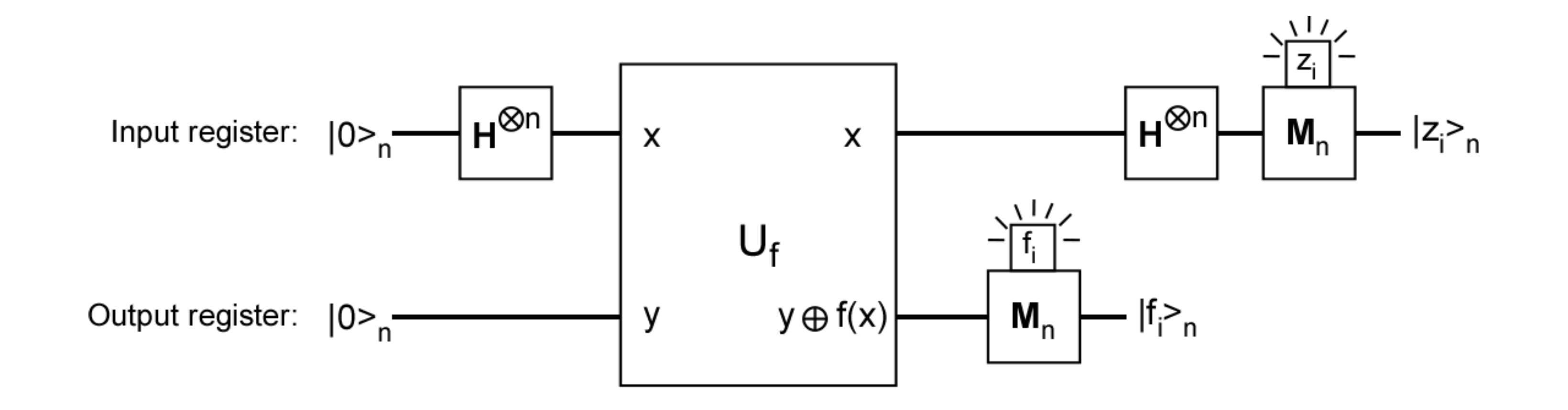
Shor’s Algorithm and the QFT

Background: In 1993 Dan Simon found a quantum algorithm that can efficiently find a hidden “period” *a* for a function defined by

$$f(x \oplus a) = f(x)$$



Shortly afterwards, in 1994, Peter Shor used a very similar approach to finding the “hidden” period of a function

$$f(x+k) = f(x) = b^x \ (\mathrm{mod\ N})$$

Goal: Explain the approach needed to solve the problem!

A. Factoring a number quantum mechanically

Shor realized that there's an equivalence between factoring a number *N* and finding the period (order) *r* of the function.

