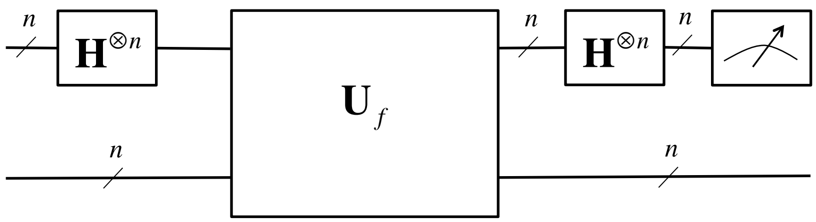
Simon's Periodicity Algorithm



PURPOSE: Detect Patterns within a Function

Simon's Periodicity Algorithm Problem Overview

- Consider an Unknown Function of the Form:

$$f : \{0,1\}^n \rightarrow \{0,1\}^n$$

- Function is "Hidden" in a Black Box
- Known that there exists a string:

$$\mathbf{c} = c_0 c_1 c_2 \ldots c_{n-1}$$

- Such that for all strings: $\mathbf{x},\mathbf{y} \in \{0,1\}^n$

$f(\mathbf{x}) = f(\mathbf{y})$ if and only if $\mathbf{x} = \mathbf{y} \oplus \mathbf{c}$

Simon's Periodicity Algorithm Problem Overview

- XOR operation is performed bitwise on the strings **y** and **c**
- The values of f repeat themselves in some pattern **c**
- **c** is called the "period" of f
- Purpose of Simon's Algorithm is to determine **c**

Periodic Function Example

- number of bits $n=3$
- Consider $\mathbf{c}=101$

$$\overset{\mathbf{y}}{000} \oplus \overset{\mathbf{c}}{101} = \overset{\mathbf{x}}{101} \Rightarrow f(000) = f(101)$$
$$001 \oplus 101 = 100 \Rightarrow f(001) = f(100)$$
$$010 \oplus 101 = 111 \Rightarrow f(010) = f(111)$$
$$011 \oplus 101 = 110 \Rightarrow f(011) = f(110)$$
$$100 \oplus 101 = 001 \Rightarrow f(100) = f(001)$$
$$101 \oplus 101 = 000 \Rightarrow f(101) = f(000)$$
$$110 \oplus 101 = 011 \Rightarrow f(110) = f(011)$$
$$111 \oplus 101 = 010 \Rightarrow f(111) = f(010)$$

this must hold if $f(\mathbf{x})=f(\mathbf{y})$ over **c**, the period of f

if $\mathbf{c}=0^n$, what does that imply about f

Periodic Function Example

- number of bits n=3
- Consider $\mathbf{c}$=101

$$\begin{array}{l} \mathbf{y} \quad\quad \mathbf{c} \quad\quad \mathbf{x} \\ 000 \oplus 101 = 101 \Rightarrow f(000) = f(101) \\ 001 \oplus 101 = 100 \Rightarrow f(001) = f(100) \\ 010 \oplus 101 = 111 \Rightarrow f(010) = f(111) \\ 011 \oplus 101 = 110 \Rightarrow f(011) = f(110) \\ 100 \oplus 101 = 001 \Rightarrow f(100) = f(001) \\ 101 \oplus 101 = 000 \Rightarrow f(101) = f(000) \\ 110 \oplus 101 = 011 \Rightarrow f(110) = f(011) \\ 111 \oplus 101 = 010 \Rightarrow f(111) = f(010) \end{array}$$

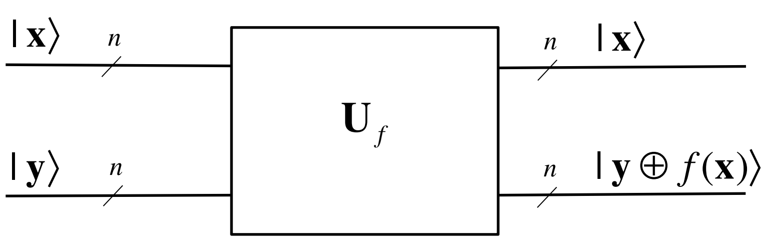
this must hold if $f(\mathbf{x})=f(\mathbf{y})$ over $\mathbf{c}$, the period of f

if $\mathbf{c}=0^n$, what does that imply about f

f is one-to-one

Function Specification

- Unknown function specified as a unitary operation of the form:



- Setting $\mathbf{y}=0^n$ Provides a Convenient way to evaluate $f(\mathbf{x})$

Classical Solution to Problem

- Evaluate $f(\mathbf{x})$ on different binary strings
- After Each Evaluation, Check if Function Response has Already Been Found
- If two strings $\mathbf{x}_1$ and $\mathbf{x}_2$ are found such that $f(\mathbf{x}_1)=f(\mathbf{x}_2)$ then it is assured that:

$$\mathbf{x}_1 = \mathbf{x}_2 \oplus \mathbf{c}$$

- How do we find $\mathbf{c}$?

