Factoring Using Shor's Quantum Algorithm

Frank Rioux
Emeritus Professor of Chemistry
CSB|SJU

This tutorial presents a toy calculation dealing with quantum factorization using Shor's algorithm. Before beginning that task, traditional classical factorization is reviewed with the example of finding the prime factors of 15. As shown below the key is to find the period of $\mathbf{a^x}$ **modulo 15**, where **a** is chosen randomly.

$a := 4$ $N := 15$ $f(x) := \mathrm{mod}\left(a^x, N\right)$ $Q := 8$ $x := 0 .. Q - 1$

x =	f(x) =
0	1
1	4
2	1
3	4
4	1
5	4
6	1
7	4

Seeing that the period of f(x) is two, the next step is to use the Euclidian algorithm by calculating the greatest common denominator of two functions involving the period and **a**, and the number to be factored, **N**.

$\mathrm{period} := 2$ $\gcd\left(a^{\frac{\mathrm{period}}{2}} - 1, N\right) = 3$ $\gcd\left(a^{\frac{\mathrm{period}}{2}} + 1, N\right) = 5$

We proceed by ignoring the fact that we already know that the period of f(x) is 2 and demonstrate how it is determined using a quantum (discrete) Fourier transform. After the registers are loaded with x and f(x) using a **quantum** computer, they exist in the following **superposition**.

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle = \frac{1}{2}\left[|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|1\rangle + |3\rangle|4\rangle + \cdots\right]$$

The next step is to find the period of f(x) by performing a quantum Fourier transform (QFT) on the input register |x>.

$Q := 4$ $m := 0 .. Q - 1$ $n := 0 .. Q - 1$ $\mathrm{QFT}_{m,n} := \frac{1}{\sqrt{Q}} \cdot \exp\left(i \cdot \frac{2 \cdot \pi \cdot m \cdot n}{Q}\right)$ $\mathrm{QFT} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$

x = 0 $\mathrm{QFT} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5 \\ 0.5 \\ 0.5 \end{pmatrix}$ x = 1 $\mathrm{QFT} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ 0.5i \\ -0.5 \\ -0.5i \end{pmatrix}$ x = 2 $\mathrm{QFT} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.5 \\ -0.5 \\ 0.5 \\ -0.5 \end{pmatrix}$ x = 3 $\mathrm{QFT} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.5 \\ -0.5i \\ -0.5 \\ 0.5i \end{pmatrix}$

The operation of the QFT on the x-register is expressed algebraically in the middle term below. Quantum interference in this term yields the result on the right which shows a period of 2 on the x-register.

$$QFT(x)\frac{1}{2}\left[|0\rangle|1\rangle+|1\rangle|4\rangle+|2\rangle|1\rangle+|3\rangle|4\rangle\right] = \begin{array}{c}\frac{1}{4}\left[|0\rangle+|1\rangle+|2\rangle+|3\rangle\right]|1\rangle \\ + \\ \frac{1}{4}\left[|0\rangle+i|1\rangle-|2\rangle-i|3\rangle\right]|4\rangle \\ + \\ \frac{1}{4}\left[|0\rangle-|1\rangle+|2\rangle-|3\rangle\right]|1\rangle \\ + \\ \frac{1}{4}\left[|0\rangle-i|1\rangle-|2\rangle+i|3\rangle\right]|4\rangle\end{array} = \frac{1}{2}\left[|0\rangle\left(|1\rangle+|4\rangle\right)+|2\rangle\left(|1\rangle-|4\rangle\right)\right]$$

Figure 5 in "Quantum Computation," by David P. DiVincenzo, *Science* **270**, 258 (1995) provides a graphical illustration of the steps of Shor's factorization algorithm.