat{v} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{ij} v_j$$

We are to prove the convolution theorem:

Claim 1. *For any $e, f \in \mathbb{C}^N$:*

$$\widehat{(e * f)}_r = \widehat{e_r} \cdot \widehat{f_r}$$

Proof. Let us start with the left hand side $\widehat{(e * f)}_i$:

$$\begin{aligned}
\widehat{(e * f)}_r = \quad & \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{rj} (e * f)_j = \\
& \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{rj} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e_k f_{(j-k)(modN)} = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{rj} e_k f_{(j-k)(modN)} = \\
& \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{rj+rk-rk} e_k f_{(j-k)(modN)} = \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \omega_N^{r(j-k)} f_{(j-k)(modN)} = \\
& \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \left(\omega_N^{(j-k)}\right)^r f_{(j-k)(modN)} = \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \left(e^{2\pi i \frac{j-k}{N}}\right)^r f_{(j-k)(modN)} = \\
& \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \left(e^{2\pi i \frac{(j-k)(modN)}{N}}\right)^r f_{(j-k)(modN)} = \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \left(\omega_N^{(j-k)(modN)}\right)^r f_{(j-k)(modN)} = \\
& \frac{1}{N} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \sum_{j=0}^{N-1} \omega_N^{r(j-k)(modN)} f_{(j-k)(modN)} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{rk} e_k \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{rj} f_j = \\
& \widehat{e_r} \cdot \widehat{f_r}
\end{aligned}$$

□

where the addition of the $modN$ term in the power is due to the periodic property of the sin and cos functions that compose $e^{i\theta}$ with period of 2π, as seen in class and the last transition is with a change of index of the form $j \leftarrow (j-k)(modN)$ and realizing each index iterates over the whole range.

Question 2 - Order finding and Factoring

Let us consider $\mathbb{Z}_{21}^*$ and let us denote it as described in class:

$$\mathbb{Z}_{21}^* = \langle G_{21}, \cdot_{mod21} \rangle$$

$\mathbb{Z}_{21}^*$ is the group with a set of all natural numbers between 1 and 20 who are co-prime with 21, and $\cdot_{mod21}$ is the binary operation of multiplication modulo 21. Formally:

$$G_{21} = \{k \in [1,20] \mid gcd(21,k) = 1\} \; ; \; \forall a,b \in G_{21} \; : \; a \cdot_{mod21} b = a \cdot b \; mod21$$

Let us write out G_{21} explicitly:

$$G_{21} = \{1,2,4,5,8,10,11,13,16,17,19,20\}$$

One can see that 1 is the neutral element in $\mathbb{Z}_{21}^*$ with regards to the defined operation. For each element $x \in G_{21}$, let us consider the following table as required:

x	$r_x = ord_{21}(x)$	is r_x even and is $x^{r_x/2} \neq -1 \; mod21$
1	1	no
2	6	yes
4	3	no
5	6	no
8	2	yes
10	6	yes
11	6	yes
13	2	yes
16	3	no
17	6	no
19	6	yes
20	2	no

For elements $x \in G_{21}$ that satisfy r_x is even and $x^{r_x/2} \neq -1 \; mod21$:

x	$x^{r_x/2}$	$gcd(x^{r_x/2} - 1, 21)$	$gcd(x^{r_x/2} + 1, 21)$
2	8	7	3
8	8	7	3
10	13	3	7
11	8	7	3
13	13	3	7
19	13	3	7

One can see that $|G_{21}| = \varphi(21) = 12$ (where $\varphi(n)$ is Euler's totient function - a function that exactly counts the number of elements in $\mathbb{Z}_n^*$). The second table shows there are exactly 6 elements $x \in G_{21}$ that satisfy that r_x is even and $x^{r_x/2} \neq -1 \; mod21$. Thus:

$$Pr(r \; is \; even \; and \; x^{r_x/2} \neq -1 \; mod21) = \frac{6}{12} = \frac{1}{2}$$

with accordance to what we saw in class.

