PHY365: Quantum Information
Part 2 (Lecture 10 and Beyond)

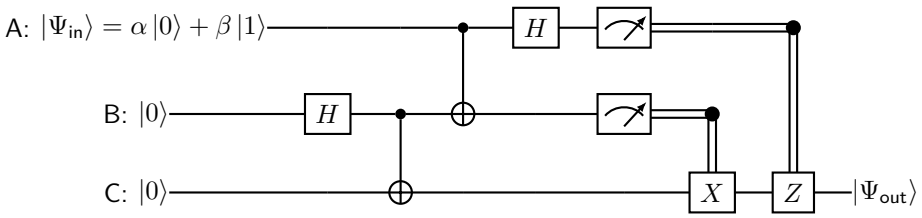
QiLin Xue

Winter 2022

Contents

1 Quantum Teleportation

Quantum teleportation is the transfer of the quantum state of one qubit to another (not the actual physical qubit) using a shared entangled resource and two classical bits of information. It is performed using the following circuit.



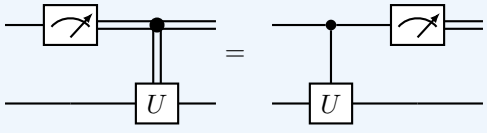
1. The input is
$$|\psi_1\rangle = \alpha|000\rangle + \beta|100\rangle \tag{1.1}$$

2. We create the entangled resource between B and C
$$|\Psi_1\rangle \to |\Psi_{\text{in}}\rangle \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to |\Psi_{\text{out}}\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.2}$$
which is
$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + |111\rangle) \tag{1.3}$$

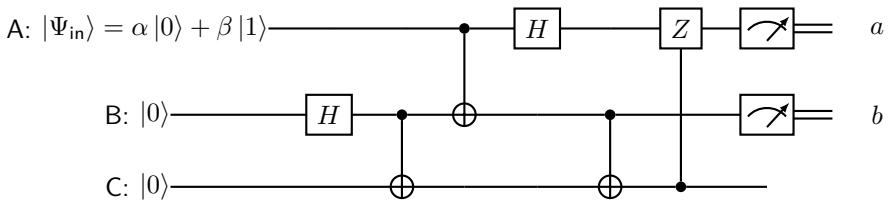
3. Bell state detection:
$$|\Psi_3\rangle = \text{CNOT}_{AB} \otimes I_C |\Psi_2\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \tag{1.4}$$
and
$$|\Psi_4\rangle = (\hat{H}_A \otimes I \otimes I)|\Psi_3\rangle = \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle). \tag{1.5}$$
We can clean this up a bit into:
$$|\Psi_4\rangle = \frac{1}{2}(\alpha\{|000\rangle + |100\rangle + |011\rangle + |111\rangle\} + \beta\{|010\rangle - |110\rangle + |001\rangle - |101\rangle\}) \tag{1.6}$$
$$= \frac{1}{2}(|00\rangle\{\alpha|0\rangle + \beta|1\rangle\} + |01\rangle\{\alpha|1\rangle + \beta|0\rangle\} + |10\rangle\{\alpha|0\rangle - \beta|1\rangle\} + |11\rangle\{\alpha|1\rangle - \beta|0\rangle\}) \tag{1.7}$$
$$= \frac{1}{2}\left(|00\rangle \hat{I}|\Psi_{\text{in}}\rangle + |01\rangle \hat{X}|\psi_{\text{in}}\rangle + |10\rangle \hat{Z}|\psi_{\text{in}}\rangle + |11\rangle \hat{X}\hat{Z}|\psi_{\text{in}}\rangle\right) \tag{1.8}$$

4. Sending classical bits: The target qubit is now in a linear combination of several states, depending on what the first two qubits are. Once the first two qubits are measured, and results are sent, then C can take the inverse to retrieve $|\psi_{\text{in}}\rangle$. After measurement, the state is:
$$|\Psi_{\text{proj}}\rangle_c = \hat{X}^b \hat{Z}^a |\Psi_{\text{in}}\rangle \tag{1.9}$$
To reconstruct it, we can apply:
$$|\Psi_{\text{out}}\rangle = \hat{Z}^a \hat{X}^b |\Psi_{\text{proj}}\rangle_c = |\Psi_{\text{in}}\rangle \tag{1.10}$$

