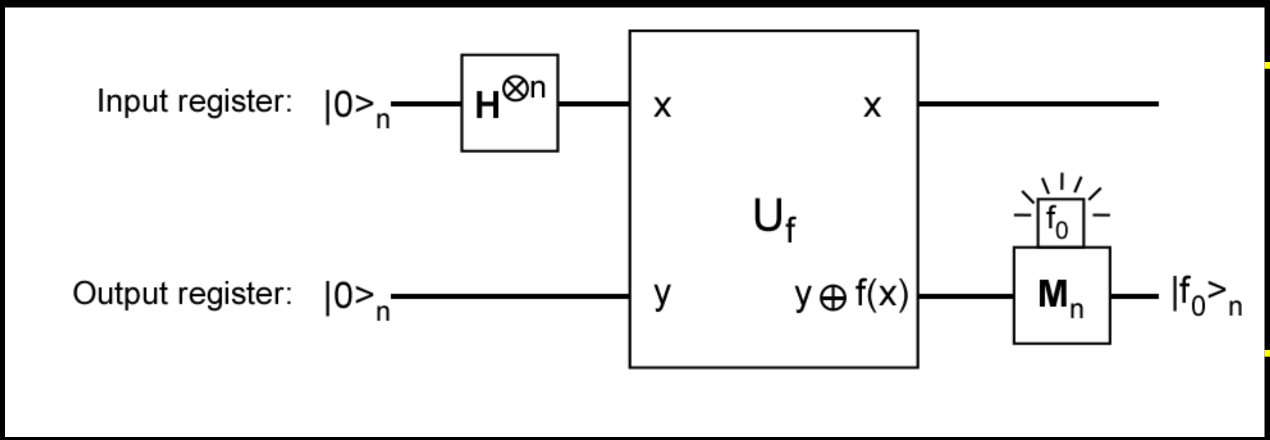
B. Quantum Fourier Transforms and Period Finding

Using an “oracle query” approach to find the period of a function

$$f(x+r) = f(x) = b^x \text{ (mod N)}$$

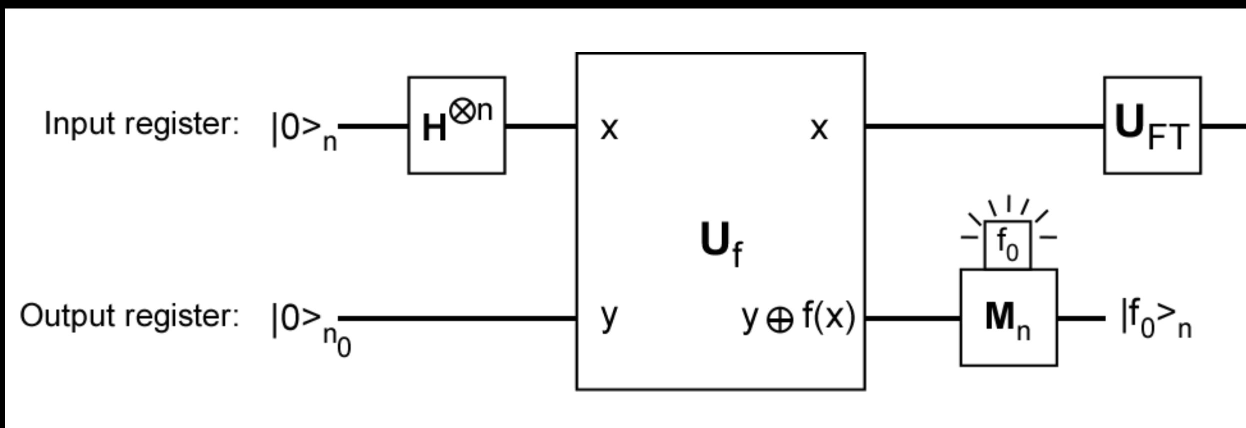
$$|\psi_3\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f_0\rangle_{n_0}$$



After measurement of the output register the input register is a state which is periodic in *r*.

Using the Quantum Fourier Transform on the input register:

$$|\psi_4\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{2\pi i(x_0+kr)y/2^n} |y\rangle_n |f_0\rangle_{n_0}$$



Goal #1: Show how to *efficiently* evaluate the QFT!

