

We can analyze the amplitudes more generally for an n -qubit QFT circuit as follows.

$$\omega^{x \cdot 2^{n-k}} = e^{\frac{2\pi i \cdot 2^{n-k}}{2^n} \cdot x} \quad (33)$$

$$= e^{2\pi i \left[\frac{2^{n-k}}{2^n} \right] [x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \dots + x_n \cdot 2^{n-n}]} \quad (34)$$

$$= \prod_{j=1}^n e^{2\pi i \left[\frac{2^{n-k}}{2^n} \right] \cdot x_j \cdot 2^{n-j}} \quad (35)$$

$$= \prod_{j=1}^n e^{2\pi i \left[\frac{2^{n-k-j}}{2^n} \right] \cdot x_j} \quad (36)$$

$$= \prod_{j=n-k+1}^n e^{2\pi i [2^{n-k-j}] \cdot x_j}. \quad (37)$$

Note the index change in the last line. In the case where $n - k - j < 0$, then the exponent is an integer multiple of $2\pi i$, which makes the term in the product always equal 1. The condition can be simplified to $n - k < j$, meaning we can discard the terms in the product less than or equal to $n - k$.

The final line gives insight into what the circuit may need to look like. Since x_j is the j -th bit of x , we see that when $x_j = 0$, it will kill off that entire term (set it to 1). In other words, we only want to apply the phase when $x_j = 1$. This sounds a lot like a controlled gate!

Question 36. What is the relative phase of the second qubit after applying a QFT circuit to the three qubit input state $|101\rangle$?

The controlled gate we want to apply has to apply a relative phase conditioned on the x_j -th qubit being 1. To do this, let's define a new gate:

$$P_a = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^a} \end{bmatrix}. \quad (38)$$

We have all the pieces now to construct the algorithm.

Algorithm 1 Quantum Fourier Transform

```
1: for  $k = 1$  to  $n$  do                                     ▶ Apply  $|x^k\rangle \rightarrow |0\rangle + e^{2\pi i \cdot x \cdot 2^{k-1}} |1\rangle$ 
2:   Apply  $H$  to  $|x_k\rangle$ 
3:   for  $j = k + 1$  to  $n$  do
4:     if  $x_j = 1$ , apply  $R_{j-k+1}$ 
5:   end for
6: end for
7: Reorder the qubits using swap gates
```

Question 37. Draw the Quantum Fourier Transform circuit for 4 qubits.

2.2 Properties of the Fourier Transform

Learning Outcomes

Upon following these notes and the corresponding lecture, students will be able to

- describe the property of the function period finding is trying to decide.
- produce and interpret a continued fractions representation of a decimal valued number.
- analyze the period finding algorithm and its correctness.

The power of the QFT is in its ability to *represent* periodic sequences or functions. This may mean that it is also effective at *finding* periodic structure in sequences as well! Before exploring this thought, let's look at some properties of the Fourier Transform.

Let me introduce some more notation we will use through the remainder of this section. We've learned and practiced the mapping from a standard basis state to a Fourier basis state. What happens if we apply the Fourier transform to a superposition of standard basis states?

Question 38. Consider the two qubit state

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle. \quad (39)$$

What is the result of applying the QFT to this state?

More generally, if we have an n qubit state

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad (40)$$

and apply QFT_N to it, we get the following:

$$QFT_N |\psi\rangle = QFT_N \left(\sum_{x=0}^{N-1} \alpha_x |x\rangle \right) \quad (41)$$

$$= \sum_{x=0}^{N-1} \alpha_x QFT_N |x\rangle \quad (42)$$

$$= \sum_{x=0}^{N-1} \alpha_x \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x \cdot y} |y\rangle \quad (43)$$

$$= \sum_{y=0}^{N-1} \underbrace{\sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} \alpha_x \omega^{x \cdot y}}_{\widetilde{\alpha}_y} |y\rangle \quad (44)$$

We will call the amplitudes $\widetilde{\alpha}_y$ the Fourier amplitudes. Using the vector notation, this means the QFT is doing the following transformation:

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \\ \alpha_{N-1} \end{bmatrix} \xrightarrow{QFT_N} \begin{bmatrix} \widetilde{\alpha}_0 \\ \widetilde{\alpha}_1 \\ \vdots \\ \widetilde{\alpha}_{N-2} \\ \widetilde{\alpha}_{N-1} \end{bmatrix} \quad (45)$$

Question 39. Consider the state $|\psi\rangle$ from Question 38. What is $\widetilde{\alpha}_3$?