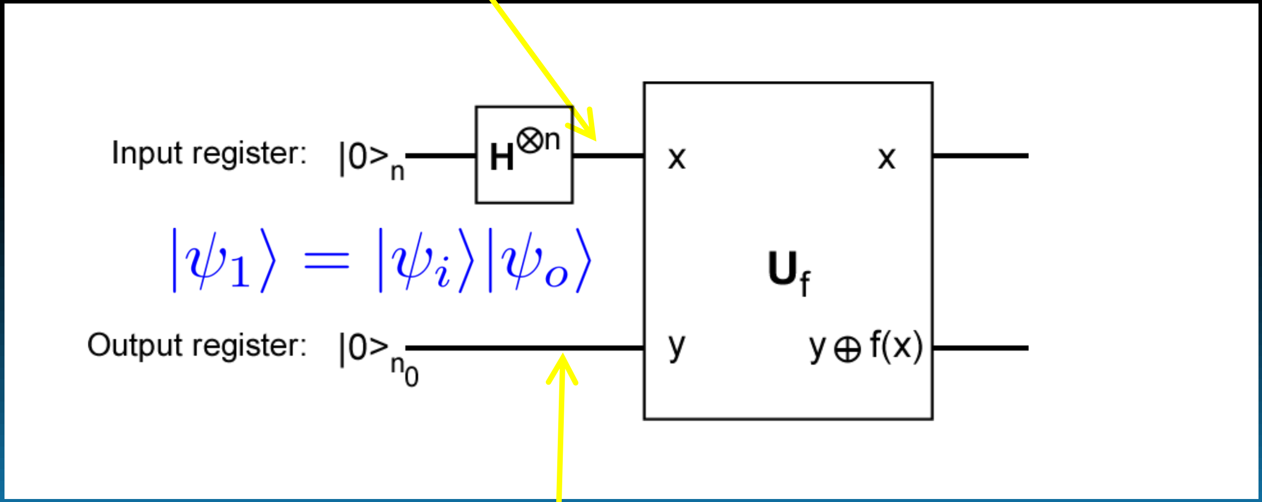
$$f(x) = b^x \pmod{\mathrm{N}}$$

1. Quantum Parallelism

Shor's algorithm starts the same way as Simon's – except in this case the "oracle" computes a known function.

$$|\psi_i\rangle_n = \mathbf{H}^{\otimes n}|0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} |x\rangle_n$$

n is the number of bits needed to represent the number of *x* values you need to evaluate $n = 2n_0$



$$|\psi_1\rangle = |\psi_i\rangle|\psi_o\rangle$$

n_0 is the number of bits needed to represent *N*

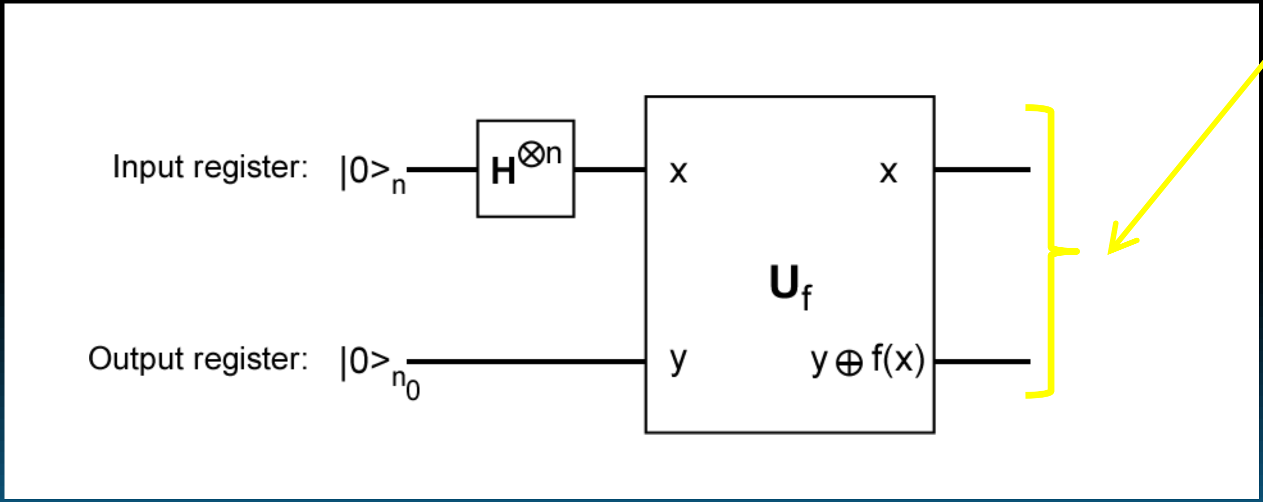
$$|\psi_o\rangle_{n_0} = |0\rangle_{n_0}$$

2. Output of the "oracle"

The output of the (linear) oracle is a state that is entangled between the input and output registers.