Question 3 - Hadamard Transform over a Subspace

Let $A \subset \mathbb{F}_2^n$ be a subspace and let us define a new operator $\odot$ for $x, y \in \mathbb{F}_2^n$:

$$\odot : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \{0,1\}$$
$$x \odot y = \Big(\sum_{i=0}^{n-1} x_i y_i\Big) mod N$$

We are to show that:

$$H^{\otimes n} \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle = \frac{1}{\sqrt{|A^\perp|}} \sum_{y \in A^\perp} |y\rangle$$

where: $A^\perp = \{y \in \mathbb{F}_2^n \mid \forall x \in A,\ \sum_{i=1}^n x_i y_i = 0\ mod 2\}$ Let us start with the LHS:

$$H^{\otimes n} \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} H^{\otimes n} |x\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} \sum_{y \in \mathbb{F}_2^n} \frac{(-1)^{x \odot y}}{\sqrt{2^n}} |y\rangle =$$
$$\frac{1}{\sqrt{2^n}\sqrt{|A|}} \sum_{x \in A} \sum_{y \in \mathbb{F}_2^n} (-1)^{x \odot y} |y\rangle = \frac{1}{\sqrt{2^n}\sqrt{|A|}} \sum_{y \in \mathbb{F}_2^n} \sum_{x \in A} (-1)^{x \odot y} |y\rangle =$$
$$\frac{1}{\sqrt{2^n}\sqrt{|A|}} \Big(\sum_{y \in \mathbb{F}_2^n \setminus A^\perp} \sum_{x \in A} (-1)^{x \odot y} |y\rangle + \sum_{y \in A^\perp} \sum_{x \in A} (-1)^{x \odot y} |y\rangle \Big)$$

At this point, we would like the expression $\sum_{y \in \mathbb{F}_2^n \setminus A^\perp} \sum_{x \in A} (-1)^{x \odot y} |y\rangle$ to be summed up to zero. In order to do so, let us define the transformation T_y for $y \in \mathbb{F}_2^n$ as follows:

$$T_y : A \to \{0,1\}$$
$$T_y(x) = x \odot y = \Big(\sum_{i=0}^{n-1} x_i y_i\Big) mod N$$

Lemma 1. *T_y is a linear transformation*

Proof. We will show additivity and homogeneity of T_y:

- For $v, u \in A$, $T_y(v+u) = T_y(v) + T_y(u)$

$$\begin{aligned} T_y(v+u) = \quad & y \odot (v+u) = \\ & \Big(\sum_{i=0}^{n-1} y_i (v+u)_i\Big) mod N = \Big(\sum_{i=0}^{n-1} y_i v_i + y_i u_i\Big) mod N = \\ & \Big(\sum_{i=0}^{n-1} y_i v_i\Big) mod N + \Big(\sum_{i=0}^{n-1} y_i u_i\Big) mod N = T_y(v+u) = T_y(v) + T_y(u) \end{aligned}$$

- For $v \in \mathbb{F}_2$ and $\alpha \in \mathbb{F}$, $T_y(\alpha v) = \alpha T_y(v)$

$$T_y(\alpha v) = y \odot \alpha v = \Big(\sum_{i=0}^{n-1} y_i \alpha v_i\Big) mod N = \alpha \Big(\sum_{i=0}^{n-1} y_i v_i\Big) mod N = \alpha T_y(v)$$

□

Now, we would like to show that for each $y \in \mathbb{F}_2^n \setminus A^\perp$, $\sum_{x\in A}(-1)^{x\odot y}|y\rangle = 0$, in order to do so we will use T_y and the Rank–Nullity theorem. So, let $y \in \mathbb{F}_2^n \setminus A^\perp$ and T_y to be the corresponding transformation as defined above. Since $y \notin A^\perp$, there exists $x \in A$ such that $y \odot x = 1$. We will show that for half of the elements in A it holds that $x \odot y = 0$ and for the other half it holds that $x \odot y = 1$ and thus the resulting expression will sum up to zero as required. Let us recall the Rank-Nullity theorem:

Theorem 1. *For any two vector spaces U, V and a linear transformation $T : U \to V$:*

$$dim(Ker(T)) + dim(Im(T)) = dim(U)$$

Applying the theorem for T_y and A:

$$dim(Ker(T_y)) + dim(Im(T_y)) = dim(A)$$

Since $dim(Im(T_y)) = dim(\{0, 1\}) = 1$:

$$dim(Ker(T_y)) + 1 = dim(A)$$

Since, $A \subseteq \mathbb{F}_2^n$, then $|A| = 2^{dim(A)}$ and so on for every vector space or subspace in $\mathbb{F}_2^n$:

$$\begin{aligned} 2^{dim(Ker(T_y))+1} &= 2^{dim(A)} \\ 2|Ker(T_y)| &= |A| \\ |Ker(T_y)| &= \frac{|A|}{2} \end{aligned}$$

Let us observe that:

$$\begin{aligned} Ker(T_y) &= \{x \in A \mid T_y(x) = y \odot x = 0\} \\ A \setminus Ker(T_y) &= \{x \in A \mid T_y(x) = y \odot x = 1\} \end{aligned}$$

and since $|Ker(T_y)| = \frac{|A|}{2}$

$$|Ker(T_y)| = |A \setminus Ker(T_y)| = \frac{|A|}{2}$$

Now let us observe that:

$$\sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\sum_{x\in A}(-1)^{x\odot y}|y\rangle = \sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\Big(\sum_{x\in A x\odot y=0}(-1)^{x\odot y}|y\rangle + \sum_{\substack{x\in A\\ x\odot y=1}}(-1)^{x\odot y}|y\rangle\Big) =$$

$$\sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\Big(\sum_{\substack{x\in A\\ x\odot y=0}}(-1)^{x\odot y} + \sum_{\substack{x\in A\\ x\odot y=1}}(-1)^{x\odot y}\Big)|y\rangle = \sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\Big(\sum_{\substack{x\in A\\ x\odot y=0}}1 - \sum_{\substack{x\in A\\ x\odot y=1}}1\Big)|y\rangle =$$

$$\sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\Big(|Ker(T_y)| - |A\setminus Ker(T_y)|\Big) = \sum_{y\in\mathbb{F}_2^n\setminus A^\perp} 0 = 0$$

And recall that:

$$\begin{aligned} H^{\otimes n}\frac{1}{\sqrt{|A|}}\sum_{x\in A}|x\rangle = \quad & \frac{1}{\sqrt{2^n}\sqrt{|A|}}\Big(\sum_{y\in\mathbb{F}_2^n\setminus A^\perp}\sum_{x\in A}(-1)^{x\odot y}|y\rangle + \sum_{y\in A^\perp}\sum_{x\in A}(-1)^{x\odot y}|y\rangle\Big) \\ &= \frac{1}{\sqrt{2^n}\sqrt{|A|}}\sum_{y\in A^\perp}\sum_{x\in A}(-1)^{x\odot y}|y\rangle = \frac{1}{\sqrt{2^n}\sqrt{|A|}}\sum_{y\in A^\perp}\sum_{x\in A}|y\rangle = \\ &\frac{1}{\sqrt{2^n}\sqrt{|A|}}\sum_{x\in A}\sum_{y\in A^\perp}|y\rangle = \frac{|A|}{\sqrt{2^n}\sqrt{|A|}}\sum_{y\in A^\perp}|y\rangle = \frac{\sqrt{|A|}}{\sqrt{2^n}}\sum_{y\in A^\perp}|y\rangle \end{aligned}$$

Lemma 2. *For A and $A^\perp$ as defined above, $|A^\perp| = \frac{2^n}{|A|}$*

Proof. Let denote B to be the basis of A and k to be its dimension, then:

$$B = \{b_0, b_1, ..., b_{k-1}\}$$

let us define matrix $T \subseteq \mathbb{F}_2^{n \times n}$ that the first k rows are the elements of B, and the rest $n-k$ rows are zeros:

$$T = \begin{bmatrix} & b_0 & \\ & b_1 & \\ & \vdots & \\ & b_{k-1} & \\ 0 & \cdots & 0 \\ & \vdots & \\ 0 & \cdots & 0 \end{bmatrix}$$