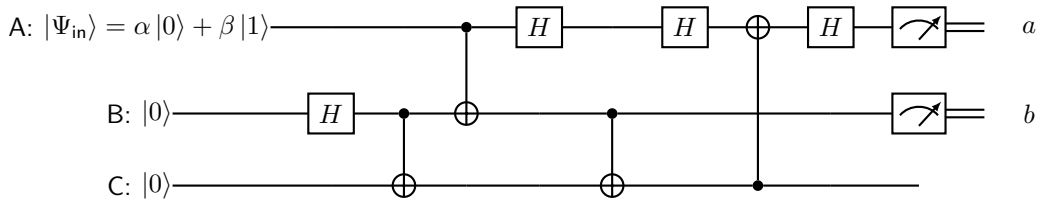
Let us now attempt to analyze this using a circuit-based approach. To do so, we need to use the **Griffiths-Niu Theorem.**

> **Theorem**: The following circuits, according to the Griffiths-Niu Theorem, are equivalent:
>
> 
>

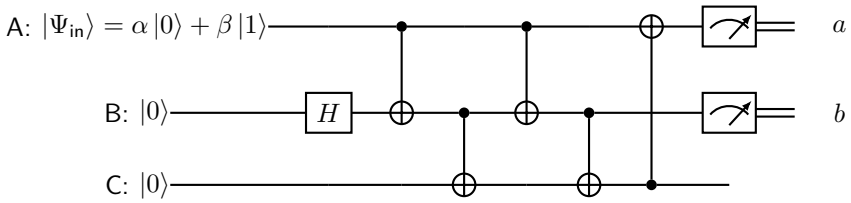
Using this theorem, we can redraw our circuit as:



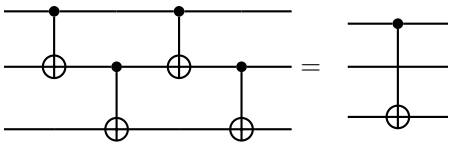
Recall that for a control-Z, it doesn't matter which one is the control and which one is the target. Using the identity $Z = HXH$, we can reduce it further:



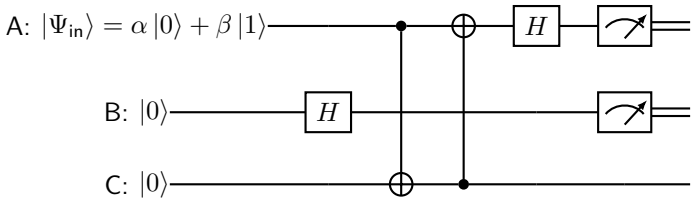
Since $H^2 = I$, we can simplify the top part. Furthermore, we can introduce another CNOT between the first and the second branch.



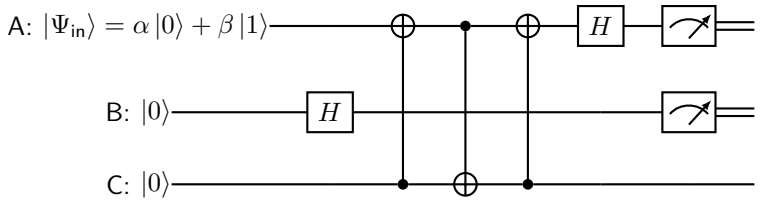
We were allowed to introduce this CNOT gate since $XH|0\rangle = H|0\rangle$. This actually makes it easier since the following two circuits are also equivalent:



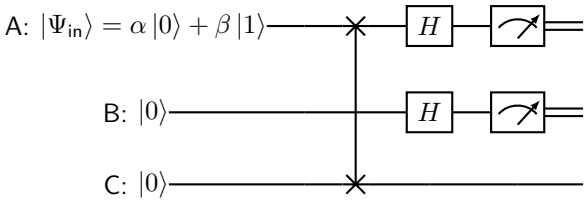
This can be proved by looking at how it maps the basis elements. Using this substitution, we end up with:



We can now introduce another CNOT gate, which doesn't do anything since C will always be $|0\rangle$.



