Now the top qubits of state $|\varphi_3\rangle$ are measured. Rather than figuring out what we will get after measuring the top qubit, let us ask the following question: What is the probability that the top qubits of $|\varphi_3\rangle$ will collapse to the state $|\mathbf{0}\rangle$? We can answer this by setting $\mathbf{z} = \mathbf{0}$ and realizing that $\langle \mathbf{z}, \mathbf{x}\rangle = \langle \mathbf{0}, \mathbf{x}\rangle = 0$ for all $\mathbf{x}$. In this case, we have reduced $|\varphi_3\rangle$ to

$$\left[\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{6.78}$$

So, the probability of collapsing to $|\mathbf{0}\rangle$ is totally dependent on $f(\mathbf{x})$. If $f(\mathbf{x})$ is constant at 1, the top qubits become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)|\mathbf{0}\rangle}{2^n} = \frac{-(2^n)|\mathbf{0}\rangle}{2^n} = -1|\mathbf{0}\rangle. \tag{6.79}$$

If $f(\mathbf{x})$ is constant at 0, the top qubits become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}1|\mathbf{0}\rangle}{2^n} = \frac{2^n|\mathbf{0}\rangle}{2^n} = +1|\mathbf{0}\rangle. \tag{6.80}$$

And finally, if f is balanced, then half of the $\mathbf{x}$'s will cancel the other half and the top qubits will become

$$\frac{\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{f(\mathbf{x})}|\mathbf{0}\rangle}{2^n} = \frac{0|\mathbf{0}\rangle}{2^n} = 0|\mathbf{0}\rangle. \tag{6.81}$$

When measuring the top qubits of $|\varphi_3\rangle$, we will only get $|\mathbf{0}\rangle$ if the function is constant. If anything else is found after being measured, then the function is balanced.

In conclusion, we have solved the – admittedly contrived – problem in one function evaluation as opposed to the $2^{n-1}+1$ function evaluations needed in classical computations. That is an exponential speedup!

Exercise 6.2.5 What would happen if we were tricked and the given function was neither balanced nor constant? What would our algorithm produce? ■

6.3 SIMON'S PERIODICITY ALGORITHM

Simon's algorithm is about finding patterns in functions. We will use methods that we already learned in previous sections, but we will also employ other ideas. This algorithm is a combination of quantum procedures as well as classical procedures.

Suppose that we are given a function $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ that we can evaluate but it is given to us as a black box. We are further assured that there exists a secret (hidden) binary string $\mathbf{c} = c_0c_1c_2\cdots c_{n-1}$, such that for all strings $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$, we have

$$f(\mathbf{x}) = f(\mathbf{y}) \quad \text{if and only if } \mathbf{x} = \mathbf{y} \oplus \mathbf{c}, \tag{6.82}$$

where $\oplus$ is the bitwise exclusive-or operation. In other words, the values of f repeat themselves in some pattern and the pattern is determined by $\mathbf{c}$. We call $\mathbf{c}$ the **period** of f. The goal of Simon's algorithm is to determine $\mathbf{c}$.

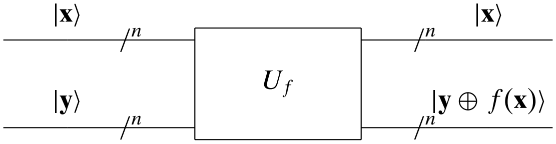
Example 6.3.1 Let us work out an example. Let $n = 3$. Consider $\mathbf{c} = 101$. Then we are going to have the following requirements on f:

- $000 \oplus 101 = 101$; hence, $f(000) = f(101)$.
- $001 \oplus 101 = 100$; hence, $f(001) = f(100)$.
- $010 \oplus 101 = 111$; hence, $f(010) = f(111)$.
- $011 \oplus 101 = 110$; hence, $f(011) = f(110)$.
- $100 \oplus 101 = 001$; hence, $f(100) = f(001)$.
- $101 \oplus 101 = 000$; hence, $f(101) = f(000)$.
- $110 \oplus 101 = 011$; hence, $f(110) = f(011)$.
- $111 \oplus 101 = 010$; hence, $f(111) = f(010)$. □

Exercise 6.3.1 Work out the requirements on f if $\mathbf{c} = 011$. ■

Notice that if $\mathbf{c} = 0^n$, then the function is one to one. Otherwise the function is two to one.