Classical Solution to Problem

- Evaluate $f(\mathbf{x})$ on different binary strings
- After Each Evaluation, Check if Function Response has Already Been Found
- If two strings $\mathbf{x}_1$ and $\mathbf{x}_2$ are found such that $f(\mathbf{x}_1)=f(\mathbf{x}_2)$ then it is assured that:

$$\mathbf{x}_1 = \mathbf{x}_2 \oplus \mathbf{c}$$

- How do we find $\mathbf{c}$?

$$\mathbf{x}_2 \oplus \mathbf{x}_1 = \mathbf{x}_2 \oplus \mathbf{x}_2 \oplus \mathbf{c} = \left(\mathbf{x}_2 \oplus \mathbf{x}_2\right) \oplus \mathbf{c} = 0 \oplus \mathbf{c} = \mathbf{c}$$

$$\mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{c}$$

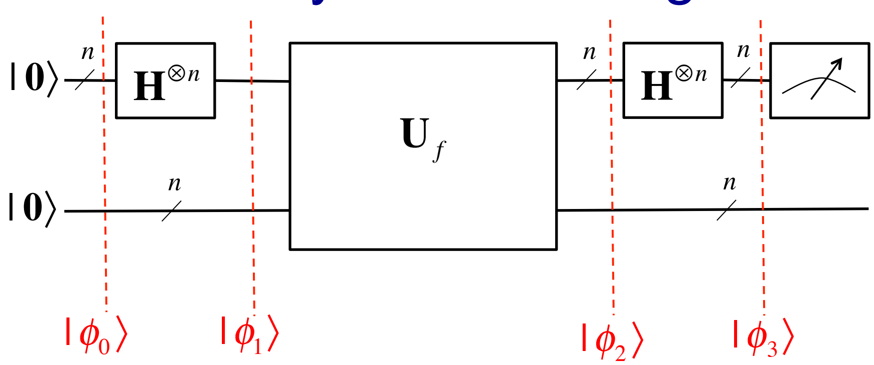
Classical Solution Complexity

- If $f(\mathbf{x})$ is not one-to-one (it is two-to-one) then a repeat will be found before half of inputs are evaluated
- If more than half of inputs checked with no match, then $f(\mathbf{x})$ is one-to-one and $\mathbf{c}=0^n$
- Worst case number of evaluations:

$$\frac{2^n}{2}+1=2^{n-1}+1$$

- Exponential Complexity

Periodicity Quantum Algorithm



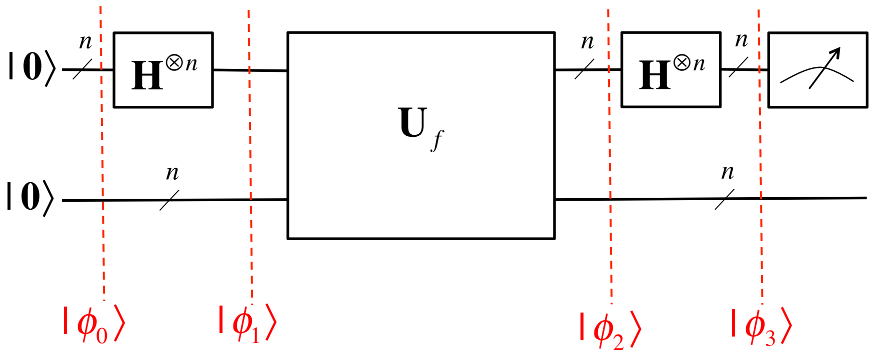
$$|\phi_0\rangle = |\mathbf{00}\rangle \qquad |\phi_2\rangle = \mathbf{U}_f |\phi_1\rangle$$

$$|\phi_1\rangle = \left(\mathbf{H}^{\otimes n} \otimes \mathbf{I}_n\right)|\phi_0\rangle \qquad |\phi_3\rangle = \left(\mathbf{H}^{\otimes n} \otimes \mathbf{I}_n\right)|\phi_2\rangle$$

$$|\phi_3\rangle = \mathbf{G}_{simon}|\phi_0\rangle$$

$$\mathbf{G}_{simon} = \left(\mathbf{H}^{\otimes n} \otimes \mathbf{I}_n\right)\mathbf{U}_f\left(\mathbf{H}^{\otimes n} \otimes \mathbf{I}_n\right)$$