Three alternating CNOT gates is equivalent to the SWAP gate, so we can write:



2 No-Cloning Theorem

It is impossible to clone a qubit. If this was possible, we can make an amplifier A that can effectively "measure" a qubit, allowing faster than light communication to happen. Here is how an amplifier actually works. An amplifier can act on single bits:

$$A|0\rangle = |00\rangle$$
$$A|1\rangle = |11\rangle$$

If it acts on a linear combination, it gives:

$$A\left(\frac{|0\rangle + |1\rangle}{2}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.1}$$

which is en entangled pair, and not the tensor product between two of these linear combinations.

3 Quantum Algorithms

NB: There's a course on this! CSC2332

3.1 Deutsch Algorithm

Consider a function $f(x)$ that takes a bit as an input and a bit as an output. Note that there are only four possible functions. Some of them are constant (all outputs are the same), and some are balanced (equal number of 1s and 0s as outputs). How can we determine if $f(x)$ is balanced, using only one evaluation?

To do this quantumly, we need a unitary operation to evaluate $f(x)$. However, we can't evaluate it directly via $|x\rangle \to |f(x)\rangle$ since if $f(x)$ is constant, then it is non-unitary. Instead, we examine the map:

$$|x, 0\rangle \to |x, f(x)\rangle$$
$$|x, 1\rangle \to \left|x, \overline{f(x)}\right\rangle$$

Let's see if this works! Recall that there are only four possible functions $f(x)$. Let's look at them each:

(a) $f(0) = 0, f(1) = 0$

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |10\rangle$$
$$|11\rangle \to |11\rangle$$

Then:

$$\hat{U} = \hat{I} \otimes \hat{I}$$

(b) $f(0) = 0, f(1) = 1$

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

Then

$$\hat{U} = CNOT$$

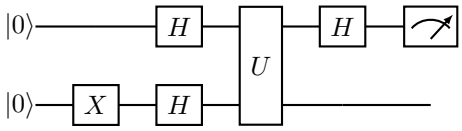
(c) $f(0) = 1, f(1) = 0$ We have:

$$\hat{U} = CNOT(\hat{I} \otimes \hat{X})$$

(d) $f(0) = 1, f(1) = 1$

$$\hat{U} = \hat{I} \otimes \hat{X}$$

To accomplish this, we will apply the following circuit:



The input to the unitary gate U is

$$|\Psi_{\text{in}}\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle).$$

Then after the unitary gate, we have:

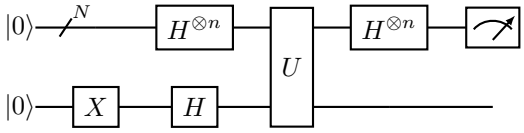
$$\begin{aligned} U_f |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= |x\rangle \left(\frac{|f(x)\rangle - \left|\overline{f(x)}\right\rangle}{\sqrt{2}}\right) \\ &= (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}\left((-1)^{f(x)} |0\rangle + (-1)^{f(x)} |1\rangle\right)(|0\rangle - |1\rangle) \end{aligned}$$

where $|x\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$. Then working through each of the four cases, we can see that this circuit can determine if the circuit is balanced or not.

After measurement, if qubit 1 is 0, then it's constant. Otherwise, it's balanced.

3.2 Deutsch-Josza Algorithm

Let us attempt to make the previous result more powerful. Suppose $x \in \{0, 1, \ldots, 2^N - 1\}$ is n-bits and $f(x) \in \ 0, 1$ is still a 1-bit function. Suppose that $f(x)$ is either constant or balanced. To do so, the circuit is remarkably similar!