From Rank–Nullity theorem:

$$\begin{aligned} &dim(\mathbb{F}_2^n) = dim(Ker(T)) + Rank(T) \\ &n = dim(Ker(T)) + k \\ &2^n = 2^{dim(Ker(T))+k} = 2^{dim(Ker(T))}2^k = 2^{dim(Ker(T))}|A| \\ &\frac{2^n}{|A|} = 2^{dim(Ker(T))} \end{aligned}$$

Now we will show that $ker(T) = A^\perp$ with bidirectional containment:

- $ker(T) \subseteq A^\perp$
  Let $x \in Ker(T)$, so by $Ker(T)$ definition, $Tx = 0$. Since the multiplication of the first rows of T which are the elements of B, the basis of A, with x, results in zeros, it holds that for any $y \in A$, $y^T x = 0 = x \odot y$. Thus, $x \in A^\perp$
- $A^\perp \subseteq ker(T)$
  Let $x \in A^\perp$, so by $A^\perp$ definition, for any $y \in A$, $x \odot y = 0$, and specifically for the elements of the basis, which are in the first k rows of T. Thus, $Tx = 0$ and $x \in Ker(T)$.

So:

$$\frac{2^n}{|A|} = 2^{dim(Ker(T))} = 2^{dim(A^\perp)} = |A^\perp|$$

□

For conclusion:

$$H^{\otimes n}\frac{1}{\sqrt{|A|}}\sum_{x\in A}|x\rangle = \frac{\sqrt{|A|}}{\sqrt{2^n}}\sum_{y\in A^\perp}|y\rangle = \frac{1}{\sqrt{\frac{2^n}{|A|}}}\sum_{y\in A^\perp}|y\rangle = \frac{1}{\sqrt{|A^\perp|}}\sum_{y\in A^\perp}|y\rangle$$

Question 4 - Addition by Using Quantum Fourier Transform

Let us consider a system of $n \in \mathbb{N}$ qubits and let $N = 2^n$. Let us denote $|x\rangle$ as a basis vector of an n-qubits system, as in a $2^n = N$ dimensional vector. Instead of writing out x as a binary string of length n, let us consider x as a decimal number in the range $0 \leq x \leq N-1$ such that each number represents a different basis vector; i.e. 0 stands for 0^n, 1 stands for $0^{n-1}1$, 2 represents $0^{n-2}10$ and so forth.

4.1

In this section we are to implement the following phase shift as a circuit:

$$|x\rangle \to e^{\frac{2\pi i x}{N}}|x\rangle$$

One can express x in the following manner:

$$x = \sum_{k=0}^{n-1} x_{n-k} 2^k$$

where $x_1, ..., x_n \in \{0, 1\}$. Thus:

$$\frac{x}{N} = \frac{x}{2^n} = \sum_{k=0}^{n-1} x_{n-k} 2^{k-n} = \sum_{k=0}^{n-1} \frac{x_{n-k}}{2^{n-k}} = \sum_{k=1}^{n} \frac{x_k}{2^k}$$

where the last transition is by a change of summation index and adding the terms in reversed order. Thus we have that the state $|x\rangle$ can be expressed in terms of $x_1, ..., x_n$ in the following manner:

$$|x\rangle = |x_1 x_2 ... x_{n-1} x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |x_n\rangle = \bigotimes_{j=1}^{n} |x_j\rangle$$

For each $x_j \in \{0, 1\}$ such that $0 \leq j \leq n-1$ let us define a corresponding gate by the transformation T_j using the one-qubit phase shift gate with the parameter $\theta = \frac{2\pi}{2^j}$:

$$T_j = U_{\frac{2\pi}{2^j}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^j}} \end{bmatrix}$$

For all θ, U_θ is unitary since its columns form an orthonormal basis of $\mathbb{C}^2$ with respect to the usual inner product. Thus T_j is unitary.