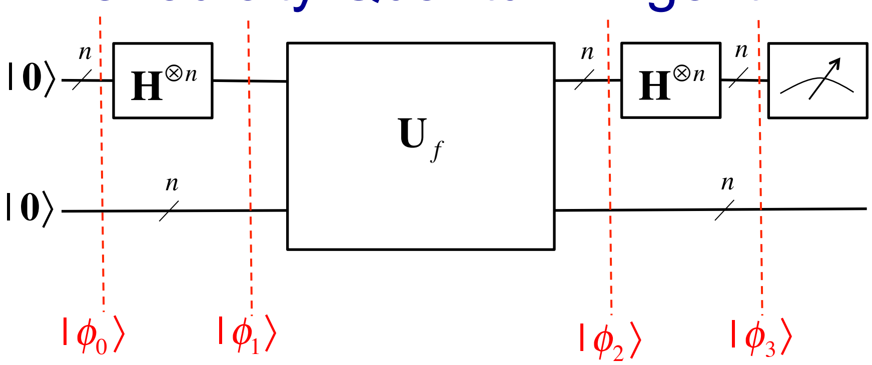
Periodicity Quantum Algorithm



- Places Upper n Qubits in State of Superposition
- EXAMPLE: n=3:

$$|\phi_1\rangle = \left(\mathbf{H}^{\otimes 3} \otimes \mathbf{I}_3\right) |\phi_0\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3} |\mathbf{x},\mathbf{0}\rangle}{\sqrt{2^3}} = \frac{|000,000\rangle + |001,000\rangle + ... + |111,000\rangle}{\sqrt{8}}$$

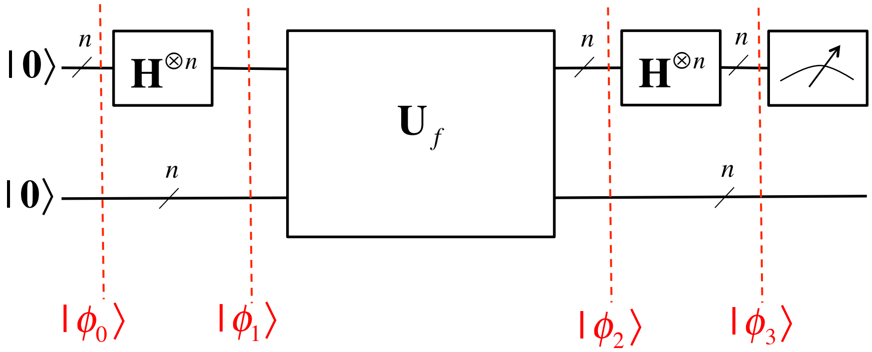
Periodicity Quantum Algorithm



- $\mathbf{U}_f$ causes evaluation of f for the superimposed quantum state

$$|\phi_2\rangle = \mathbf{U}_f \left(\mathbf{H}^{\otimes 3} \otimes \mathbf{I}_3\right) |\phi_1\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3} |\mathbf{x}, f(\mathbf{x})\rangle}{\sqrt{2^3}}$$

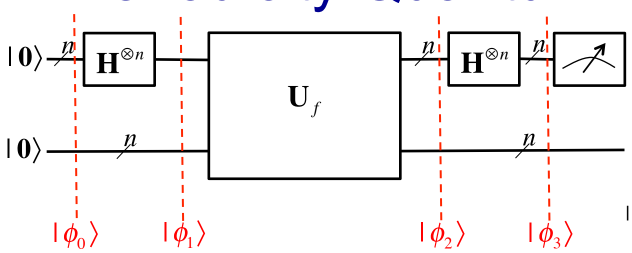
Periodicity Quantum Algorithm



- n-Dimensional Hadamard Transform applied again

$$|\phi_3\rangle = \left(\mathbf{H}^{\otimes 3} \otimes \mathbf{I}_3\right)|\phi_2\rangle = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^n} \sum\limits_{\mathbf{z}\in\{0,1\}^n} (-1)^{\langle \mathbf{z},\mathbf{x}\rangle} |\mathbf{z}, f(\mathbf{x})\rangle}{\sqrt{2^n}}$$