2.2.1 The Fourier transform converts between translation and phase

Let

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad (46)$$

and

$$|\psi_{+j}\rangle = \sum_{x=0}^{N-1} \alpha_x |x + j \bmod N\rangle = \sum_{x=0}^{N-1} \alpha_x |x + j\rangle. \quad (47)$$

The $+j$ state is simply the state we get by shifting the amplitudes cyclically by j positions. The last inequality is just a notational difference, where we will abbreviate the mod N in this notation.

Question 40. Suppose we have the following two qubit state:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle . \quad (48)$$

What is $|\psi_{+1}\rangle$?

Question 41. Apply the QFT to $|\psi_{+j}\rangle$.

Again, let's take a look at what happens to an n -qubit state $|\psi_{+j}\rangle$ and apply the Fourier transform to it.

$$\widetilde{|\psi_{+j}\rangle} = \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \frac{\alpha_x \omega^{(x+j) \cdot y}}{\sqrt{N}} |y\rangle \quad (49)$$

$$= \sum_{y=0}^{N-1} \omega^{jy} \underbrace{\sum_{x=0}^{N-1} \frac{\alpha_x \omega^{x \cdot y}}{\sqrt{N}}}_{\widetilde{\alpha}_y} |y\rangle \quad (50)$$

$$= \sum_{y=0}^{N-1} \omega^{jy} \widetilde{\alpha}_y |y\rangle . \quad (51)$$

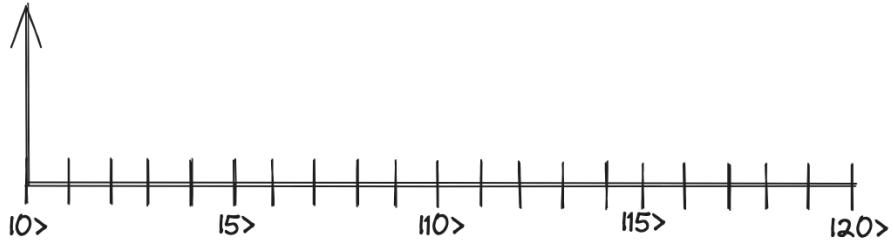
We can think of the index in the standard basis as representing the index of a particular wave x that we use to construct our periodic function. When we translate our position by applying the $+j$ transformation and apply the Fourier transform after this, we now want to pick the $x + j$ -th wave instead.

2.2.2 Fourier Transform of Factors

Suppose r is an integer that divides N (N/r is an integer). Define the state

$$|\phi_r\rangle = \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr\rangle. \quad (52)$$

Question 42. Let $N = 21$ and $r = 3$. What are the amplitudes that appear in this vector? Draw them in the figure below.



Proposition 2.2. Let r be an integer that divides N . Then,

$$QFT_N |\phi_r\rangle = |\phi_{N/r}\rangle. \quad (53)$$

Question 43. Continuing the example from Question 42, what is $|\phi_{N/r}\rangle$?

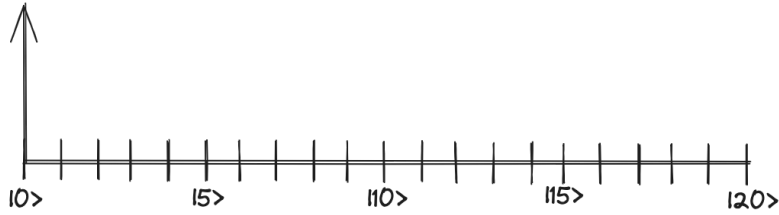
Question 44. Still continuing the example from Question 42, what is $QFT_N |\phi_r\rangle$?

2.2.3 Periodic Superpositions with a Shift

The crux of Shor's algorithm is the solution to the following problem: Suppose we have a periodic superposition but with a shift:

$$\sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr + l\rangle. \quad (54)$$

Can we find an algorithm to find r ?



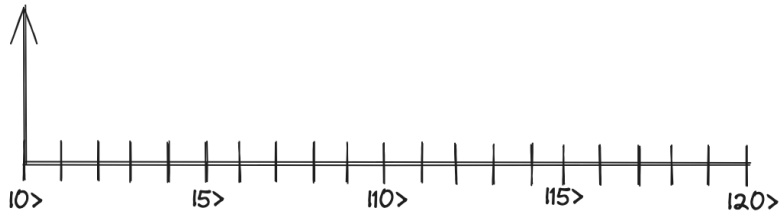
To further complicate the problem, every time we generate a new version of the state, the shift constant l will be different. This causes issues later, because when we use the QFT for factoring, the offset does not allow us to cleanly divide N in the way that it does in Proposition 2.2.

Let's formalize the problem. We consider starting with some state

$$|\phi_r\rangle = \frac{1}{\sqrt{s}} \sum_{k=0}^{s-1} |kr + l\rangle \quad (55)$$

where we have defined $0 \leq l < r$ and $s = \lfloor \frac{N}{r} \rfloor$. There are two challenges we will have to resolve to correctly figure out what r is.

1. N will generally be a power of 2, meaning that r does not divide N most of the time.
2. The shift l causes the QFT to not work as cleanly.



Proposition 2.3. Consider applying an n -qubit QFT to some state

$$|\phi_r\rangle = \frac{1}{\sqrt{s}} \sum_{k=0}^{s-1} |kr + l\rangle. \quad (56)$$

We can express this state as

$$QFT_N |\phi_r\rangle = \sum_{a=0}^{N-1} \widetilde{\alpha}_a |a\rangle. \quad (57)$$

If we measure this output state, then with high probability we measure a value a such that

1. $|a - k\frac{N}{r}| \leq \frac{1}{2}$ for some k .
2. $\gcd(k, r) = 1$.

The first property can be rewritten as

$$\left| \frac{a}{N} - \frac{k}{r} \right| \leq \frac{1}{2N}. \quad (58)$$

From our measurement result, we know what a is, and N depends on the system size. What the above equation is saying is that $\frac{a}{N}$ is a *very* close approximation of $\frac{k}{r}$. We can use this information to find k and r , independent of what l is!

2.3 Period Finding

Let's look at our first algorithm that uses the QFT. This will be another query based algorithm, meaning that we will have access to some blackbox function, and are trying to decide some property for this function.

Suppose we have some function $f : \{0, \dots, N-1\} \rightarrow \{0, \dots, M-1\}$ or alternatively in the bitstring notation, $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. Here, we've defined the integers such that $N = 2^n$ and $M \leq 2^m$. This function will also have the property that for some integer r ,

$$f(x) = f(y) \Leftrightarrow x - y \text{ is an integer multiple of } r \leq M < \sqrt{N}. \quad (59)$$

Given quantum access to this function via a unitary U_f , the goal is to find r .

Example.

This problem is interesting because there is no known efficient classical algorithm! The best we can do is a brute force search for "collisions" $f(x) = f(y)$, which on average will require $\sim 2^{n/2}$ time.

Question 45. Consider the function $f : \{0, 1\}^4 \rightarrow \{0, 1\}^4$, where

$$f(s) = 3^s \pmod{16}. \quad (60)$$

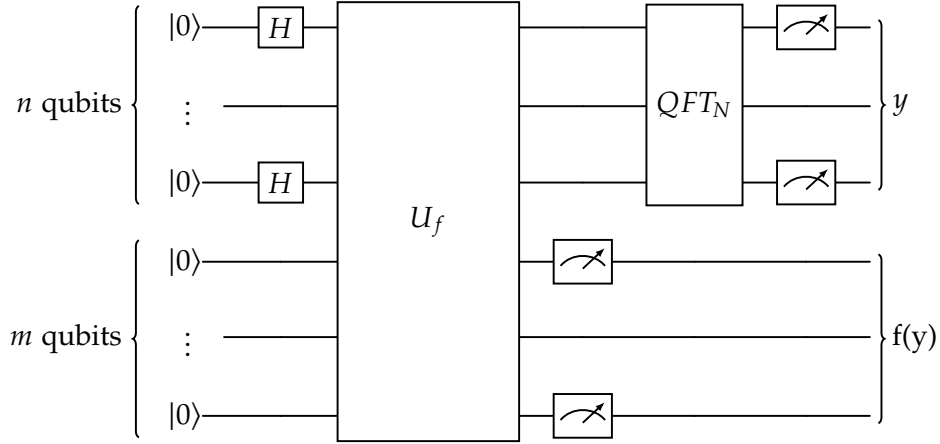
What is the period of f ?

I'll begin by just writing out the algorithm, and we will go over the analysis after seeing it. The algorithm will use two registers, the first using n qubits (to store numbers mod N), and the second register will have $\lceil \log M \rceil$ qubits to store numbers mod M . We will also have quantum access to the function f via a unitary U_f which has the action

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle. \quad (61)$$

Algorithm 2 Period Finding

- 1: Start with $|0 \dots 0\rangle |0 \dots 0\rangle$
 - 2: Apply $H^{\otimes n}$ on the first register to get $\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle |0\rangle$
 - 3: Apply U_f
 - 4: Measure the 2nd register.
 - 5: Ignore the 2nd register and apply $QFT_N(\text{mod } N)$ to the 1st register.
 - 6: Measure the 1st register to get value a .
 - 7: Postprocessing: Use a and N to find k and r .
-



Let's go through each step starting at 3 to see what the state is. At step 3, we will have prepared the state

$$\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle |f(y)\rangle \quad (62)$$

Now recall that the function $f(y)$ is periodic in r , meaning that for every $f(y)$, there will be r inputs that map to it.

Question 46. Consider the function we used in Question 45. If we had unitary access to this function and measured $|9\rangle$ in the second register, what is the state of the algorithm?

More generally, measuring the second register will allow us to collapse into a superposition of inputs that all map to the same state. More concretely, suppose we measured the value w in the second register. Then the first register will be an even superposition of all $|jr + l\rangle$ such that $f(jr + l) = w$, and $0 \leq j < \lfloor \frac{N}{r} \rfloor, 0 \leq l \leq r - 1$. We can write this in ket notation too:

$$\frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr + l\rangle |w\rangle \quad s := \left\lfloor \frac{N}{r} \right\rfloor. \quad (63)$$

We can safely ignore the second register for the remaining analysis, because the two registers are now in a product state.

By Proposition 2.3, we know that applying a QFT to this state and measuring will allow us with high probability to observe a state a such that

$$\left| a - k \frac{N}{r} \right| \leq \frac{1}{2} \quad \gcd(k, r) = 1. \quad (64)$$

The above equation can be combined with our assumption that $r < \sqrt{N}$ to get

$$\left| \frac{a}{N} - \frac{k}{r} \right| \leq \frac{1}{2N} \leq \frac{1}{2r^2}. \quad (65)$$

We will be using **continued fractions** to find k and r .

We will assume that $\gcd(k, r) = 1$. To analyze the final step, let's look at how continued fractions works. Let $\gamma = \frac{a}{N}$. We know that with high probability,

$$\left| \gamma - \frac{k}{r} \right| \leq \frac{1}{2r^2}. \quad (66)$$

The continued fractions representation of a real number is a sequence of integers $a_0, a_1, \dots, a_n$ as:

$$\gamma \approx a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots \frac{1}{a_n}}}} \quad (67)$$

We can clip this sequence at some a_k to get an approximation of γ . We will define the P_k and Q_k as the numerator and denominator we get respectively for the approximation of γ .

Question 47. Let $\gamma = 7.27$. Find the continued fractions representation of γ . What is P_3 and Q_3 ?

Once the continued fractions representation is found, we get a series of approximations to γ :

$$\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \dots, \frac{P_n}{Q_n} \quad (68)$$

such that

$$Q_0 < Q_1 < Q_2 < \dots < Q_n. \quad (69)$$

Each of the Q_j 's are candidates for r , and with access to the function f we can directly test the n candidates to see if we have the correct period. We know this will happen by the theorem stated below.

Theorem 2.4 (Proven in Nielsen and Chuang). If $|\gamma - \frac{k}{r}| \leq \frac{1}{r^2}$, then $k = P_j$ and $r = Q_j$ for some j .

Our algorithm will try each one and take the smallest Q_j such that

$$x^{Q_j} = 1 \pmod{N}. \quad (70)$$

We end the section with two important facts:

- If γ is a rational number, eventually for some n , $\frac{P_n}{Q_n} = \gamma$.
- $\frac{P_j}{Q_j}$ is the best approximation to γ by *any* ratio of integers whose denominator is $\leq Q_j$.