1. Review: The Quantum Fourier Transform (QFT)

The n-Qbit Quantum Fourier Transform is a unitary basis transformation defined by its action on the basis states |x>

$$\mathbf{U}_{FT}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{0\le y<2^n} \left(e^{2\pi i/2^n}\right)^{xy} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{0\le y<2^n} \omega^{xy}\, |y\rangle$$

where *x* and *y* are n-bit integers, and *xy* represents ordinary integer multiplication. Since the operation is linear, it acts on a general superposition of states

$$|\psi\rangle = \sum_{0\le x<2^n} \gamma(x)|x\rangle$$

in exactly the same way to give

$$\begin{aligned}
\mathbf{U}_{FT}|\psi\rangle &= \sum_{0\le x<2^n} \gamma(x)\mathbf{U}_{FT}|x\rangle \\
&= \sum_{0\le x<2^n} \gamma(x)\frac{1}{\sqrt{2^n}} \sum_{0\le y<2^n} \omega^{xy}\, |y\rangle \\
&= \sum_{0\le y<2^n} \frac{1}{\sqrt{2^n}} \sum_{0\le x<2^n} \gamma(x)\, \omega^{xy}|y\rangle
\end{aligned}$$

This is a double sum with $(2^n)^2$ multiplications – wicked inefficient!

2. Efficient implementation of the QFT

Given the definition of the QFT

$$\mathbf{U}_{FT}|x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{0\le y<2^n} \left(e^{2\pi i/2^n}\right)^{xy} |y\rangle_n$$

we can think about how to break this up into operators on each Qbit by writing the states explicitly as

$$|x\rangle_n = |x_{n-1}\rangle|x_{n-2}\rangle \ldots |x_1\rangle|x_0\rangle$$
$$|y\rangle_n = |y_{n-1}\rangle|y_{n-2}\rangle \ldots |y_1\rangle|y_0\rangle$$

and thinking about the sum as a sequence nested sums over each binary digit.

$$\mathbf{U}_{FT}|x\rangle_n = \frac{1}{\sqrt{2}} \sum_{0\le y_{n-1}<2} \frac{1}{\sqrt{2}} \sum_{0\le y_{n-2}<2} \cdots \frac{1}{\sqrt{2}} \sum_{0\le y_1<2} \frac{1}{\sqrt{2}} \sum_{0\le y_0<2} \left(e^{2\pi i/2^n}\right)^{xy} |y\rangle_n$$

and write the product out as a function of those binary digits, too.

$$xy = \left(2^{n-1}x_{n-1} + 2^{n-2}x_{n-2} + \ldots + 2x_1 + x_0\right)$$
$$\times \left(2^{n-1}y_{n-1} + 2^{n-2}y_{n-2} + \ldots + 2y_1 + y_0\right)$$

Example 1:

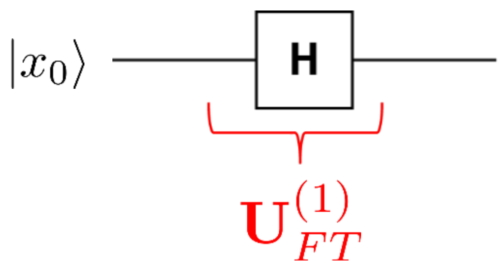
$e^{i\pi} = -1$

What is the QFT for a 1-Qbit state

$$\mathbf{U}_{FT}^{(1)}|x_0\rangle = \frac{1}{\sqrt{2}} \sum_{0 \le y_0 < 2} \left(e^{2\pi i/2^1}\right)^{xy} |y_0\rangle$$

Where $xy = x_0 y_0$

$$\mathbf{U}_{FT}^{(1)}|x_0\rangle = \frac{1}{\sqrt{2}} \sum_{0 \le y_0 < 2} e^{2\pi i(\frac{x_0}{2})y_0}|y_0\rangle = \frac{1}{\sqrt{2}} \sum_{0 \le y_0 < 2} (-1)^{x_0 y_0} |y_0\rangle = \mathbf{H}|x_0\rangle$$



$$\mathbf{H}|x_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right)$$

Since the operator is linear it acts as the QFT on superpositions, too!