Periodicity Quantum Algorithm



$$|\phi_3\rangle = \frac{\sum\limits_{\mathbf{x}\in\{0,1\}^n} \sum\limits_{\mathbf{z}\in\{0,1\}^n} (-1)^{\langle \mathbf{z},\mathbf{x}\rangle} |\mathbf{z}, f(\mathbf{x})\rangle}{\sqrt{2^n}}$$

- n-Dimensional Hadamard Transform applied again
- For each $\mathbf{x}$ and $\mathbf{z}$ in the Summations, Consider when: $|\mathbf{z}, f(\mathbf{x})\rangle = |\mathbf{z}, f(\mathbf{x} \oplus \mathbf{c})\rangle$
- When this occurs, coefficient is:

$$\frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c}\rangle}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle \oplus \langle \mathbf{z},\mathbf{c}\rangle}}{2}$$

$$= \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle}(-1)^{\langle \mathbf{z},\mathbf{c}\rangle}}{2}$$

Periodicity Quantum Algorithm

$$\frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c} \rangle}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle \oplus \langle \mathbf{z},\mathbf{c} \rangle}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}(-1)^{\langle \mathbf{z},\mathbf{c} \rangle}}{2}$$

- When: $\langle \mathbf{z},\mathbf{c} \rangle = 1$

$$\frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}(-1)^{\langle \mathbf{z},\mathbf{c} \rangle}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}(-1)^{1}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} - (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}}{2} = 0$$

- When: $\langle \mathbf{z},\mathbf{c} \rangle = 0$

$$\frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}(-1)^{\langle \mathbf{z},\mathbf{c} \rangle}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}(-1)^{0}}{2} = \frac{(-1)^{\langle \mathbf{z},\mathbf{x} \rangle} + (-1)^{\langle \mathbf{z},\mathbf{x} \rangle}}{2} = 1$$

- Therefore, when measuring the top qubits, we only find those binary strings where: $\langle \mathbf{z},\mathbf{c} \rangle = 0$

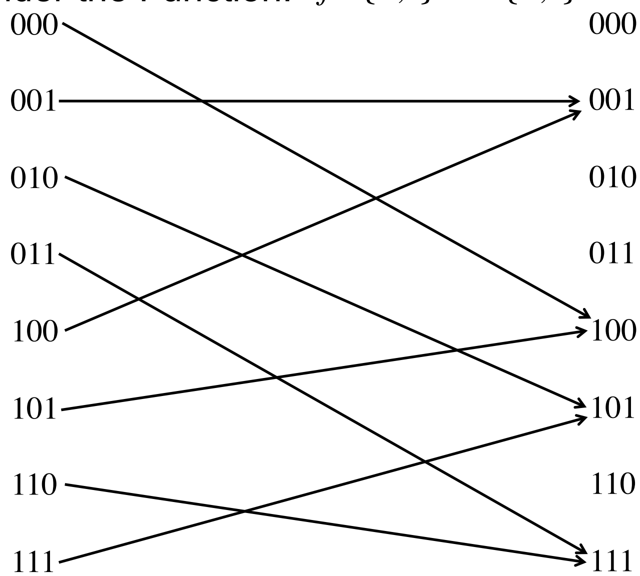
Example Function

- Consider the Function: $f : \{0,1\}^3 \rightarrow \{0,1\}^3$
- Truth Table Representation – Embedded Inside $\mathbf{U}_f$

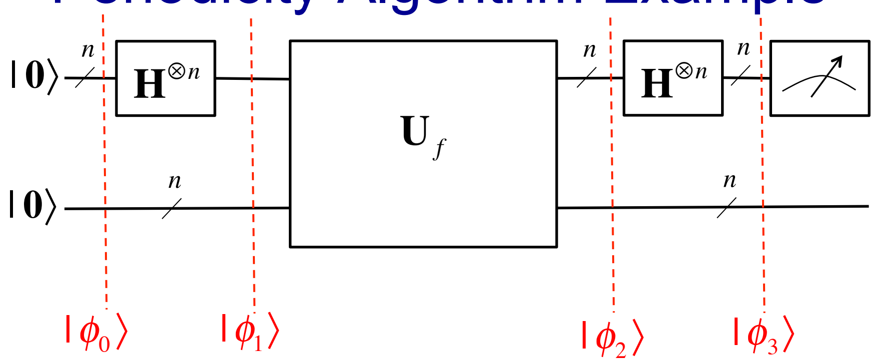
$x_1\ x_2\ x_3$	f
0 0 0	100
0 0 1	001
0 1 0	101
0 1 1	111
1 0 0	001
1 0 1	100
1 1 0	111
1 1 1	101

Periodicity Algorithm Example

- Consider the Function: $f:\{0,1\}^3 \rightarrow \{0,1\}^3$



Periodicity Algorithm Example



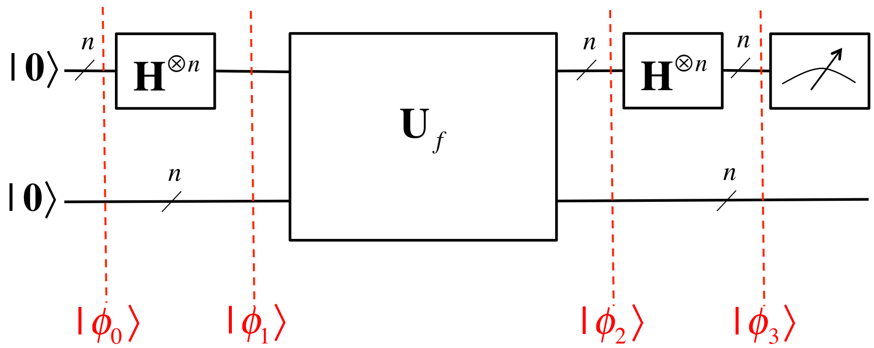
$$|\phi_0\rangle = |\mathbf{00}\rangle = |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle = |000\rangle \otimes |000\rangle$$

$$|\phi_1\rangle = \left(\mathbf{H}^{\otimes 3} \otimes \mathbf{I}_3\right)|\phi_0\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3} |\mathbf{x},\mathbf{0}\rangle}{\sqrt{2^3}} = \frac{|000,000\rangle + |001,000\rangle + \ldots + |111,000\rangle}{\sqrt{8}}$$

$$= \frac{1}{\sqrt{8}}(|000\rangle\otimes|000\rangle + |001\rangle\otimes|000\rangle + |010\rangle\otimes|000\rangle + |011\rangle\otimes|000\rangle$$

$$+ |100\rangle\otimes|000\rangle + |101\rangle\otimes|000\rangle + |110\rangle\otimes|000\rangle + |111\rangle\otimes|000\rangle)$$

Periodicity Algorithm Example



$$|\phi_2\rangle = \mathbf{U}_f\left(\mathbf{H}^{\otimes 3}\otimes\mathbf{I}_3\right)|\phi_0\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3}|\mathbf{x},f(\mathbf{x})\rangle}{\sqrt{2^3}} = \frac{\sum_{\mathbf{x}\in\{0,1\}^3}|\mathbf{x}\rangle\otimes|f(\mathbf{x})\rangle}{\sqrt{8}}$$

Periodicity Algorithm Example

$$|\phi_2\rangle = \mathbf{U}_f\left(\mathbf{H}^{\otimes 3}\otimes\mathbf{I}_3\right)|\phi_0\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3}|\mathbf{x},f(\mathbf{x})\rangle}{\sqrt{2^3}} = \frac{\sum_{\mathbf{x}\in\{0,1\}^3}|\mathbf{x}\rangle\otimes|f(\mathbf{x})\rangle}{\sqrt{8}}$$

$$|\phi_2\rangle = \frac{1}{\sqrt{8}}(|000\rangle\otimes|100\rangle + |001\rangle\otimes|001\rangle + |010\rangle\otimes|101\rangle + |011\rangle\otimes|111\rangle$$
$$+|100\rangle\otimes|001\rangle + |101\rangle\otimes|100\rangle + |110\rangle\otimes|111\rangle + |111\rangle\otimes|101\rangle)$$

- In the Next Stage of the Cascade:

$$|\phi_3\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3}\sum_{\mathbf{z}\in\{0,1\}^3}(-1)^{\langle\mathbf{z},\mathbf{x}\rangle}|\mathbf{z}\rangle\otimes|f(\mathbf{x})\rangle}{\left(\sqrt{8}\right)\left(\sqrt{8}\right)}$$

Periodicity Algorithm Example

- Writing this out Term by Term Yields:

$$
\begin{aligned}
|\phi_3\rangle = \frac{1}{8}(&(+1)|000\rangle\otimes|f(000)\rangle+(+1)|000\rangle\otimes|f(001)\rangle+(+1)|000\rangle\otimes|f(010)\rangle+(+1)|000\rangle\otimes|f(011)\rangle \\
&+(+1)|000\rangle\otimes|f(100)\rangle+(+1)|000\rangle\otimes|f(101)\rangle+(+1)|000\rangle\otimes|f(110)\rangle+(+1)|000\rangle\otimes|f(111)\rangle \\
&+((+1)|001\rangle\otimes|f(000)\rangle+(-1)|001\rangle\otimes|f(001)\rangle+(+1)|001\rangle\otimes|f(010)\rangle+(-1)|001\rangle\otimes|f(011)\rangle \\
&+(+1)|001\rangle\otimes|f(100)\rangle+(-1)|001\rangle\otimes|f(101)\rangle+(+1)|001\rangle\otimes|f(110)\rangle+(-1)|001\rangle\otimes|f(111)\rangle \\
&+((+1)|010\rangle\otimes|f(000)\rangle+(+1)|010\rangle\otimes|f(001)\rangle+(-1)|010\rangle\otimes|f(010)\rangle+(-1)|010\rangle\otimes|f(011)\rangle \\
&+(+1)|010\rangle\otimes|f(100)\rangle+(+1)|010\rangle\otimes|f(101)\rangle+(-1)|010\rangle\otimes|f(110)\rangle+(-1)|010\rangle\otimes|f(111)\rangle \\
&+((+1)|011\rangle\otimes|f(000)\rangle+(-1)|011\rangle\otimes|f(001)\rangle+(-1)|011\rangle\otimes|f(010)\rangle+(+1)|011\rangle\otimes|f(011)\rangle \\
&+(+1)|011\rangle\otimes|f(100)\rangle+(-1)|011\rangle\otimes|f(101)\rangle+(-1)|011\rangle\otimes|f(110)\rangle+(+1)|011\rangle\otimes|f(111)\rangle
\end{aligned}
$$

Periodicity Algorithm Example

$$
\begin{aligned}
&+(+1)|100\rangle\otimes|f(000)\rangle+(+1)|100\rangle\otimes|f(001)\rangle+(+1)|100\rangle\otimes|f(010)\rangle+(+1)|100\rangle\otimes|f(011)\rangle \\
&+(-1)|100\rangle\otimes|f(100)\rangle+(-1)|100\rangle\otimes|f(101)\rangle+(-1)|100\rangle\otimes|f(110)\rangle+(-1)|100\rangle\otimes|f(111)\rangle \\
&+((+1)|101\rangle\otimes|f(000)\rangle+(-1)|101\rangle\otimes|f(001)\rangle+(+1)|101\rangle\otimes|f(010)\rangle+(-1)|101\rangle\otimes|f(011)\rangle \\
&+(-1)|101\rangle\otimes|f(100)\rangle+(+1)|101\rangle\otimes|f(101)\rangle+(-1)|101\rangle\otimes|f(110)\rangle+(+1)|101\rangle\otimes|f(111)\rangle \\
&+((+1)|110\rangle\otimes|f(000)\rangle+(+1)|110\rangle\otimes|f(001)\rangle+(-1)|110\rangle\otimes|f(010)\rangle+(-1)|110\rangle\otimes|f(011)\rangle \\
&+(-1)|110\rangle\otimes|f(100)\rangle+(-1)|110\rangle\otimes|f(101)\rangle+(+1)|110\rangle\otimes|f(110)\rangle+(+1)|110\rangle\otimes|f(111)\rangle \\
&+((+1)|111\rangle\otimes|f(000)\rangle+(-1)|111\rangle\otimes|f(001)\rangle+(-1)|111\rangle\otimes|f(010)\rangle+(+1)|111\rangle\otimes|f(011)\rangle \\
&+(-1)|111\rangle\otimes|f(100)\rangle+(+1)|111\rangle\otimes|f(101)\rangle+(+1)|111\rangle\otimes|f(110)\rangle+(-1)|111\rangle\otimes|f(111)\rangle)
\end{aligned}
$$

- Coefficients in Red are the Elements of: $\mathbf{H}^{\otimes 3}$
- Evaluating the Function f in the Previous Equation Yields the Following:

Periodicity Algorithm Example

- Evaluating the Function f in the Previous Equation Yields the Following:

$$
\begin{aligned}
|\phi_3\rangle = \frac{1}{8}(&(+1)|000\rangle\otimes|100\rangle + (+1)|000\rangle\otimes|001\rangle + (+1)|000\rangle\otimes|101\rangle + (+1)|000\rangle\otimes|111\rangle \\
&+ (+1)|000\rangle\otimes|001\rangle + (+1)|000\rangle\otimes|100\rangle + (+1)|000\rangle\otimes|111\rangle + (+1)|000\rangle\otimes|101\rangle \\
&+ ((+1)|001\rangle\otimes|100\rangle + (-1)|001\rangle\otimes|001\rangle + (+1)|001\rangle\otimes|101\rangle + (-1)|001\rangle\otimes|111\rangle \\
&+ (+1)|001\rangle\otimes|001\rangle + (-1)|001\rangle\otimes|100\rangle + (+1)|001\rangle\otimes|111\rangle + (-1)|001\rangle\otimes|101\rangle \\
&+ ((+1)|010\rangle\otimes|100\rangle + (+1)|010\rangle\otimes|001\rangle + (-1)|010\rangle\otimes|101\rangle + (-1)|010\rangle\otimes|111\rangle \\
&+ (+1)|010\rangle\otimes|001\rangle + (+1)|010\rangle\otimes|100\rangle + (-1)|010\rangle\otimes|111\rangle + (-1)|010\rangle\otimes|101\rangle \\
&+ ((+1)|011\rangle\otimes|100\rangle + (-1)|011\rangle\otimes|001\rangle + (-1)|011\rangle\otimes|101\rangle + (+1)|011\rangle\otimes|111\rangle \\
&+ (+1)|011\rangle\otimes|001\rangle + (-1)|011\rangle\otimes|100\rangle + (-1)|011\rangle\otimes|111\rangle + (+1)|011\rangle\otimes|101\rangle
\end{aligned}
$$

Periodicity Algorithm Example

- Evaluating the Function f in the Previous Equation Yields the Following (continued):

$$
\begin{aligned}
&+ (+1)|100\rangle\otimes|100\rangle + (+1)|100\rangle\otimes|001\rangle + (+1)|100\rangle\otimes|101\rangle + (+1)|100\rangle\otimes|111\rangle \\
&+ (-1)|100\rangle\otimes|001\rangle + (-1)|100\rangle\otimes|100\rangle + (-1)|100\rangle\otimes|111\rangle + (-1)|100\rangle\otimes|101\rangle \\
&+ ((+1)|101\rangle\otimes|100\rangle + (-1)|101\rangle\otimes|001\rangle + (+1)|101\rangle\otimes|101\rangle + (-1)|101\rangle\otimes|111\rangle \\
&+ (-1)|101\rangle\otimes|001\rangle + (+1)|101\rangle\otimes|100\rangle + (-1)|101\rangle\otimes|111\rangle + (+1)|101\rangle\otimes|101\rangle \\
&+ ((+1)|110\rangle\otimes|100\rangle + (+1)|110\rangle\otimes|001\rangle + (-1)|110\rangle\otimes|101\rangle + (-1)|110\rangle\otimes|111\rangle \\
&+ (-1)|110\rangle\otimes|001\rangle + (-1)|110\rangle\otimes|100\rangle + (+1)|110\rangle\otimes|111\rangle + (+1)|110\rangle\otimes|101\rangle \\
&+ ((+1)|111\rangle\otimes|100\rangle + (-1)|111\rangle\otimes|001\rangle + (-1)|111\rangle\otimes|101\rangle + (+1)|111\rangle\otimes|111\rangle \\
&+ (-1)|111\rangle\otimes|001\rangle + (+1)|111\rangle\otimes|100\rangle + (+1)|111\rangle\otimes|111\rangle + (-1)|111\rangle\otimes|101\rangle)
\end{aligned}
$$