Note that when you apply $\hat{H}^{\otimes n}$, you get a superposition of all possible n qubit states. The overall idea is that each individual bit will either contribute to a phase shift of $(-1)^x$. Similar to before, the state after the unitary is

$$|\Psi\rangle = \sum_{x=0}^{2^N-1} \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Note that:

$$\hat{H}^{\otimes n} |x\rangle = \frac{1}{2} \sum_{z=0}^{2^N-1} \frac{1}{\sqrt{2^n}} (-1)^{x \cdot z} |z\rangle,$$

where z_i refers to the ith bit of x. The result is the same as before. If f is constant, the measurement will be 0. Otherwise, it is 1.

3.3 Berstein-Vazirani

This is a restricted version of the previous problem. Suppose a, x are n-bit numbers with digits $a_{n-1}a_{n-2}\ldots a_1a_0$ and $x_{n-1}x_{n-2}\ldots x_1x_0$. Suppose we have the function:

$$f(x) = a \cdot x = a_0x_0 \oplus a_1x_1 \cdots \oplus a_{n-1}x_{n-1}$$

The question is: for how many different arguments x do we need to evaluate $f(x)$ in order to find a?

Classically, you need n evaluations, by doing $a_m = f(2^m)$. It happens that we can just apply the same circuit as before, and the measurements will give us a!

3.4 Quantum Fourier Transform

Recall that the standard fourier transform turns a function $x(t)$ from its time domain to its frequency domain, i.e.

$$\tilde{x}(\omega) = \int_{-\infty}^{\infty} x(t) e^{2\pi i \nu t} dt$$

There are only a few functions where this can be computed analytically. When working with real data, we would typically have a set $\{x_0, x_1, \ldots, x_{N-1}\}$ where the data points are taken from a set of equally spaced time intervals $x(T + \ell\Delta t)$. The **discrete fourier transform** then gives a sequence

$$\{\tilde{x}_0, \tilde{x}_1, \ldots, \tilde{x}_{N-1}\}$$

where

$$\tilde{x}_k = \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} \exp\left(2\pi i \frac{k\ell}{N}\right) x_\ell.$$

This is quite a resource heavy computation. There is a faster method to do this calculation, known as the Fast Fourier Transform (FFT), which only works when $N = 2^n$ is a power of 2.

Let us now examine the Quantum Fourier Transform. Let $|\ell_1\rangle$ be the most significant and $|\ell_n\rangle$ be the least significant bit.

$$|\ell_1\rangle \text{——}$$

$$|\ell_2\rangle \text{——}$$

$$\vdots \quad \vdots$$

$$|\ell_n\rangle \text{——}$$

Let

$$|\ell\rangle = |\ell_1\rangle \otimes |\ell_2\rangle \otimes \cdots \otimes |\ell_n\rangle\,, \tag{3.1}$$

such that $\ell = (\ell_1 \ell_2 \ldots \ell_n)_2$. Then the quantum fourier transform is given by the unitary operator $\hat{U}_{\mathsf{QFT}}$ defined by

$$\hat{U}_{\mathsf{QFT}} |\ell\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2\pi i \cdot \frac{k\ell}{2^n}\right) |k.\rangle$$

In general, an n-qubit state is a linear combination of the basis $|\ell\rangle$ states, i.e.

$$\hat{U}_{\mathsf{QFT}} |\Psi\rangle = \hat{U}_{\mathsf{QFT}} \sum_\ell c_\ell |\ell\rangle \tag{3.2}$$

$$= \sum_{\ell k} c_\ell \exp\left(2\pi i \frac{k\ell}{2^n}\right) |k\rangle \tag{3.3}$$

$$= \sum_k \tilde{c}_k |k\rangle\,, \tag{3.4}$$

where $\tilde{c}_k$ is the DFT of $\{c_k\}$.