Example 2:

What is the QFT for a 2-Qbit state

$$\mathbf{U}_{FT}|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\le y_1<2}\frac{1}{\sqrt{2}}\sum_{0\le y_0<2}\left(e^{2\pi i/2^2}\right)^{xy}|y_1\rangle|y_0\rangle$$

For the 2-Qbit states

$$xy = (2x_1 + x_0)\,2y_1 + (2x_1 + x_0)\,y_0$$

$$\frac{2\pi i xy}{2^2} = 2\pi i\left(x_1 + \frac{x_0}{2}\right)y_1 + 2\pi i\left(\frac{x_1}{2} + \frac{x_0}{4}\right)y_0$$

$$e^{i2\pi} = +1 \qquad\qquad e^{i\pi} = -1$$

$$\mathbf{U}_{FT}|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\le y_1<2}\left(e^{2\pi i}\right)^{x_1 y_1}\left(e^{i\pi}\right)^{x_0 y_1}|y_1\rangle$$

$$\times\frac{1}{\sqrt{2}}\sum_{0\le y_0<2}\left(e^{i\pi}\right)^{y_0 x_0}\left(e^{i\pi/2}\right)^{y_0 x_1}|y_0\rangle$$

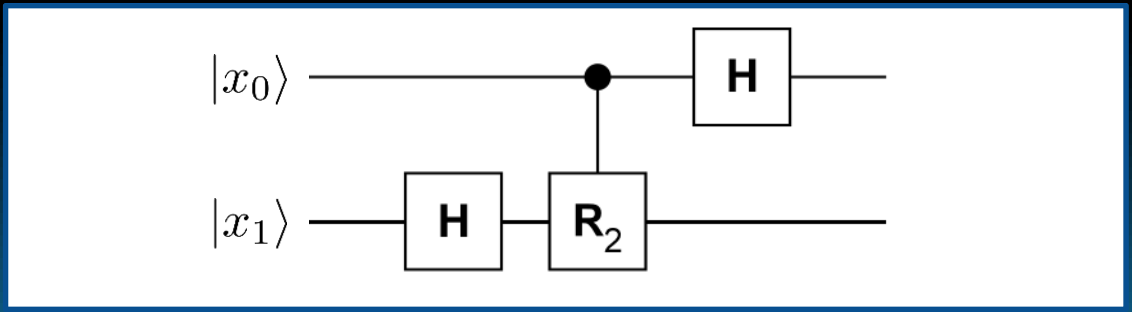
$$e^{i\pi} = -1 \qquad\qquad e^{i\pi/2} = i$$

$$\mathbf{U}_{FT}|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\le y_1<2} e^{2\pi i(\frac{x_0}{2})y_1}|y_1\rangle \frac{1}{\sqrt{2}}\sum_{0\le y_0<2} e^{2\pi i(\frac{x_1}{2}+\frac{x_0}{4})y_0}|y_0\rangle$$
$$= \frac{1}{\sqrt{2}}\sum_{0\le y_1<2} (-1)^{x_0 y_1}\,|y_1\rangle \frac{1}{\sqrt{2}}\sum_{0\le y_0<2} (-1)^{y_0 x_1}\left(e^{i\pi/2}\right)^{x_0 y_0}|y_0\rangle$$

