Quantum Fourier Transform II

The Quantum Fourier Transform (QFT) is a key ingredient in Shor's algorithm. Remember that we defined it as a linear combination of computational basis states for an n-Qbit register.

Suppose we have an n-bit register, which can hold N=2^n states, which we label in the usual manner $|0\rangle_n$ $|1\rangle_n$ $|3\rangle_n$ ... $|2^n\text{-}1\rangle_n$. Let’s define a linear superposition of these states

$$|\psi_m\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{m\,k}{N}}\,|\mathrm{k}\rangle_n$$

or

$$U_{\mathrm{FT}}|\mathrm{m}\,\rangle_n = |\psi_m\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{m\,k}{N}}\,|\mathrm{k}\rangle_n$$

We also learned that the q m th' matrix element of U_{FT} is given by

$$\langle \mathrm{q}\mid U_{\mathrm{FT}}|\ \mathrm{m}\,\rangle = \frac{1}{\sqrt{N}}\ e^{i\,2\pi\,\frac{m\,q}{N}}$$

and so it is easy to construct a matrix representation for U_{FT}, the Quantum Fourier Transform gate.

```
U[Num_] := 1 / Sqrt[Num] Table[Exp[2 I i j Pi / Num], {i, 0, Num - 1}, {j, 0, Num - 1}];
```

```
MatrixForm[U[2]]
```

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

```
Udag = Conjugate[Transpose[U[2]]];
MatrixForm[Udag]
```

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

```
FullSimplify[Udag.U[2]];
MatrixForm[%]
```

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

For large n this procedure gets cumbersome as we need to construct a n x n gate. Remember how classical gates, such as the n-bit adder can be built up from modular units of smaller gates. Can we do the same for the QFT gate? i.e. find a way to modularize it, this would be of great practically utility since we know how to build small 2 - Qubit gates and by connecting them together, like Lego blocks, we can construct the large n x n QFT gate. This is the question we are going to study below.

On some properties of QFT

Lets look at some specific cases, U_{FT} in detail. Suppose n=1 (N=2) (a single Qubit QFT)

we find (using the definition $U_{\mathrm{FT}}|\mathrm{m}\,\rangle_n = \frac{1}{\sqrt{N}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{m\,k}{N}}\,|\mathrm{k}\rangle_n$)

$$U_{\mathrm{FT}}|0\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{k=1} e^{i\,2\pi\,\frac{0\,k}{2}}\,|\mathrm{k}\rangle_n = \frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)$$

$$U_{\mathrm{FT}}|1\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{k=1} e^{i\,2\pi\,\frac{1\,k}{2}}\,|\mathrm{k}\rangle_n = \frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle\,)$$

which, as we remarked above, is also the Hadamard gate. Suppose now that n=2 (N=4) the computational basis are
$|0\rangle_2 = |00\rangle$, $|1\rangle_2 = |01\rangle$, $|2\rangle_2 = |10\rangle$, $|3\rangle_2 = |11\rangle$

and

$$U_{\mathrm{FT}}\,|00\rangle_2 = \frac{1}{\sqrt{4}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{0\,k}{4}}\,|\mathrm{k}\rangle_n = |0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2 = \frac{1}{2}(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,) =$$
$$\frac{1}{2}(\,|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$

$$U_{\mathrm{FT}}\,|01\rangle_2 = \frac{1}{\sqrt{4}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{1\,k}{4}}\,|\mathrm{k}\rangle_n = |0\rangle_2 + \mathrm{i}\,|1\rangle_2 - |2\rangle_2 - \mathrm{i}\,|3\rangle_2 = \frac{1}{2}(\,|00\rangle + \mathrm{i}\,|01\rangle - |10\rangle - \mathrm{i}\,|11\rangle) =$$
$$(\,|0\rangle - |1\rangle\,) \otimes (\,|0\rangle + \mathrm{i}\,|1\rangle\,)$$

```
Exp[2 Pi I k / 4] /. k → 0
```

```
1
```

$$U_{\mathrm{FT}}\,|10\rangle_2 = \frac{1}{\sqrt{4}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{2\,k}{4}}\,|\mathrm{k}\rangle_n = |0\rangle_2 - |1\rangle_2 + |2\rangle_2 - |3\rangle_2 = \frac{1}{2}(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,) =$$
$$\frac{1}{2}(\,|0\rangle + |1\rangle\,) \otimes (\,|0\rangle - |1\rangle\,)$$

$$U_{\mathrm{FT}}\,|11\rangle_2 = \frac{1}{\sqrt{4}} \sum_{k=0}^{k=N-1} e^{i\,2\pi\,\frac{3\,k}{4}}\,|\mathrm{k}\rangle_n = |0\rangle_2 - \mathrm{i}\,|1\rangle_2 - |2\rangle_2 + \mathrm{i}\,|3\rangle_2 = \frac{1}{2}(\,|00\rangle - \mathrm{i}\,|01\rangle - |10\rangle + \mathrm{i}\,|11\rangle) =$$
$$\frac{1}{2}(\,|0\rangle - |1\rangle\,) \otimes (\,|0\rangle - \mathrm{i}\,|1\rangle\,)$$

For these two cases we note that the QFT transform breaks up into pieces that involve products of single Qbit states. Is this true for any n-Qbit QFT ? The answer is yes, first validate this rule by trying evaluating, as above, the 3-Qbit QFT (See Class Project below).