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} \mathbf{U}_f |x\rangle_n |0\rangle_{n_0}$$

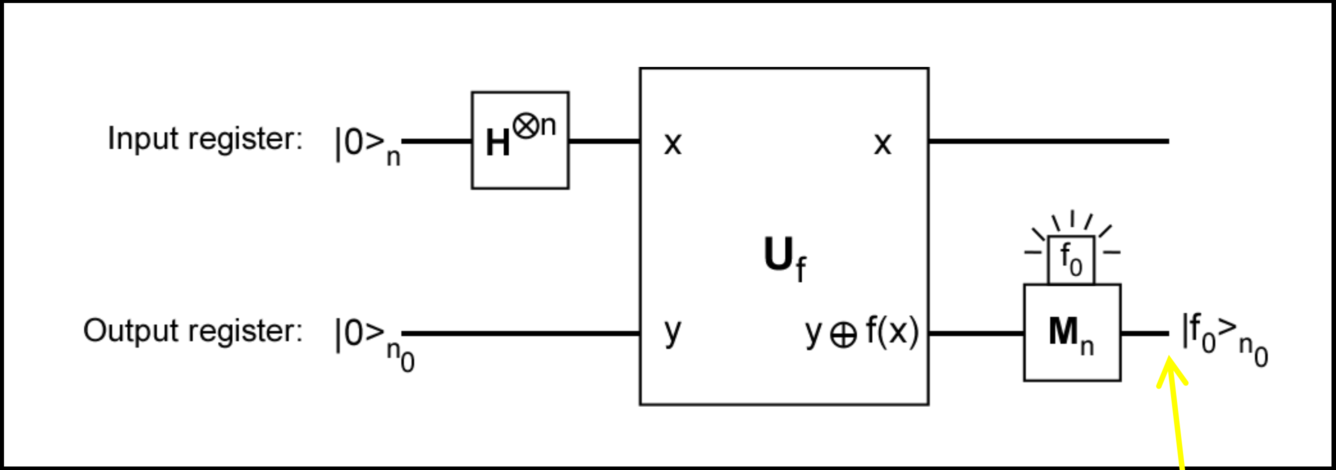
$$= \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} |x\rangle_n |f(x)\rangle_{n_0}$$



All possible x values and their associated f(x) values are equally weighted.

3. Manipulating the output to get an answer!

The output register is *measured*, and gives specific value of f(x), which is drawn with equal probability from all possible values of f(x).



$$f_0 = b^{x_0} \text{ (mod N)}$$

$$|\psi_o\rangle = |f_0\rangle_{n_0}$$

$$|f_0\rangle_{n_0} = |f(x_0)\rangle_{n_0} = |f(x_0 + kr)\rangle_{n_0}$$

For any integer *k* and the period *r*

This is a partial measurement – which leaves the system in a (normalized) state which is conditioned on the output register being in the state $|f_0\rangle$.

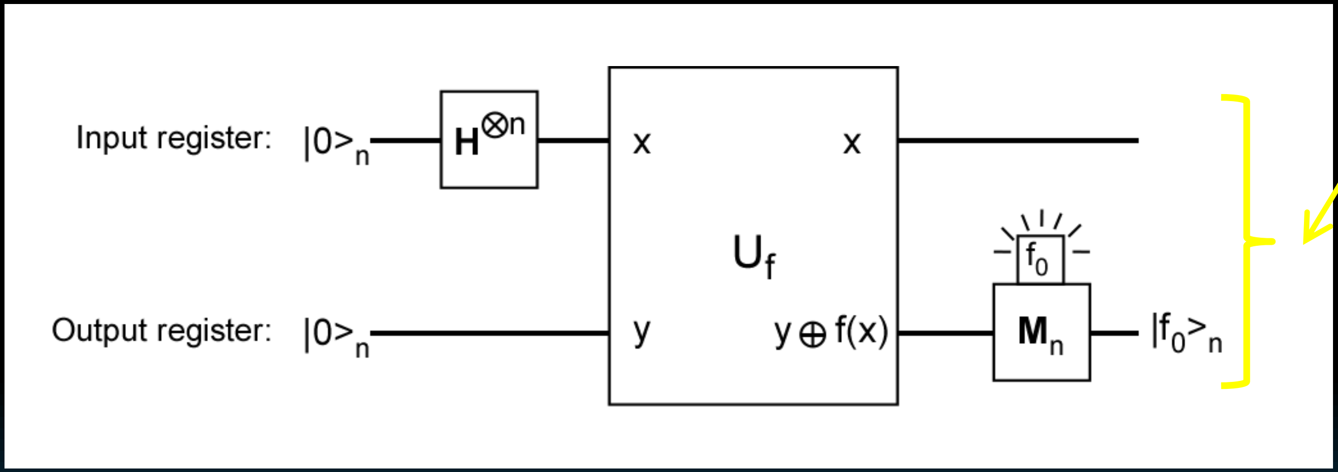
There are many (m) possible values of the input register that are consistent with a specific value of the output register:

m is the number of states that have k values that satisfy

$$x_0 + kr \leq 2^n$$

$$m = \left\lceil \frac{2^n}{r} \right\rceil$$

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

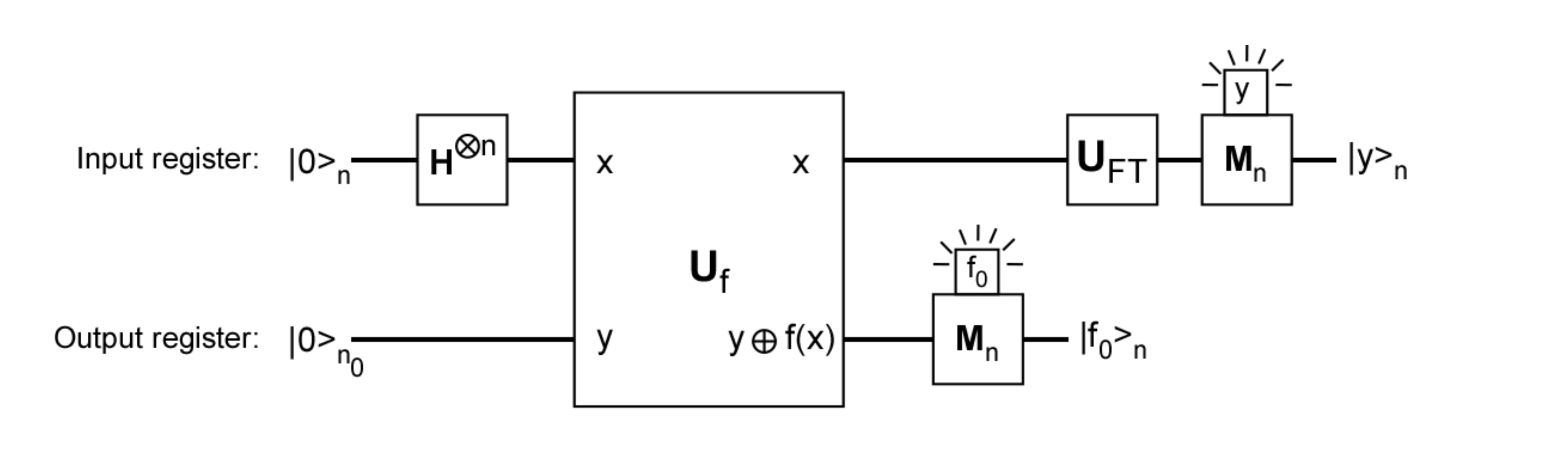


If we could just *clone* the output state, we could measure the state multiple times and determine a set of values separated by multiples of r (and therefore r), but the no-cloning theorem says we're out of luck with that approach!

4. Manipulating the output to get an answer, Part 2.

We need to do something more clever than the n-Qbit Hadamard to figure out the periodicity of the state.

That thing is the "Quantum Fourier Transform," which preferentially populates states $|y\rangle_n$ that come at integer factors of the period *r* independent of x_0.



The Fourier Transform and
the Quantum Fourier Transform
are the subjects of the next
ScreenCast