Looks like a Hadamard of $|x_0\rangle$ but in the $|y_1\rangle$ Qbit

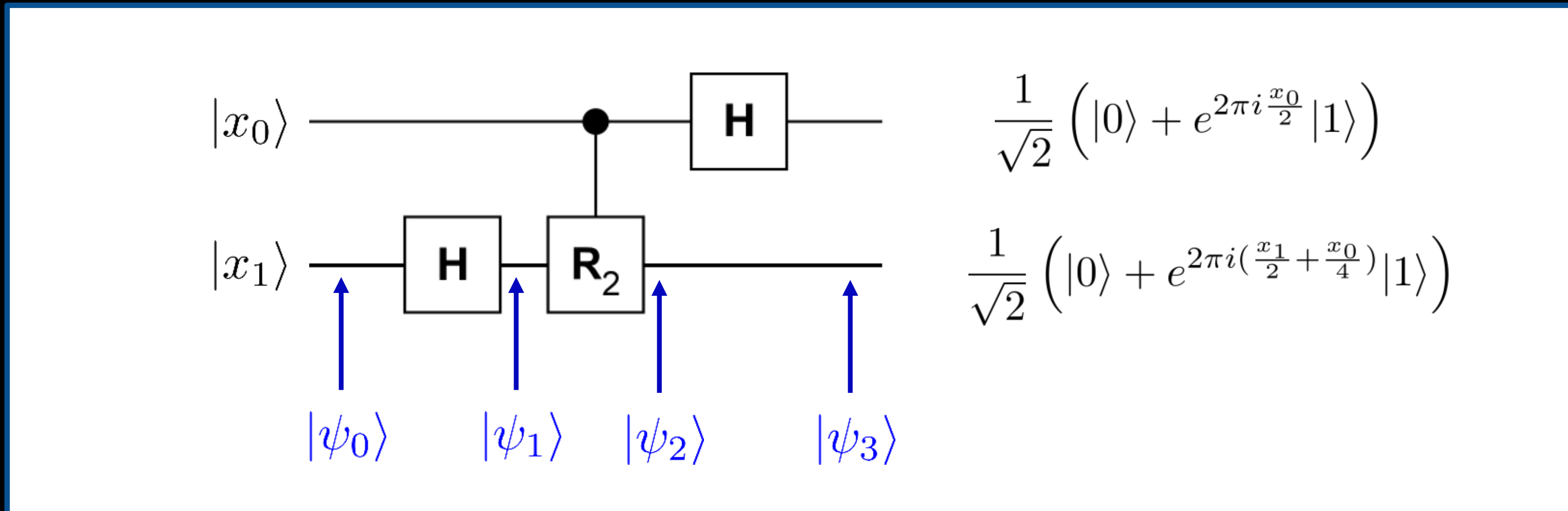
Looks like a Hadamard of $|x_1\rangle$ but in the $|y_0\rangle$ Qbit **and** with an additional $\pi/2$ phase shift controlled by $|x_0\rangle$.

Model implementation:



$$\mathbf{R}_d = \tilde{\mathbf{n}} + e^{2\pi i/2^d}\mathbf{n} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^d} \end{pmatrix} \qquad (\mathbf{cR}_d)_{01}\,|x_1\rangle|x_0\rangle = \left(e^{2\pi i/2^d}\right)^{x_0 x_1}|x_1\rangle|x_0\rangle$$

Let’s follow the state through the circuit:



$$|\psi_0\rangle = |x_1\rangle|x_0\rangle$$

$$|\psi_1\rangle = \mathbf{H}_1|\psi_0\rangle = \frac{1}{\sqrt{2}} \sum_{0\le z_1<2} \left(e^{i\pi}\right)^{x_1 z_1} |z_1\rangle|x_0\rangle$$