In general it turns out that

$U_{\mathrm{FT}}|\, b_{n-1}\; b_{n-2}\; ...\; b_1 b_0\rangle = \;\frac{1}{2^{n/2}}\,(\,|\,0\,\rangle + e^{i\,2\pi\,[.b_0]}\,|1\,\rangle)\;\;(\,|\,0\,\rangle + e^{i\,2\pi\,[.b_1\,b_0]}\,|1\,\rangle)\;\;...\;\;(\,|\,0\,\rangle +$
$e^{i\,2\pi\,[.b_{n-1}\;b_{n-2}...\,b_1\,b_0]}\,|1\,\rangle)$.

where the b_n are the bit entries (0,1) in our register and the symbol

$[.\; b_0] \equiv b_0 \times 2^{-1}$

$[.\; b_0 b_1] \equiv b_0 \times 2^{-1} + b_1 \times 2^{-2}$

etc.

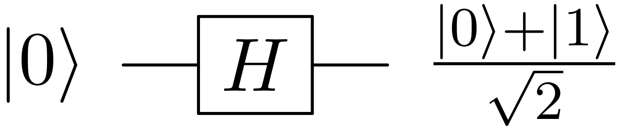
The importance of this result should be obvious. According to it, U_{FT} can simply be expressed as direct product of various linear
combinations of the single Qbits $|0\rangle$,$|1\rangle$. These linear combinations could be generated by a single bit gate (a 2 dimensional matrix).
However these gates must be connected somehow, for example lets look at the pair

$$\frac{1}{2^{n/2}}\,(\,|\,0\,\rangle + e^{i\,2\pi\,[.b_0]}\,|1\,\rangle)\;\;(\,|\,0\,\rangle + e^{i\,2\pi\,[.b_1\,b_0]}\,|1\,\rangle)$$

note that the one bit gate acting on the second Qbit depends on the value b_0, so this really describes a 2-Qbit gate.

Diagrammatics

It's now a good time to review how we describe quantum gates diagrammatically. Consider the Hadamard gate, a one Qbit gate, which
we represent diagrammatically as

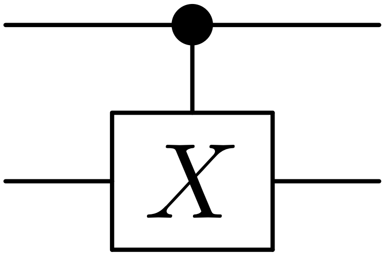


The gate is represented by the box and the single lead wire on the left represents the incoming state. The outgoing state
is represented by the lead wire on the right of the box (gate). The Hadamard gate is a single Qbit gate since there is only
one lead entering or leaving the box.

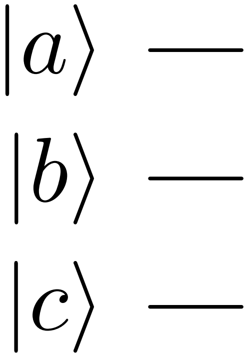
We also learned about the Controlled - Not gate CNOT. It is a two-Qubit gate and it's truth table looked like this

CNOT |00〉 = |00〉
CNOT |01〉 = |01〉
CNOT |10〉 = |11〉
CNOT |11〉 = |10〉

we can represent this by the following diagram



For an incoming state | a b c 〉 the lead wires would look like



For the CNOT gate
The top lead represents the control bit and the bottom lead represents target bit, which passes through a Pauli gate X.

The Pauli gate only gets activated (turned on) if the top lead has value |1〉.

We can define other control type gates simply by replacing the Pauli gate with another single Qbit gate. We now define
the following single Qbit phase gate

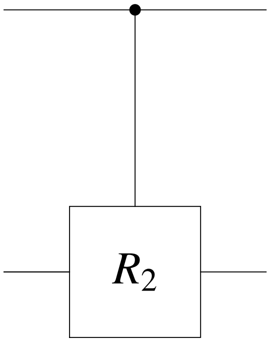
R_n It has the effect of multiplying any of the two single Qbit states by a phase factor

$e^{i\,2\pi/2^n}$ if the state is |1〉 and
by the phase factor 1 if the state is |0〉

The matrix representation for the R_n gate is

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\,2\pi/2^n} \end{pmatrix}$$

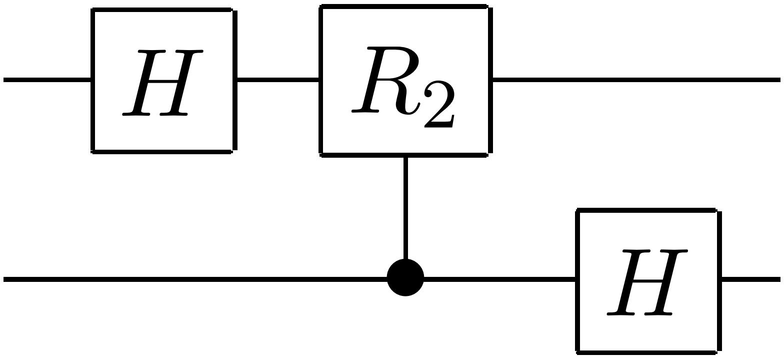
so let's consider the following



The truth table for this, two-Qbit, controlled phase gate is

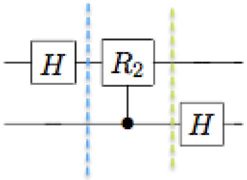
CR_2| 0 0 〉 = |0 0 〉
CR_2| 0 1 〉 = |0 1 〉
CR_2| 1 0 〉 = |1 0 〉 = |1 0 〉
CR_2| 1 1 〉 = $e^{i\,2\pi/4}$|1 1 〉 = i |1 1 〉

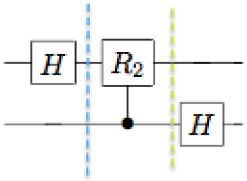
Lets now look at the following circuit



Class exercise: let the input state be $| 0\, 0 \rangle$, find the output state.

We start from left and proceed to right





At the dashed blue the input state $| 0 \rangle | 0\rangle$ goes into $H\otimes 1 | 0 \rangle | 0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\ |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)$

Now we pass through the control-R_2gate i.e and we get at the green line

$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

Can you see why this is true?

Finally, after the green dashed line we pass through another Hadamard gate

$1\otimes H\ \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}|0\rangle H|0\rangle + \frac{1}{\sqrt{2}}|1\rangle H|0\rangle = \frac{1}{2}|0\rangle(|0\rangle + |1\rangle) + \frac{1}{2}|0\rangle(|0\rangle + |1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$

We note this is the same as U_{FT} $|00\rangle_2$

Let's see what happens for the incoming state $|0\ 1\rangle$

At the green line we have

$$H\otimes 1\,|\,0\,\rangle|\,1\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle+|1\rangle)\ \ |1\rangle = \frac{1}{\sqrt{2}}(\,|01\rangle+|11\rangle)$$

Now we pass through the control-R_2gate

$$CR_2\ \frac{1}{\sqrt{2}}(\,|01\rangle+|11\rangle) = \frac{1}{\sqrt{2}}(\,|01\rangle+i\,|11\rangle)$$

Can you see why ?

Finally passing through the Hadamard gate again

$$1\otimes H\ \ \frac{1}{\sqrt{2}}(\,|01\rangle+i\,|11\rangle) = \frac{1}{2}\,(\,|0\rangle\otimes\,(|0\rangle-|1\rangle)\,+i\,|1\rangle\,\otimes\,(|0\rangle-|1\rangle\ \ ) = \frac{1}{2}\,(\,|0\rangle\,+\,i\,|1\rangle)\,\otimes\,(|0\rangle-|1\rangle)$$

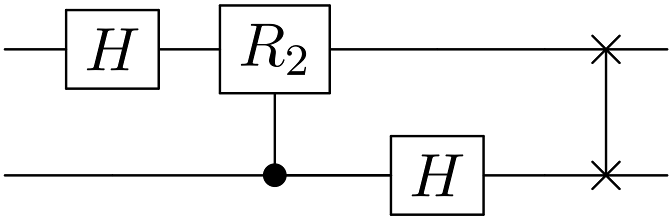
Note this is equal to $S_2 U_{\mathrm{FT}}$ $|01\rangle_2$ where $S_2$is a swap operator for 2 Qbits i.e

$S_2|\,a\ b\,\rangle=|b\ a\rangle$

(In general S_3 $|a\ b\ c\rangle$ = $|c\rangle S_2|\,a\ b\rangle$ = $|c\ b\ a\,\rangle$ etc.)
Let's check to see if indeed

for the remaining states $|1\ 0\,\rangle$ and $|\,1\ 1\,\rangle$ the above circuit is equal to