The function f will be given as a unitary operation that can be visualized as



(6.83)

where $|\mathbf{x}, \mathbf{y}\rangle$ goes to $|\mathbf{x}, \mathbf{y} \oplus f(\mathbf{x})\rangle$. U_f is again its own inverse. Setting $\mathbf{y} = 0^n$ would give us an easy way to evaluate $f(\mathbf{x})$.

How would one solve this problem classically? We would have to evaluate f on different binary strings. After each evaluation, check to see if that output has already been found. If one finds two inputs $\mathbf{x_1}$ and $\mathbf{x_2}$ such that $f(\mathbf{x_1}) = f(\mathbf{x_2})$, then we are assured that

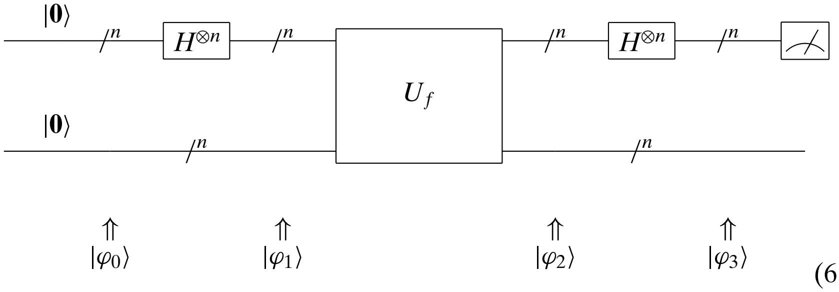
$$\mathbf{x_1} = \mathbf{x_2} \oplus \mathbf{c} \tag{6.84}$$

and can obtain $\mathbf{c}$ by $\oplus$-ing both sides with $\mathbf{x_2}$:

$$\mathbf{x_1} \oplus \mathbf{x_2} = \mathbf{x_2} \oplus \mathbf{c} \oplus \mathbf{x_2} = \mathbf{c}. \tag{6.85}$$

If the function is a two-to-one function, then we will not have to evaluate more than half the inputs before we get a repeat. If we evaluate more than half the strings and still cannot find a match, then we know that f is one to one and that $\mathbf{c} = 0^n$. So, in the worst case, $\frac{2^n}{2} + 1 = 2^{n-1} + 1$ function evaluations will be needed. Can we do better?

The quantum part of Simon's algorithm basically consists of performing the following operations several times:



(6.86)

In terms of matrices this is

$$(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes I)|\mathbf{0}, \mathbf{0}\rangle. \tag{6.87}$$

Let us look at the states of the system. We start at

$$|\varphi_0\rangle = |\mathbf{0}, \mathbf{0}\rangle. \tag{6.88}$$

We then place the input in a superposition of all possible inputs. From Equation (6.63) we know that it looks like

$$|\varphi_1\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}, \mathbf{0}\rangle}{\sqrt{2^n}}. \tag{6.89}$$

Evaluation of f on all these possibilities gives us

$$|\varphi_2\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}, f(\mathbf{x})\rangle}{\sqrt{2^n}}. \tag{6.90}$$

And finally, let us apply $H^{\otimes n}$ to the top output, as in Equation (6.64):

$$|\varphi_3\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^n} \sum_{\mathbf{z}\in\{0,1\}^n} (-1)^{\langle \mathbf{z},\mathbf{x}\rangle} |\mathbf{z}, f(\mathbf{x})\rangle}{2^n}. \tag{6.91}$$

Notice that for each input $\mathbf{x}$ and for each $\mathbf{z}$, we are assured by the one who gave us the function that the ket $|\mathbf{z}, f(\mathbf{x})\rangle$ is the same ket as $|\mathbf{z}, f(\mathbf{x} \oplus \mathbf{c})\rangle$. The coefficient for this ket is then

$$\frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c}\rangle}}{2}. \tag{6.92}$$

Let us examine this coefficient in depth. We saw that $\langle -, -\rangle$ is an inner product and from Equation (6.57)

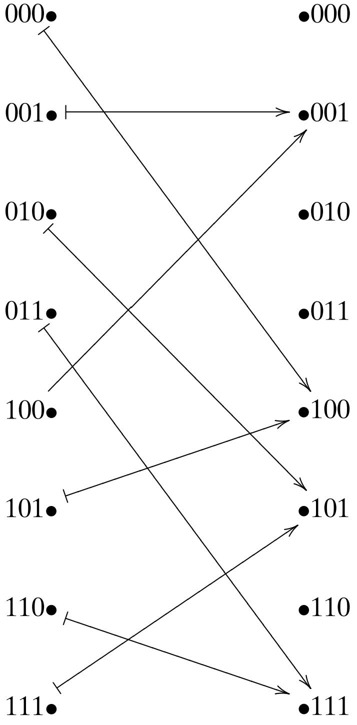
$$\begin{aligned} \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\oplus\mathbf{c}\rangle}}{2} &= \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle\oplus\langle \mathbf{z},\mathbf{c}\rangle}}{2} \\ &= \frac{(-1)^{\langle \mathbf{z},\mathbf{x}\rangle} + (-1)^{\langle \mathbf{z},\mathbf{x}\rangle}(-1)^{\langle \mathbf{z},\mathbf{c}\rangle}}{2}. \end{aligned} \tag{6.93}$$

So, if $\langle \mathbf{z}, \mathbf{c}\rangle = 1$, the terms of the numerator of this coefficient will cancel each other out and we would get $\frac{0}{2}$. In contrast, if $\langle \mathbf{z}, \mathbf{c}\rangle = 0$, the sum will be $\frac{\pm 2}{2} = \pm 1$. Hence, upon measuring the top qubits, we will only find those binary strings such that $\langle \mathbf{z}, \mathbf{c} \rangle = 0$.

This algorithm becomes completely clear only after we look at a concrete example.

Reader Tip. Warning: admittedly, working out all the gory details of an example can be a bit scary. We recommend that the less meticulous reader move on to the next section for now. Return to this example on a calm sunny day, prepare a good cup of your favorite tea or coffee, and go through the details: the effort will pay off. ♡

Consider the function $f : \{0,1\}^3 \longrightarrow \{0,1\}^3$ defined as



(6.94)

Let us go through the states of the algorithm with this function:

$$|\varphi_0\rangle = |\mathbf{0}, \mathbf{0}\rangle = |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle, \tag{6.95}$$

$$|\varphi_1\rangle = \frac{\sum_{\mathbf{x} \in \{0,1\}^3} |\mathbf{x}\rangle}{\sqrt{8}} \otimes |\mathbf{0}\rangle. \tag{6.96}$$

We might also write this as

$$|\varphi_1\rangle = \frac{1}{\sqrt{8}}(|000\rangle \otimes |000\rangle + |001\rangle \otimes |000\rangle + |010\rangle \otimes |000\rangle + |011\rangle \otimes |000\rangle$$
$$+ |100\rangle \otimes |000\rangle + |101\rangle \otimes |000\rangle + |110\rangle \otimes |000\rangle + |111\rangle \otimes |000\rangle).$$

After applying U_f, we have

$$|\varphi_2\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3} |\mathbf{x}\rangle \otimes |f(\mathbf{x})\rangle}{\sqrt{8}} \tag{6.97}$$

or

$$\begin{aligned}|\varphi_2\rangle = \frac{1}{\sqrt{8}}(&|000\rangle \otimes |100\rangle + |001\rangle \otimes |001\rangle + |010\rangle \otimes |101\rangle + |011\rangle \otimes |111\rangle\\ &+ |100\rangle \otimes |001\rangle + |101\rangle \otimes |100\rangle + |110\rangle \otimes |111\rangle + |111\rangle \otimes |101\rangle).\end{aligned}$$

Then applying $H^{\otimes n} \otimes I$ we get

$$|\varphi_3\rangle = \frac{\sum_{\mathbf{x}\in\{0,1\}^3} \sum_{\mathbf{z}\in\{0,1\}^3} (-1)^{\langle \mathbf{z},\mathbf{x}\rangle} |\mathbf{z}\rangle \otimes f(\mathbf{x})\rangle}{8}. \tag{6.98}$$

This amounts to

$$\begin{aligned}|\varphi_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\\
&+ (+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}$$

Notice that the coefficients follow the exact pattern as $H^{\otimes 3}$ on page 184.

Evaluating the function f gives us

$$\begin{aligned}
|\varphi_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 \\
&+ (+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}$$

Combining like terms and canceling out gives us

$$\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+2)|000\rangle \otimes |100\rangle + (+2)|000\rangle \otimes |001\rangle + (+2)|000\rangle \otimes |101\rangle + (+2)|000\rangle \otimes |111\rangle \\
&+ (+2)|010\rangle \otimes |100\rangle + (+2)|010\rangle \otimes |001\rangle + (-2)|010\rangle \otimes |101\rangle + (-2)|010\rangle \otimes |111\rangle \\
&+ (+2)|101\rangle \otimes |100\rangle + (-2)|101\rangle \otimes |001\rangle + (+2)|101\rangle \otimes |101\rangle + (-2)|101\rangle \otimes |111\rangle \\
&+ (+2)|111\rangle \otimes |100\rangle + (-2)|111\rangle \otimes |001\rangle + (-2)|111\rangle \otimes |101\rangle + (+2)|111\rangle \otimes |111\rangle)
\end{aligned}$$

or

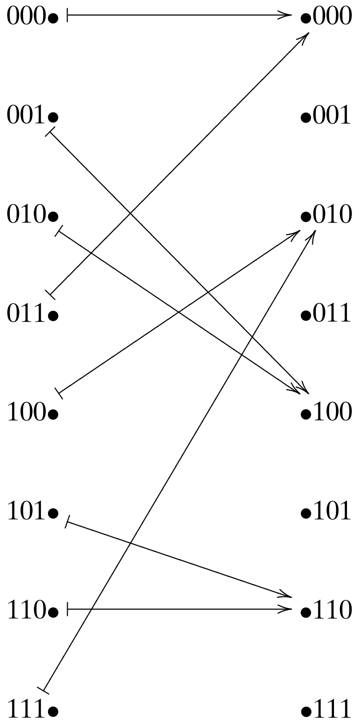
$$\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+2)|000\rangle \otimes (|100\rangle + |001\rangle + |101\rangle + |111\rangle) \\
&+ (+2)|010\rangle \otimes (|100\rangle + |001\rangle - |101\rangle - |111\rangle) \\
&+ (+2)|101\rangle \otimes (|100\rangle - |001\rangle + |101\rangle - |111\rangle) \\
&+ (+2)|111\rangle \otimes (|100\rangle - |001\rangle - |101\rangle + |111\rangle)).
\end{aligned}$$

When we measure the top output, we will get, with equal probability, 000, 010, 101, or 111. We know that for all these, the inner product with the missing $\mathbf{c}$ is 0. This gives us the set of equations:

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

If we write $\mathbf{c}$ as $\mathbf{c} = c_1c_2c_3$, then Equation (ii) tells us that $c_2 = 0$. Equation (iii) tells us that $c_1 \oplus c_3 = 0$ or that either $c_1 = c_3 = 0$ or $c_1 = c_3 = 1$. Because we know that $\mathbf{c} \neq 000$, we come to the conclusion that $\mathbf{c} = 101$.

Exercise 6.3.2 Do a similar analysis for the function f defined as



(6.99)

■

After running Simon's algorithm several times, we will get n different $\mathbf{z}_i$ such that $\langle \mathbf{z}_i, \mathbf{c} \rangle = 0$. We then put these results into a classical algorithm that solves "linear equations." They are linear equations; rather than using the usual $+$ operation, we use $\oplus$ on binary strings. Here is a nice worked-out example.

Example 6.3.2 Imagine that we are dealing with a case where $n = 7$. That means we are given a function $f : \{0, 1\}^7 \longrightarrow \{0, 1\}^7$. Let us assume that we ran the algorithm 7 times and we get the following results:

$$\begin{aligned} &\text{(i)} \ \langle 1010110, \mathbf{c} \rangle = 0\\ &\text{(ii)} \ \langle 0010001, \mathbf{c} \rangle = 0\\ &\text{(iii)} \ \langle 1100101, \mathbf{c} \rangle = 0 \end{aligned}$$

$$\begin{aligned}
&\text{(iv)} && \langle 0011011, \mathbf{c}\rangle = 0\\
&\text{(v)} && \langle 0101001, \mathbf{c}\rangle = 0\\
&\text{(vi)} && \langle 0011010, \mathbf{c}\rangle = 0\\
&\text{(vii)} && \langle 0110111, \mathbf{c}\rangle = 0.
\end{aligned}$$

To clear the first column of 1's, we are going to "add" (really pointwise exclusive or) the first equation to the third equation. This gives us

$$\begin{aligned}
&\text{(i)} && \langle 1010110, \mathbf{c}\rangle = 0\\
&\text{(ii)} && \langle 0010001, \mathbf{c}\rangle = 0\\
&\text{(iii)} && \langle 0110011, \mathbf{c}\rangle = 0\\
&\text{(iv)} && \langle 0011011, \mathbf{c}\rangle = 0\\
&\text{(v)} && \langle 0101001, \mathbf{c}\rangle = 0\\
&\text{(vi)} && \langle 0011010, \mathbf{c}\rangle = 0\\
&\text{(vii)} && \langle 0110111, \mathbf{c}\rangle = 0.
\end{aligned}$$

To clear the second column of 1's, we are going to "add" the third equation to the fifth and seventh equations. This gives us

$$\begin{aligned}
&\text{(i)} && \langle 1010110, \mathbf{c}\rangle = 0\\
&\text{(ii)} && \langle 0010001, \mathbf{c}\rangle = 0\\
&\text{(iii)} && \langle 0110011, \mathbf{c}\rangle = 0\\
&\text{(iv)} && \langle 0011011, \mathbf{c}\rangle = 0\\
&\text{(v)} && \langle 0011010, \mathbf{c}\rangle = 0\\
&\text{(vi)} && \langle 0011010, \mathbf{c}\rangle = 0\\
&\text{(vii)} && \langle 0000100, \mathbf{c}\rangle = 0.
\end{aligned}$$

To clear the third column of 1's, we are going to "add" the second equation to Equations (i), (iii), (iv), (v), and (vi). This gives us

$$\begin{aligned}
&\text{(i)} && \langle 1000111, \mathbf{c}\rangle = 0\\
&\text{(ii)} && \langle 0010001, \mathbf{c}\rangle = 0\\
&\text{(iii)} && \langle 0100010, \mathbf{c}\rangle = 0\\
&\text{(iv)} && \langle 0001010, \mathbf{c}\rangle = 0\\
&\text{(v)} && \langle 0001011, \mathbf{c}\rangle = 0\\
&\text{(vi)} && \langle 0001011, \mathbf{c}\rangle = 0\\
&\text{(vii)} && \langle 0000100, \mathbf{c}\rangle = 0.
\end{aligned}$$

To clear the fourth column of 1's, we are going to "add" Equation (iv) to Equations (v) and (vi). We are going to clear the fifth column by adding Equation (vii) to Equation (i). This gives us

$$\begin{aligned}
&\text{(i)} && \langle 1000011, \mathbf{c}\rangle = 0\\
&\text{(ii)} && \langle 0010001, \mathbf{c}\rangle = 0\\
&\text{(iii)} && \langle 0100010, \mathbf{c}\rangle = 0\\
&\text{(iv)} && \langle 0001010, \mathbf{c}\rangle = 0\\
&\text{(v)} && \langle 0000001, \mathbf{c}\rangle = 0\\
&\text{(vi)} && \langle 0000001, \mathbf{c}\rangle = 0\\
&\text{(vii)} && \langle 0000100, \mathbf{c}\rangle = 0.
\end{aligned}$$

And finally, to clear the sixth column of 1's, we are going to "add" Equation (v) to Equations (i), (ii), and (vi). We get

$$\begin{array}{rl}
\text{(i)} & \langle 1000010, \mathbf{c} \rangle = 0 \\
\text{(ii)} & \langle 0010000, \mathbf{c} \rangle = 0 \\
\text{(iii)} & \langle 0100010, \mathbf{c} \rangle = 0 \\
\text{(iv)} & \langle 0001010, \mathbf{c} \rangle = 0 \\
\text{(v)} & \langle 0000001, \mathbf{c} \rangle = 0 \\
\text{(vi)} & \langle 0000000, \mathbf{c} \rangle = 0 \\
\text{(vii)} & \langle 0000100, \mathbf{c} \rangle = 0.
\end{array}$$

We can interpret these equations as

$$\begin{array}{rl}
\text{(i)} & c_1 \oplus c_6 = 0 \\
\text{(ii)} & c_3 = 0 \\
\text{(iii)} & c_2 \oplus c_6 = 0 \\
\text{(iv)} & c_4 \oplus c_6 = 0 \\
\text{(v)} & c_7 = 0 \\
\text{(vi)} & \\
\text{(vii)} & c_5 = 0.
\end{array}$$

Notice that if $c_6 = 0$, then $c_1 = c_2 = c_4 = 0$ and that if $c_6 = 1$, then $c_1 = c_2 = c_4 = 1$. Because we are certain that f is not one to one and $\mathbf{c} \neq 0000000$, we can conclude that $\mathbf{c} = 1101010$. □

Exercise 6.3.3 Solve the following linear equations in a similar manner:

$$\begin{array}{rl}
\text{(i)} & \langle 11110000, \mathbf{c} \rangle = 0 \\
\text{(ii)} & \langle 01101001, \mathbf{c} \rangle = 0 \\
\text{(iii)} & \langle 10010110, \mathbf{c} \rangle = 0 \\
\text{(iv)} & \langle 00111100, \mathbf{c} \rangle = 0 \\
\text{(v)} & \langle 11111111, \mathbf{c} \rangle = 0 \\
\text{(vi)} & \langle 11000011, \mathbf{c} \rangle = 0 \\
\text{(vii)} & \langle 10001110, \mathbf{c} \rangle = 0 \\
\text{(viii)} & \langle 01110001, \mathbf{c} \rangle = 0.
\end{array}$$

(Hint: The answer is $\mathbf{c} = 10011001$.) ■

In conclusion, for a given periodic f, we can find the period $\mathbf{c}$ in n function evaluations. This is in contrast to the $2^{n-1} + 1$ needed with the classical algorithm.

Reader Tip. We shall see this concept of finding the period of a function in Section 6.5 when we present Shor's algorithm. ♡

6.4 GROVER'S SEARCH ALGORITHM

How do you find a needle in a haystack? You look at each piece of hay separately and check each one to see if it is the desired needle. That is not very efficient.