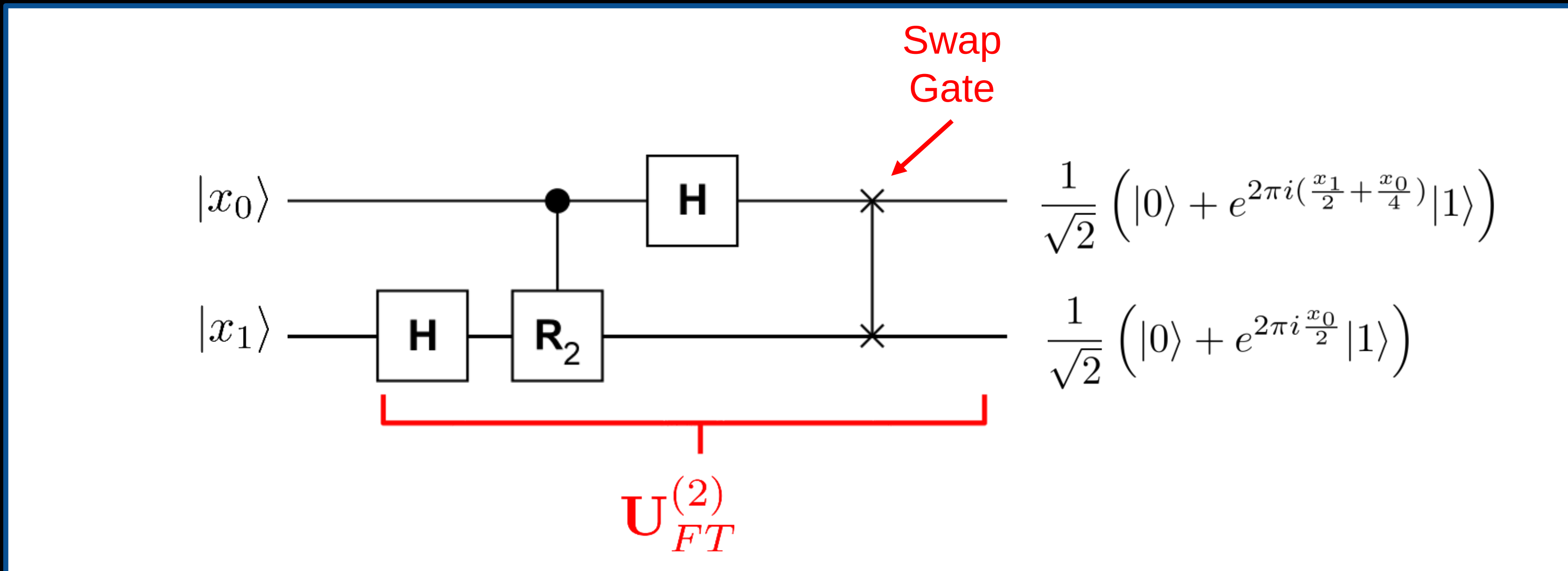
$$|\psi_2\rangle = (\mathbf{cR}_2)_{01}\,|\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{0\le z_1<2} \left(e^{i\pi}\right)^{x_1 z_1} \left(e^{i\pi/2}\right)^{x_0 z_1} |z_1\rangle|x_0\rangle$$

$$|\psi_3\rangle = \mathbf{H}_0|\psi_2\rangle = \frac{1}{\sqrt{2}} \sum_{0\le z_1<2} \left(e^{i\pi}\right)^{x_1 z_1} \left(e^{i\pi/2}\right)^{x_0 z_1} |z_1\rangle \frac{1}{\sqrt{2}} \sum_{0\le z_0<2} \left(e^{i\pi}\right)^{x_0 z_0} |z_0\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{0\le z_1<2} e^{2\pi i (\frac{x_1}{2}+\frac{x_0}{4}) z_1}|z_1\rangle \frac{1}{\sqrt{2}} \sum_{0\le z_0<2} e^{2\pi i (\frac{x_0}{2}) z_0}|z_0\rangle$$

Reminder:

$$\mathbf{U}_{FT}|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\leq y_1<2} e^{2\pi i y_1\left(\frac{x_0}{2}\right)}|y_1\rangle\frac{1}{\sqrt{2}}\sum_{0\leq y_0<2} e^{2\pi i y_0\left(\frac{x_1}{2}+\frac{x_0}{4}\right)}|y_0\rangle$$



$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\sum_{0\leq z_1<2} e^{2\pi i z_1\left(\frac{x_1}{2}+\frac{x_0}{4}\right)}|z_1\rangle\frac{1}{\sqrt{2}}\sum_{0\leq z_0<2} e^{2\pi i z_0\left(\frac{x_0}{2}\right)}|z_0\rangle$$

$$|\psi_4\rangle = \mathbf{S}|\psi_3\rangle = \frac{1}{\sqrt{2}}\sum_{0\leq z_1<2} e^{2\pi i z_1\left(\frac{x_0}{2}\right)}|z_1\rangle\frac{1}{\sqrt{2}}\sum_{0\leq z_0<2} e^{2\pi i z_0\left(\frac{x_1}{2}+\frac{x_0}{4}\right)}|z_0\rangle$$

Example 3:

What is the QFT for a 3-Qbit state

$$\mathbf{U}_{FT}|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\le y_2<2}\frac{1}{\sqrt{2}}\sum_{0\le y_1<2}\frac{1}{\sqrt{2}}\sum_{0\le y_0<2}\left(e^{2\pi i/2^3}\right)^{xy}|y_2\rangle|y_1\rangle|y_0\rangle$$

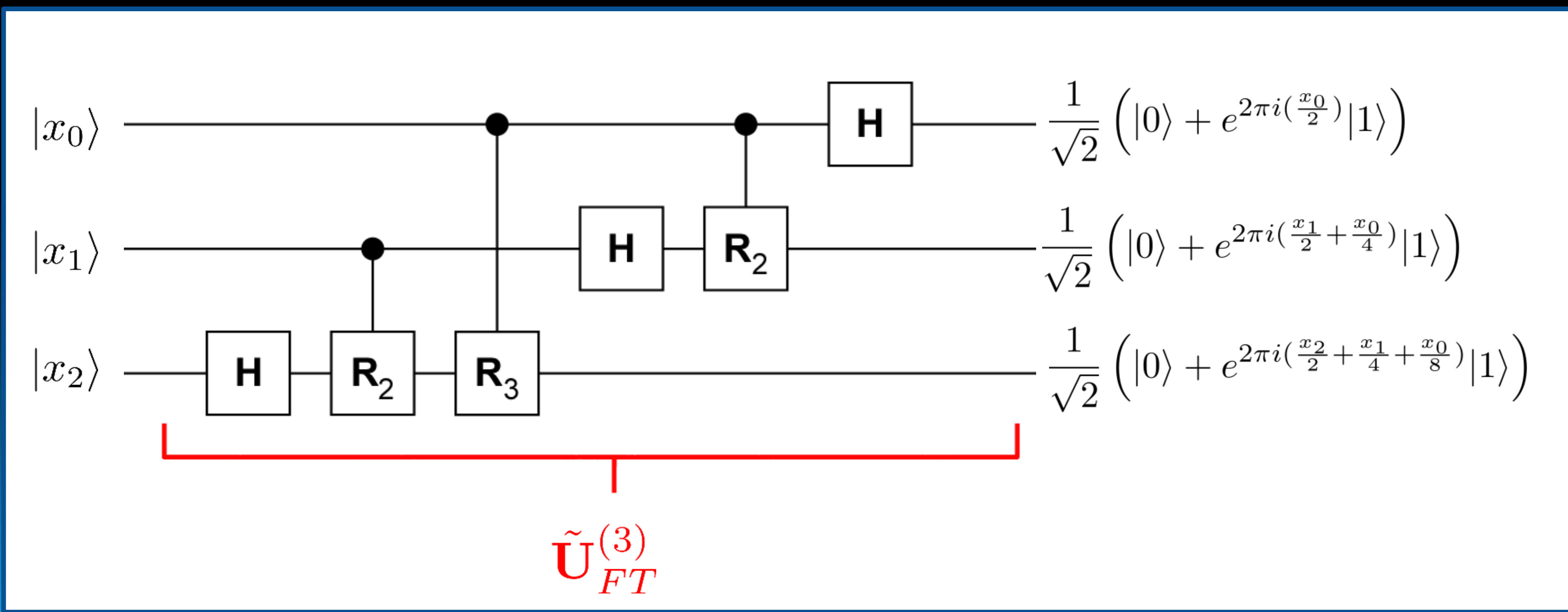
For the 3-Qbit states:

$$xy = \left(2^2x_2 + 2x_1 + x_0\right)\left(2^2y_2 + 2y_1 + y_0\right)$$

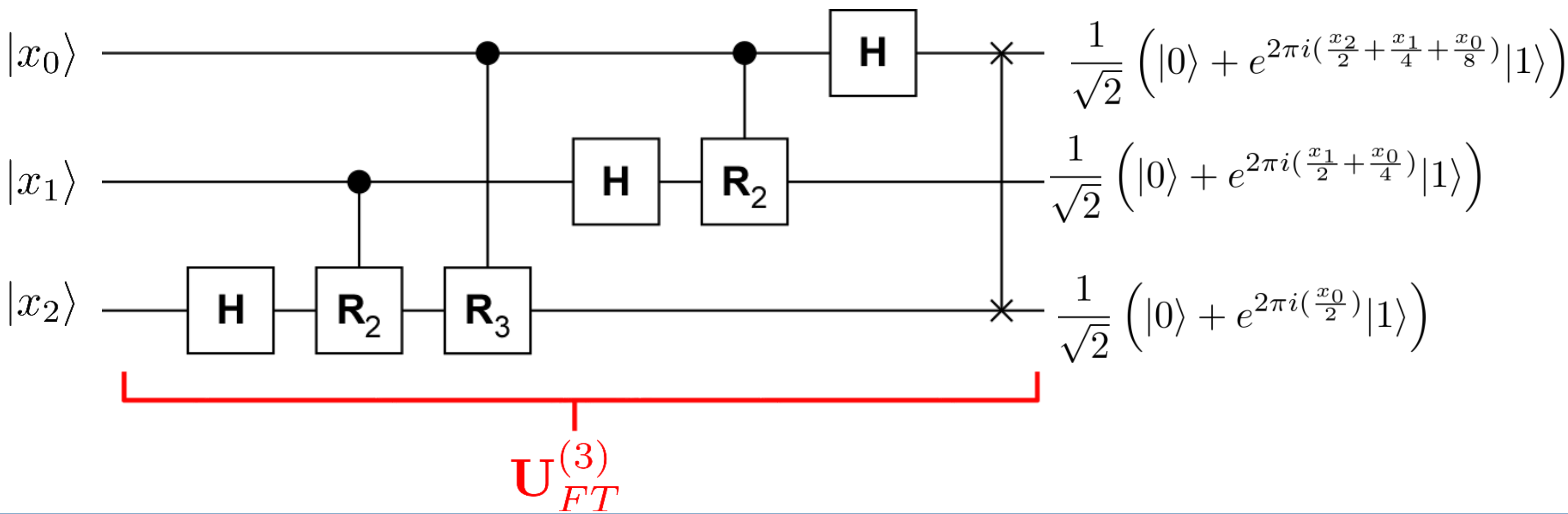
$$\begin{aligned}\frac{2\pi ixy}{2^3} &= 2\pi i\left(2x_2 + x_1 + \frac{x_0}{2}\right)y_2\\ &+ 2\pi i\left(x_2 + \frac{x_1}{2} + \frac{x_0}{4}\right)y_1\\ &+ 2\pi i\left(\frac{x_2}{2} + \frac{x_1}{4} + \frac{x_0}{8}\right)y_0\end{aligned}$$

$$e^{\frac{2\pi ixy}{2^3}} = e^{2\pi i\left(\frac{x_0}{2}\right)y_2} \cdot e^{2\pi i\left(\frac{x_1}{2}+\frac{x_0}{4}\right)y_1} e^{2\pi i\left(\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)y_0}$$

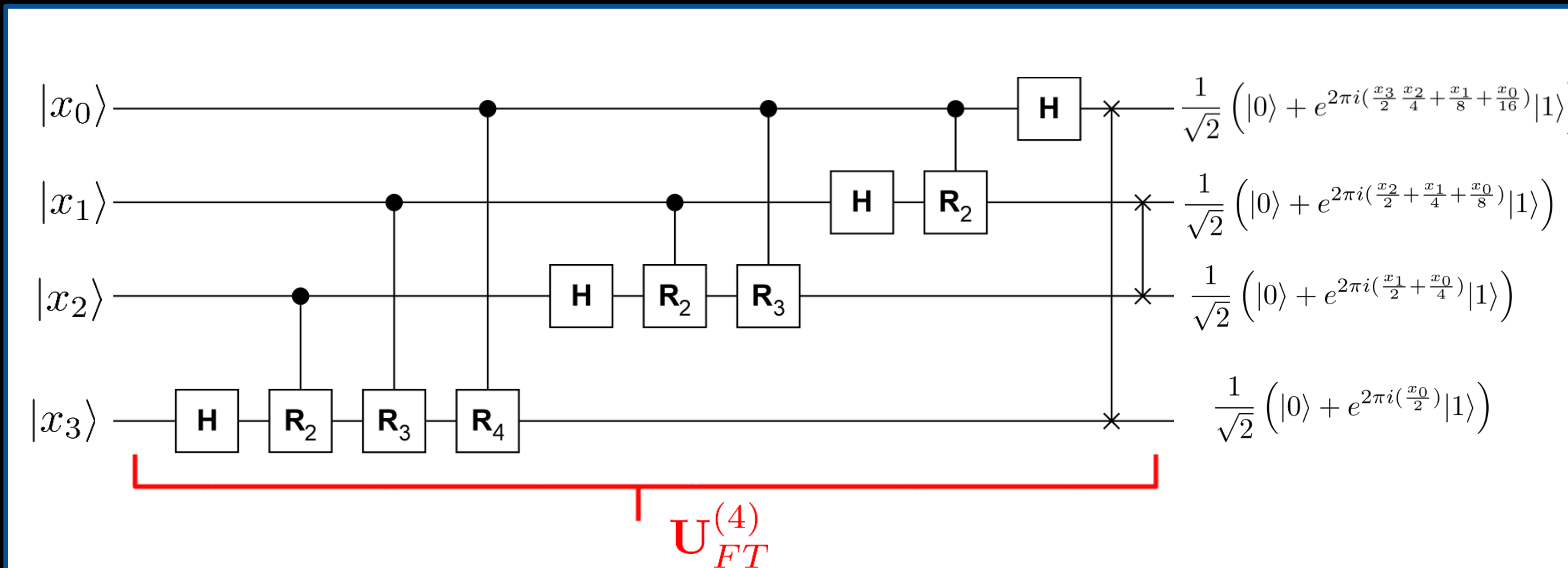
$$
\begin{aligned}
\mathbf{U}_{FT}^{(3)}|x_2\rangle|x_1\rangle|x_0\rangle = & \frac{1}{\sqrt{2}} \sum_{0 \le y_2 < 2} e^{2\pi i \left(\frac{x_0}{2}\right) y_2} |y_2\rangle \\
& \times \frac{1}{\sqrt{2}} \sum_{0 \le y_1 < 2} e^{2\pi i \left(\frac{x_1}{2} + \frac{x_0}{4}\right) y_1} |y_1\rangle \\
& \times \frac{1}{\sqrt{2}} \sum_{0 \le y_0 < 2} e^{2\pi i \left(\frac{x_2}{2} + \frac{x_1}{4} + \frac{x_0}{8}\right) y_0} |y_0\rangle
\end{aligned}
$$



$$
\begin{aligned}
\mathbf{U}_{FT}^{(3)}|x_2\rangle|x_1\rangle|x_0\rangle = {} & \frac{1}{\sqrt{2}} \sum_{0\le y_2<2} e^{2\pi i\left(\frac{x_0}{2}\right)y_2}|y_2\rangle \\
& \times \frac{1}{\sqrt{2}} \sum_{0\le y_1<2} e^{2\pi i\left(\frac{x_1}{2}+\frac{x_0}{4}\right)y_1}|y_1\rangle \\
& \times \frac{1}{\sqrt{2}} \sum_{0\le y_0<2} e^{2\pi i\left(\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8}\right)y_0}|y_0\rangle
\end{aligned}
$$



A 4-Qbit QFT circuit:



There's a clear pattern, and each additional Qbit k will require k+1 gates.

The total gate count (not including the [n/2] swap gates) is therefore:

$$G = \sum_{k=0}^{n}(k+1) = \frac{n(n+1)}{2} = O(n^2)$$

Explicit iteration to n Qbits:

$$\mathbf{U}_{FT}^{(n)}|x_{n-1}\rangle|x_{n-2}\rangle\ldots|x_1\rangle|x_0\rangle = \frac{1}{\sqrt{2}}\sum_{0\le y_{n-1}<2} e^{2\pi i\left(\frac{x_0}{2}\right)y_{n-1}}|y_{n-1}\rangle$$
$$\times\frac{1}{\sqrt{2}}\sum_{0\le y_{n-2}<2} e^{2\pi i\left(\frac{x_1}{2}+\frac{x_0}{4}\right)y_{n-2}}|y_{n-2}\rangle$$
$$\vdots$$
$$\times\frac{1}{\sqrt{2}}\sum_{0\le y_1<2} e^{2\pi i\left(\frac{x_{n-2}}{2}+\ldots+\frac{x_1}{2^{n-2}}+\frac{x_0}{2^{n-1}}\right)y_0}|y_1\rangle$$
$$\times\frac{1}{\sqrt{2}}\sum_{0\le y_0<2} e^{2\pi i\left(\frac{x_{n-1}}{2}+\frac{x_{n-2}}{4}+\ldots+\frac{x_1}{2^{n-1}}+\frac{x_0}{2^{n}}\right)y_0}|y_0\rangle$$