Lemma 3. *Let $x_j \in \{0, 1\}$ such that $0 \leq j \leq n-1$. Then $T_j|x_j\rangle = e^{\frac{2\pi i}{2^j} x_j}|x_j\rangle$.*

Proof. Let us apply T_j on $|x_j\rangle$. If $x_j = 0$:

$$T_j|x_j\rangle = T_j|0\rangle = U_{\frac{2\pi}{2^j}}|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^j}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle = e^{\frac{2\pi i}{2^j} \cdot 0}|0\rangle$$

If $x_j = 1$:

$$T_j|x_j\rangle = T_j|1\rangle = U_{\frac{2\pi}{2^j}}|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{N}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{\frac{2\pi i}{2^j}} \end{bmatrix} = e^{\frac{2\pi i}{2^j}}|1\rangle = e^{\frac{2\pi i}{2^j} \cdot 1}|1\rangle$$

□

Using that, let us define:

$$T = \bigotimes_{j=1}^{n} T_j = T_1 \otimes T_2 \otimes \cdots \otimes T_{n-1} \otimes T_n$$

This gate is of course unitary, as it is composed of n unitary gates.

Claim 2. *Let $0 \leq x \leq N-1$. Then $T|x\rangle = e^{2\pi i \frac{x}{N}}|x\rangle$*

Proof. By properties of the Kronecker product, the above representation of x and the above lemma we have:

$$\begin{aligned} T|x\rangle = \quad & \bigotimes_{j=1}^{n} T_j \bigotimes_{j=1}^{n} |x_j\rangle = \\ & \Big(T_1 \otimes T_2 \otimes \cdots \otimes T_{n-1} \otimes T_n\Big)\Big(|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |x_n\rangle\Big) = \\ & \bigotimes_{j=1}^{n} T_j|x_j\rangle = \bigotimes_{j=1}^{n} e^{\frac{2\pi i}{2^j}x_j}|x_j\rangle = \prod_{j=1}^{n} e^{\frac{2\pi i}{2^j}x_j} \bigotimes_{j=1}^{n} |x_j\rangle = e^{2\pi i \sum_{j=1}^{n} \frac{x_j}{2^j}}|x\rangle = \\ & e^{2\pi i \frac{x}{N}}|x\rangle \end{aligned}$$

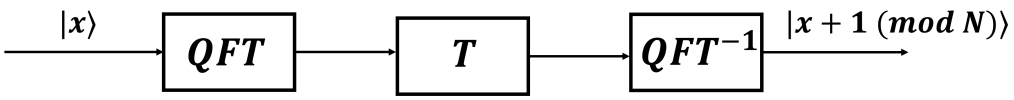
□

4.2

In this section we are to implement the transformation as a circuit:

$$|x\rangle \rightarrow |x+1(modN)\rangle$$

Using the transformation T defined in the last section, let us observe the following circuit:



Claim 3. *Let F_N be the Quantum Fourier Transform over $\mathbb{Z}_N$. Let us define $\psi = F_N^{\dagger} T F_N$ and let $0 \leq x \leq N-1$. Then ψ is unitary and $\psi|x\rangle = |x+1(modN)\rangle$.*

Proof.

Lemma 4. *For all unitary matrices $U, V \in \mathbb{C}^{k\times k}$, the matrix UV is also unitary.*

Proof. Let $U, V \in \mathbb{C}^{k\times k}$ be two unitary matrices. Since they're unitary, we have:

$$UU^{\dagger} = I_{k\times k} \ ; \ VV^{\dagger} = I_{k\times k}$$

Thus:

$$UV(UV)^{\dagger} = UVV^{\dagger}U^{\dagger} = UI_{k\times k}U^{\dagger} = UU^{\dagger} = I_{k\times k}$$

□

By the lemma and the definition of ψ we have that ψ is unitary. To prove the second part, let us consider each transition in ψ:

1. We first start out with our vector $|x\rangle$ that we apply a QFT to. Thus, by the definition of QFT as we saw in class:
$$F_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle$$

2. After the QFT, we apply the transformation T on the result and get (by the claim proven about the transformation T):
$$\begin{aligned} TF_N|x\rangle = \quad & T\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle = \\ & \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} T|y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} e^{2\pi i \frac{y}{N}} |y\rangle = \\ & \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{(x+1)y}{N}} |y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \left(e^{2\pi i \frac{(x+1)}{N}}\right)^y |y\rangle = \\ & \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \left(e^{2\pi i \frac{(x+1)(modN)}{N}}\right)^y |y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{(x+1)(modN)}{N} y} |y\rangle \end{aligned}$$
where the penultimate transition is due to the periodic property of the sin and cos functions that compose $e^{i\theta}$ with period of 2π, as seen in class.

3. Finally we apply the inverse QFT and get (by definition) ψ:
$$F_N^\dagger TF_N|x\rangle = \psi|x\rangle = F_N^\dagger \frac{1}{\sqrt{N}} \sum_{y=0}^{n-1} e^{2\pi i \frac{(x+1)(modN)}{N} y} |y\rangle = |x+1(modN)\rangle$$

□

Question 5 - A different Fourier Transform

Let us consider a system of $n \in \mathbb{N}$ qutrits and let $N = 3^n$. In this question we are to consider the Fourier Transform over the group $\mathbb{Z}_{3^n} = \mathbb{Z}_N$ and design a quantum circuit that works with qutrits and computes their Fourier Transform.
For one qutrit, let us consider the Quantum Fourier Transform in the case for $N = 3$. By the definition we saw in class, the element j, k for $0 \leq j \leq k \leq 2$ of the Fourier Transform transformation matrix will be in this case:

$$(F_3)_{j,k} = \frac{1}{\sqrt{3}} e^{\frac{2\pi i}{3} jk} = \frac{1}{\sqrt{3}} e^{\frac{2\pi i}{3} jk}$$

Let us write this matrix out explicitly:

$$F_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{2\pi i}{3^s}} & e^{\frac{4\pi i}{3^s}} \\ 1 & e^{\frac{4\pi i}{3^s}} & e^{\frac{8\pi i}{3^s}} \end{bmatrix}$$

Using the same notation used in question 4, let $0 \leq x \leq N-1$ and let us consider its equivalent representation:

$$x = \sum_{k=0}^{n-1} x_{n-k} 3^k$$

$x_1, ..., x_n \in \{0, 1, 2\}$. Let us consider the application of F_N on $|x\rangle$ as we already saw in question 4, and its equivalent form using the Kronecker product representation which we saw in class. In each element in the product, let us consider a linear combination of three basis vectors $(|0\rangle, |1\rangle, |2\rangle)$ instead of the usual two for qubits:

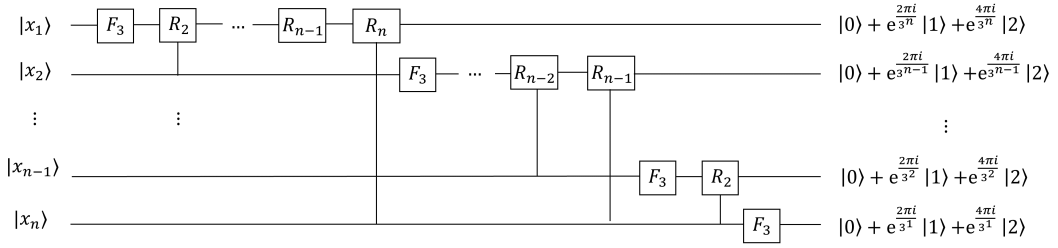
$$\begin{aligned} F_N|x\rangle = \quad & F_N|x_1 x_2 ... x_{n-1} x_n\rangle = \\ & \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |y\rangle = \\ & \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \Big(\sum_{k_l=0}^{2} e^{\frac{2\pi i}{3^l} x k_l} |k_l\rangle \Big) = \\ & \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \Big(|0\rangle + e^{\frac{2\pi i}{3^l} x} |1\rangle + e^{\frac{4\pi i}{3^l} x} |2\rangle \Big) \end{aligned}$$

Thus let us construct an augmented version of the R_s gate for qutrits which we will denote as $R_{s_{qutrit}}$:

$$R_{s_{qutrit}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2\pi i}{3^s}} & 0 \\ 0 & 0 & 0 e^{\frac{4\pi i}{3^s}} \end{bmatrix}$$

Then, we construct a circuit similar to that seen in class, but instead of applying Hadamard (which is the Fourier Transform for the case in which $N = 2$) initially for each qutrit, we first apply F_3 as defined above and then apply the augmented $R_{s_{qutrit}}$ sequentially similar to what was seen in class.