Periodicity Algorithm Example

- Combining Like Terms and Cancelling Out Where Possible Yields the Following:

$$
\begin{aligned}
|\phi_3\rangle = \frac{1}{8}((+2)|000\rangle\otimes|100\rangle + (+2)|000\rangle\otimes|001\rangle + (+2)|000\rangle\otimes|101\rangle + (+2)|000\rangle\otimes|111\rangle \\
+(+2)|010\rangle\otimes|100\rangle + (+2)|010\rangle\otimes|001\rangle + (-2)|010\rangle\otimes|101\rangle + (-2)|010\rangle\otimes|111\rangle \\
+(+2)|101\rangle\otimes|100\rangle + (-2)|101\rangle\otimes|001\rangle + (+2)|101\rangle\otimes|101\rangle + (-2)|101\rangle\otimes|111\rangle \\
+(+2)|111\rangle\otimes|100\rangle + (-2)|111\rangle\otimes|001\rangle + (-2)|111\rangle\otimes|101\rangle + (+2)|111\rangle\otimes|111\rangle)
\end{aligned}
$$

$$
\begin{aligned}
|\phi_3\rangle = \frac{1}{8}((+2)|000\rangle \otimes (|100\rangle + |001\rangle + |101\rangle + |111\rangle) \\
+(+2)|010\rangle \otimes (|100\rangle + |001\rangle - |101\rangle - |111\rangle) \\
+(+2)|101\rangle \otimes (|100\rangle - |001\rangle + |101\rangle - |111\rangle) \\
+(+2)|111\rangle \otimes (|100\rangle - |001\rangle - |101\rangle + |111\rangle))
\end{aligned}
$$

Periodicity Algorithm Example

$$
\begin{aligned}
|\phi_3\rangle = \frac{1}{8}((+2)|000\rangle \otimes (|100\rangle + |001\rangle + |101\rangle + |111\rangle) \\
+(+2)|010\rangle \otimes (|100\rangle + |001\rangle - |101\rangle - |111\rangle) \\
+(+2)|101\rangle \otimes (|100\rangle - |001\rangle + |101\rangle - |111\rangle) \\
+(+2)|111\rangle \otimes (|100\rangle - |001\rangle - |101\rangle + |111\rangle))
\end{aligned}
$$

- Measuring the Top 3 Qubits Gives (with equal probability): $|000\rangle, |010\rangle, |101\rangle, |111\rangle$

- For Each of These Measured Quantum States, it is True that the Inner Product with the Period Bitstring $\mathbf{c}$ is Zero

Periodicity Algorithm Example

- For Each of These Measured Quantum States, it is True that the Inner Product with the Period Bitstring **c** is Zero
- The Algorithm/Circuit is Measured a Sufficient Number of Times to Ensure All Possible Measurements are Obtained
- This Yields a Set of Simultaneous Equations:

$$
\begin{aligned}
&(i) \quad \langle 000,\mathbf{c}\rangle = 0\\
&(ii) \quad \langle 010,\mathbf{c}\rangle = 0\\
&(iii) \quad \langle 101,\mathbf{c}\rangle = 0\\
&(iv) \quad \langle 111,\mathbf{c}\rangle = 0
\end{aligned}
$$

Periodicity Algorithm Example

$$
\begin{aligned}
&\langle 000, c_1c_2c_3\rangle = 0\\
&\langle 010, c_1c_2c_3\rangle = 0\\
&\langle 101, c_1c_2c_3\rangle = 0\\
&\langle 111, c_1c_2c_3\rangle = 0
\end{aligned}
$$

$$
\begin{aligned}
&(0 \wedge c_1) \oplus (0 \wedge c_2) \oplus (0 \wedge c_3) = 0\\
&(0 \wedge c_1) \oplus (1 \wedge c_2) \oplus (0 \wedge c_3) = 0\\
&(1 \wedge c_1) \oplus (0 \wedge c_2) \oplus (1 \wedge c_3) = 0\\
&(1 \wedge c_1) \oplus (1 \wedge c_2) \oplus (1 \wedge c_3) = 0
\end{aligned}
$$

Periodicity Algorithm Example

$$c_2 = 0$$
$$c_1 \oplus c_3 = 0$$
$$c_1 \oplus c_2 \oplus c_3 = 0$$

- This Means that $c_1=c_3=0$ or that $c_1=c_3=1$
- We Know that $\mathbf{c}$ is NOT EQUAL to 000 Since Function was Found not to be One-to-One
- Therefore $c_1=c_3=1$
- Period of Function is:

$$\mathbf{c} = c_1 c_2 c_3 = 101$$

Periodicity Algorithm Example

- Must Run Simon's Algorithm Several Times to Measure n Different $\mathbf{z}$ Bitstrings

- Next Use a Classical Computer for Solving n Different Linear Equations