We will now attempt this for the $n = 2$ case. Then:

$$\hat{U}_{\mathsf{QFT}} |\ell\rangle = \frac{1}{2}\left\{|00\rangle + \exp\left(2\pi i \frac{\ell}{4}\right)|01\rangle + \exp\left(2\pi i \frac{2\ell}{4}\right)|10\rangle + \exp\left(2\pi i \frac{3\ell}{4}\right)|11\rangle\right\}. \tag{3.5}$$

The concurrence is

$$C = 2|\alpha\delta - \beta\gamma| = 0, \tag{3.6}$$

so these are separable. Therefore, we can rewrite this as

$$\hat{U}_{\mathsf{QFT}} |\ell\rangle = \frac{1}{2}\left[|0\rangle\left\{|0\rangle + \exp\left(2\pi i \frac{\ell}{4}\right)|1\rangle\right\} + |1\rangle\left\{|0\rangle \exp\left(2\pi i \frac{2\ell}{4}\right) + \exp\left(2\pi i \frac{3\ell}{4}\right)|1\rangle\right\}\right] \tag{3.7}$$

$$= \frac{1}{\sqrt{2}}\left\{|0\rangle + |1\rangle \exp\left(2\pi i \frac{2\ell}{4}\right)\right\} \otimes \frac{1}{\sqrt{2}}\left\{|0\rangle + |1\rangle \exp\left(2\pi i \frac{\ell}{4}\right)\right\}. \tag{3.8}$$

Note that

$$\frac{2\ell}{4} = \frac{1}{2}(2\ell_1 + \ell_2) = \ell_1 + \frac{\ell_2}{2}$$
$$\frac{\ell}{4} = \frac{\ell_1}{2} + \frac{\ell_2}{4}.$$

We can ignore the ℓ_1 term since if $\ell_1 = 0$ it does nothing and if $\ell_1 = 1$ then $e^{2\pi i} = 1$. Therefore:

$$\hat{U}_{\mathsf{QFT}} |\ell\rangle = \frac{1}{\sqrt{2}} \left\{ |0\rangle + |1\rangle \exp\left(2\pi i \frac{\ell_2}{2}\right) \right\} \otimes \frac{1}{\sqrt{2}} \left\{ |0\rangle + |1\rangle \exp\left(2\pi i \left(\frac{\ell_1}{2} + \frac{\ell_2}{4}\right)\right) \right\}. \tag{3.9}$$

Recall that

$$\hat{H} |\ell_k\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{\ell_k} |1\rangle \right). \tag{3.10}$$

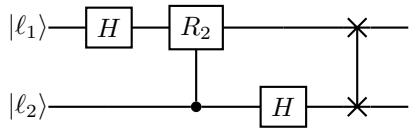
However, $(-1)^{\ell_k} = \exp\left(2\pi i \frac{\ell_k}{2}\right)$, which looks suspiciously like what we had in our Quantum Fourier Transform. In particular,

$$\hat{H} \otimes \hat{H} |\ell_1 \ell_2\rangle = \frac{1}{\sqrt{2}} \left\{ |0\rangle + |1\rangle \exp\left(2\pi i \frac{\ell_1}{2}\right) \right\} \otimes \frac{1}{\sqrt{2}} \left\{ |0\rangle + |1\rangle \exp\left(2\pi i \frac{\ell_2}{2}\right) \right\}. \tag{3.11}$$

It seems like ℓ_1 and ℓ_2 is swapped, so we have to perform a SWAP operation. To get the second qubit to the right location, we can perform a rotation that is controlled by the other qubit. In particular,

$$\hat{R}_0 = \hat{I}$$
$$\hat{R}_1 = \hat{Z}$$
$$\hat{R}_2 = \sqrt{\hat{Z}}$$
$$\hat{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$$

Therefore, the circuit looks like:



We will now try to generalize this result. We can write the $\frac{k}{2^n}$ part as:

$$\frac{k}{2^n} = \sum_{m=1}^{n} k_m \frac{2^{n-m}}{2^n} = \sum_{m=1}^{n} \frac{k_m}{2^m}. \tag{3.12}$$

This allows us to take the sum over the individual digits of k. That is,

$$\hat{U}_{\mathsf{QFT}} |\ell\rangle = \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{m=1}^{n} \exp\left(\exp 2\pi i \frac{\ell k_m}{2^m}\right) |k_m\rangle. \tag{3.13}$$