So finally let us observe the following circuit for the Fourier Transform for qutrits:



Not shown in the figure is the coefficient of $\frac{1}{\sqrt{3}}$ for conciseness. Moreover, as also seen in class, after applying this circuit, the qutrits are then reversed

Question 6 - Shor's Code

Let $|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)^{\otimes 3}$. Let us observe that this expression is exactly the 9-qubit Shor codeword for the original state $|0\rangle$. Let us suppose the first qubit of the state is measured. We are first to calculate the two possible states after the measurement was performed, assuming no errors occur other than the measurement itself.
Let us observe that each element in $|\psi\rangle$ starts with a block of either three zeros or three ones. Thus, when measuring the first qubit - we immediately know what the second and third qubits are. Thus, let us consider the two possible results of the measurement. If a 0 was measured:

$$|\psi_0\rangle = \frac{1}{2}|000\rangle \otimes (|000\rangle + |111\rangle)^{\otimes 2}$$

and if a 1 was measured:

$$|\psi_1\rangle = \frac{1}{2}|111\rangle \otimes (|000\rangle + |111\rangle)^{\otimes 2}$$

Now we are to calculate what happens in each step of the error correcting procedure. Let us consider the protocol for Shor's quantum error-correction as seen in class by its steps:

1. **Bit-flip error-correction**
   Bit-flip error-correction as seen in class guarantees error-correction for up to one bit flip. It uses auxiliary qubits to determine which qubit has flipped in each triplet block and produces a 2-bit syndrome with the index of the flipped qubit. Then it applies the X quantum gate upon it to flip it back.
   In the case discussed here, every triplet block in each element of $|\psi_0\rangle$ and $|\psi_1\rangle$ is composed of exactly three zeros or three ones either way, because no errors occur other than the measurement. Thus, all the syndromes of all the triplet blocks for both cases will be measured to 00 and thus no X gates will be applied and in either case, the state will remain the same. Thus the error-correcting procedure in this case will yield the state after the measurement, as in $|\psi_0\rangle$ and $|\psi_1\rangle$.
   In the final stage of the Bit-flip error-correction, the protocol decodes the states back from the block triplets to single qubits and thus at this stage the states will be:

$$|\psi_0\rangle = \frac{1}{2}|0\rangle \otimes (|0\rangle + |1\rangle)^{\otimes 2} = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |+\rangle \otimes |+\rangle$$
$$|\psi_1\rangle = \frac{1}{2}|1\rangle \otimes (|0\rangle + |1\rangle)^{\otimes 2} = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \otimes |+\rangle \otimes |+\rangle$$

2. **Phase-flip error-correction**
   The phase-flip error correction is applied, as seen in class in the $\{|+\rangle, |-\rangle\}$ basis. We can write the states as follows:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |-++\rangle)$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|+++\rangle - |-++\rangle)$$

   Using the auxiliary qubits (that are initialized to $|00\rangle$, the states will be:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |-++\rangle)|00\rangle$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|+++\rangle - |-++\rangle)|00\rangle$$

   After applying the phase-flip correction protocol, the states will be:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|+++\rangle|00\rangle + |-++\rangle|01\rangle)$$
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|+++\rangle|00\rangle - |-++\rangle|01\rangle)$$

Now the protocol measures the auxiliary qubit of each element. If the result is 0 - it does not perform a phase-flip correction because there is no error. If the result is other than 0 - it performs a bit correction error using the quantum Z gate on the qubit with the index corresponding to the measurement result. We can see that in both cases - the protocol will produce a final corrected result. Thus the states at this point will be:

$$|\psi_0\rangle = |+++\rangle$$
$$|\psi_1\rangle = |+++\rangle$$

In the final stage of the Phase-flip error-correction, the protocol decodes the states back from the block triplets to single qubits and thus at this stage the states will be:

$$|\psi_0\rangle = |+\rangle$$
$$|\psi_1\rangle = |+\rangle$$

3. **Decode Phase**
   In the final stage of the protocol, we decode the states back to the standard basis using the Hadamard transform and get the final results of:

$$|\psi_0\rangle = |0\rangle$$
$$|\psi_1\rangle = |0\rangle$$

Now, let us recall that the original codeword was the codeword for the original state $|0\rangle$ and thus the protocol will produce the correct result in either case.