Quantum computing

1. Compute the product of two single qubits:

   $(a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle) = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$

   Suppose the result is the Bell state $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$. Then $a_1 a_2 = 1$ and $b_1 b_2 = 1$. In particular, all four coefficients must be nonzero, a contradiction to $a_1 b_2 = 0$ and $b_1 a_2 = 0$.

2. Applying the CNOT gate to $H |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ gives the Bell state $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$. The circuit is depicted in Figure 1.

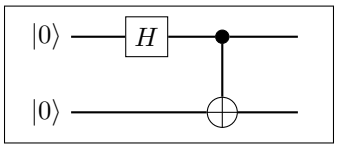

Figure 1. Applying Hadamard and CNOT gate to $|00\rangle$ gives the entangled Bell state $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

   The other three Bell states are

$$\begin{aligned} CNOT(H |0\rangle \otimes |1\rangle) &= \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle , \\ CNOT(H |1\rangle \otimes |0\rangle) &= \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle , \\ CNOT(H |1\rangle \otimes |1\rangle) &= \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle . \end{aligned}$$

3. The state $|\psi\rangle$ of a single qubit is represented by two angles (θ, φ) on the Bloch sphere:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle$$

   For the basis state $|0\rangle$, we have $\theta = 0$ and $\varphi = 0$. The basis state $|1\rangle$ is represented by the angles $\theta = \pi$ and $\varphi = 0$.

   - Pauli-Y is a rotation of π around the y-axis of the Bloch sphere. Adding π to the polar angle θ maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $\cos(\pi) |0\rangle = -|0\rangle$.
   - Pauli-Z, phase S and $\frac{\pi}{8}$ gate T are rotations of π, $\frac{\pi}{2}$ and $\frac{\pi}{4}$, respectively, around the z-axis. Adding these angles to the azimuth φ leaves $|0\rangle$ invariant and maps $|1\rangle$ to $e^{i\varphi} |1\rangle$.
   - Pauli-X is a rotation of π around the x-axis. This rotation swaps $|0\rangle$ and $|1\rangle$.
   - Hadamard gate H is a rotation of $\frac{\pi}{2}$ around the y-axis, followed by a rotation of π around the x-axis. The rotation around the y-axis maps $|0\rangle$ to

$$\cos\left(\frac{\pi}{2}\right) |0\rangle + \sin\left(\frac{\pi}{2}\right) |1\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle .$$

     $|1\rangle$ is mapped to

$$\cos\left(\frac{3}{4}\pi\right) |0\rangle + \sin\left(\frac{3}{4}\pi\right) |1\rangle = -\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle .$$

The subsequent rotation of π around the x-axis (Pauli-X) swaps the coefficients of $|0\rangle$ and $|1\rangle$. This gives $H|0\rangle$ and $H|1\rangle$, respectively.

4. We map a state $|\psi\rangle = a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$ to the projective point $[a : b] \in \mathbb{P}^1(\mathbb{C})$. First, the map is well defined, since changing the state by a global phase $\lambda = e^{i\gamma}$ gives an equivalent point $[\lambda a : \lambda b] \sim [a : b]$.

   Next, we prove that the map is injective. Suppose two states $a|0\rangle + b|1\rangle$ and $a'|0\rangle + b'|1\rangle$ have the same image in $\mathbb{P}^1(\mathbb{C})$. Then $a' = \lambda a$ and $b' = \lambda b$ for $\lambda \in \mathbb{C}^*$. The state $\lambda a|0\rangle + \lambda b|1\rangle$ satisfies $|\lambda a|^2 + |\lambda b|^2 = 1$, and therefore $|\lambda| = 1$. We see that λ is a global phase which is unimportant for the state.

   Finally, the map is surjective since projective coordinates $[a : b] \in \mathbb{P}^1(\mathbb{C})$ can be scaled such that $|a|^2 + |b|^2 = 1$.

5. Apply $H \otimes H$ to the basis states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ and write the coefficients into the columns of a 4×4 matrix. The result is

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

6. Apply the transformation $U_f(|x_1, x_2, y\rangle) = |x_1, x_2, y \oplus x_1 x_2\rangle$ to the eight basis states $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$ and write the coefficients into the columns of a 8×8 matrix. This gives

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

7. The Toffoli gate can implement the classical NAND gate. Note that

$$NAND(x_1, x_2) = 1 \oplus x_1 x_2.$$

   Suppose the first two input qubits are in basis state $|x_1\rangle$ and $|x_2\rangle$. If the third input qubit is prepared in the state $|1\rangle$, then the third output qubit is $|1 \oplus x_1 x_2\rangle$.

8. We prove the formula by induction. For $n = 1$, we have

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle),$$

i.e., the sign is + if $x = 0$, and − if $x = 1$. Now let $X = (x,\ x_{n+1}) \in \{0,1\}^{n+1}$ with $x \in \{0,1\}^n$. We use the hypothesis and compute

$$\begin{aligned} H^{\otimes(n+1)} |X\rangle &= H^{\otimes n} |x\rangle \otimes H |x_{n+1}\rangle \\ &= \left(\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} |z\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_{n+1}} |1\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} |z,0\rangle + (-1)^{x\cdot z + x_{n+1}} |z,1\rangle \right) \\ &= \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{Z\in\{0,1\}^{n+1}} (-1)^{X\cdot Z} |Z\rangle \right). \end{aligned}$$

9. For $n = 1$, i.e., $N = 2$, we have

$$U(a_0 |0\rangle + a_1 |1\rangle) = \frac{1}{\sqrt{2}} \left((a_0 + a_1) |0\rangle + (a_0 - a_1) |1\rangle \right).$$

The QFT is identical to the H operator. Now let $n = 2$, i.e., $N = 4$. Then $\omega = e^{2\pi i/4} = i$ and the QFT is given by the 4×4 matrix

$$U = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & 1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

Note that the QFT matrix is conjugate to the corresponding DFT matrix. Here is an explicit description:

$$\begin{aligned} U(a_0 |0\rangle + a_1 |1\rangle + a_2 |2\rangle + a_3 |3\rangle) = &\frac{1}{2} (a_0 + a_1 + a_2 + a_3) |0\rangle \\ &+ \frac{1}{2} (a_0 + i\, a_1 - a_2 - i\, a_3) |1\rangle \\ &+ \frac{1}{2} (a_0 - a_1 + a_2 - a_3) |2\rangle \\ &+ \frac{1}{2} (a_0 - i\, a_1 - a_2 + i\, a_3) |3\rangle \end{aligned}$$

We write $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ instead of $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. A basis state $|x\rangle$ is transformed into

$$U |x\rangle = \frac{1}{2} |00\rangle + \frac{1}{2} i^x |01\rangle + \frac{1}{2} i^{2x} |10\rangle + \frac{1}{2} i^{3x} |11\rangle.$$

The sum has a product representation:

$$\begin{aligned} U |x\rangle &= \frac{1}{2} \left(|0\rangle + i^{2x} |1\rangle \right) \otimes (|0\rangle + i^x |1\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_2} |1\rangle) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + i^{2x_1 + x_2} |1\rangle \right) \\ &= \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_2} |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1}\, i^{x_2} |1\rangle), \end{aligned}$$

where x is represented by the binary pair (x_1, x_2) with $x = 2x_1 + x_2$. For a circuit of the 2-qubit QFT, we swap the above factors:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1} i^{x_2} |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_2} |1\rangle\right)$$

This can be implemented by the quantum circuit depicted in Figure 2, where qubits need to be swapped at the end, i.e., the coefficients of $|01\rangle$ and $|10\rangle$ are swapped.

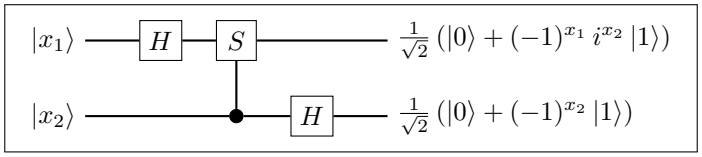

Figure 2. Circuit of the QFT for two qubits. The circuits uses two Hadamard gates and one controlled phase gate. The swap gates at the end of the circuit are not shown.

10. We have $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Let $a \in \mathbb{Z}_n^*$. Then $a^s \equiv 1 \bmod n$ if and only if $a^s \equiv 1 \bmod p$ and $a^s \equiv 1 \bmod q$. It follows that $r_p \mid r$ and $r_q \mid r$, and so r is a multiple of r_p and r_q. Furthermore, any common multiple of r_p and r_q is a multiple of r. This shows that r is the least common multiple of r_p and r_q.
11. Let $r = \operatorname{ord}(a) = 7770$. We compute

$$\gcd(a^{r/2} + 1,\, n) = \gcd(11^{3885} + 1,\, 47053) = \gcd(39248,\, 47053) = 223$$

Indeed, the factors of $n = 47053$ are $p = 223$ and $q = 211$. The method works since $r_p = 222$ is even and $r_q = 35$ is odd.
12. Mallory has a 50% chance of choosing the correct basis. If the basis is wrong, then he has a 50% chance of measuring the original key bit. Hence his error rate is 25%, and this is also the minimum error rate resulting from his intervention. The expected number of faulty bits is $\frac{m}{4}$.
13. $4n + \delta = 8320$ bits are transmitted and Mallory intercepts 64 bits. The fraction of intercepted bits is $\frac{64}{8320}$. Since $n = 2048$ check bits are selected, Mallory has intercepted around $2048 \cdot \frac{64}{8320} \approx 15.8$ check bits. His intervention generates an error rate of 25% and thus about 4 check bits will be faulty, if no other transmission errors or manipulations occur.