S_2 U_{FT} $|01\rangle_2$ and S_2 U_{FT} $|11\rangle_2$ respectively. Since S_2S_2=1 we then claim that U_{FT} for n=2, is equal to the following diagram



Matrix Representation of U_{FT}

In the previous notebooks we constructed matrix representations of U_{FT} . For the case n=2 it is given by

```
MatrixForm[U[4]]
```

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

Thus this matrix should also be obtained by an appropriate products of single and 2-Qubit operators shown in the diagram.
Remember we work from left to right.

```
zero = {1, 0};
one = {0, 1};
unit = {{1, 0}, {0, 1}};
hadamard = 1 / Sqrt[2] {{1, 1}, {1, -1}};
R2 = {{1, 0}, {0, Exp[2 Pi I / 2^k]} /. k → 2}
```

```
{{1, 0}, {0, i}}
```

```
(* for the Control R2 * we note that it can be wriiten in Dirac form *)
```

Identity $\otimes$ $|0\rangle\langle 0|$ + $R_2\otimes|1\rangle\langle 1|$

```
zerozero = KroneckerProduct[zero, zero]
oneone = KroneckerProduct[one, one]
```

```
{{1, 0}, {0, 0}}
```

```
{{0, 0}, {0, 1}}
```

```
CR2 = KroneckerProduct[unit, zerozero] + KroneckerProduct[R2, oneone];
MatrixForm[CR2]
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

```
(* from left to right, first gate *)
```

```
firstgate = KroneckerProduct[hadamard, unit];
MatrixForm[firstgate]
```

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

```
secondgate = CR2;
MatrixForm[CR2]
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

```
thirdgate = KroneckerProduct[unit, hadamard];
MatrixForm[thirdgate]
```

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

```
totalproduct = firstgate.secondgate.thirdgate;
MatrixForm[totalproduct]
```

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

Note that this matrix gives the product $\frac{1}{2^{n/2}}$ $(| 0 \rangle + e^{i\, 2\pi\, [.b_0]} |1 \rangle)$ $(| 0 \rangle + e^{i\, 2\pi\, [.b_1\, b_0]} |1 \rangle)$ swapped (i.e. bits 1 and 2 are interchanged) , but not the U_{FT} because we have not include the swap operator for two qubits. How does this operator look like? Well, by definition it requires

S $|a \rangle|b\rangle=|b\rangle|a\rangle$ for all possible a,b taking the matrix representation (as in our previous homework assignment) we obtain

```
S = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}};
MatrixForm[S]
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

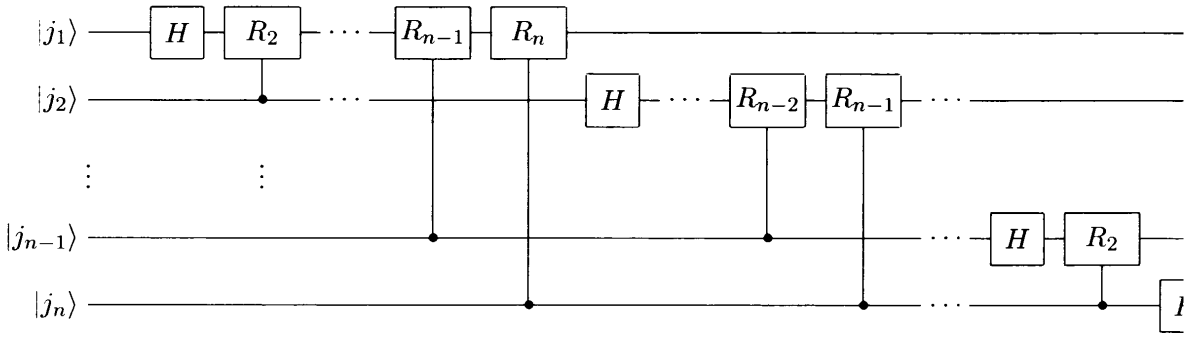
```
totalproduct = firstgate.secondgate.thirdgate.S
MatrixForm[totalproduct]
MatrixForm[U[4]]
```

$$\left\{\left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right\}, \left\{\frac{1}{2}, \frac{i}{2}, -\frac{1}{2}, -\frac{i}{2}\right\}, \left\{\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right\}, \left\{\frac{1}{2}, -\frac{i}{2}, -\frac{1}{2}, \frac{i}{2}\right\}\right\}$$

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

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

Thus we see that for n=2 the matrix representation for the above diagram does indeed equate to the matrix representation of our QFT gate. Does this work for any n? Yes! the diagram for it is (up to a final swap gate)



$|j_1\rangle$
$|j_2\rangle$
$|j_{n-1}\rangle$
$|j_n\rangle$
H
R_2
R_{n-1}
R_n
H
R_{n-2}
R_{n-1}
H
R_2