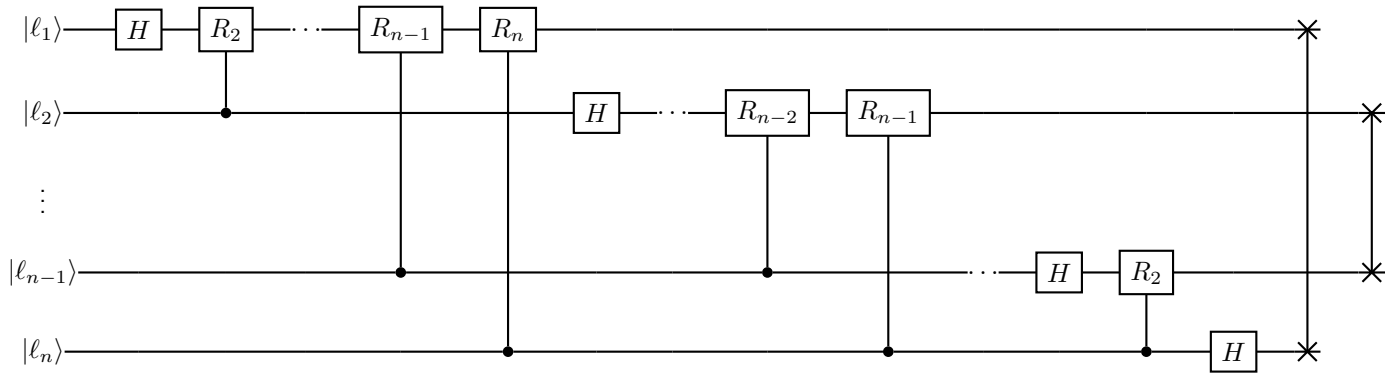
Recall that the tensor product is distributive, i.e. $(a+b) \otimes (c+d) = a \otimes c + a \otimes d + b \otimes c + b \otimes d$. Therefore, we can write the above as a product of a sum:

$$= \bigotimes_{m=1}^{n} \frac{1}{\sqrt{2}} \left\{ |0\rangle_m + \exp\left(2\pi i \frac{\ell}{2^m}\right) |1\rangle_m \right\}. \tag{3.14}$$

Recall that we can write $\ell = \ell_1 2^{n-1} + \cdots + \ell_{n-2} 2 + \ell_n$. Then:

$$\frac{\ell}{2^m} = \underbrace{\ell_1 2^{n-(m+1)} + \ell_2 2^{n-(m+2)} + \cdots + \ell_{m-n}}_{} + \frac{\ell_{m-n+1}}{2} + \cdots + \frac{\ell_1}{2^m}. \tag{3.15}$$

We can ignore the numbers in the underbrace since they are integers, so their exponent will just be 1. To process $\frac{\ell_{m-n+1}}{2}$, we can use a Hadamard and a swap and for the other terms, we can use controlled phases. The circuit looks like the following:



Complexity

Note that a single controlled R_k gate is consisted of 2 CNOTs and 3 single qubit gates. There are $\lfloor n/2 \rfloor$ swaps, which canb e implemented with 3 CNOTS each. We apply R_k $(n-1)+(n-2)+\cdots+1 = \dfrac{n(n-1)}{2}$ times. Therefore, we apply $(3n-2)n/2$ single qubit operations and $(2n+1)n/2$ CNOTS.

As a result, the QFT is polynomial in n. For reference, the DFT is $\mathcal{O}(2^{2n})$ and $)(n2^n)$.

This is one of the first real applications that show the power of quantum computing. While in theory QFT is much more efficient, it is very difficult to implement this in practice.

Modification

To make it more applicable, we can use a modification of the QFT. For example, we don't need to bother with the SWAP gates. We'll just do it after measurement! Using the identities:

- A controlled R_k gate can be flipped and still give the same thing.
- Measuring the top branch after a controlled operation is the same as measuring it before the operation (Griffiths-Niu Theorem)

We can now redraw the diagram: