Qiskit Fall Fest 2025: Malaysia

Hosts: Lee Chang Xin[3], Choong Pak Shen[1,5]
Advisors: Vannajan Sanghiran Lee[1,2], Nurisya Mohd Shah[1,4,5]

[1]Malaysia Quantum Information Initiative (MyQI)
[2]CoE Quantum Information Science and Technology (QIST), Universiti Malaya
[3]Department of Physics, Universiti Malaya
[4]Department of Physics, Universiti Putra Malaysia
[5]Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia

October 30, 2025

Universiti Malaya student team

1. Mok Zhen Yang
2. Chee Tian Hou
3. Tan Kai Zhe
4. Errol Tay Lee Han
5. Tan Yee Tern
6. Tee Hui En

Universiti Putra Malaysia student team

1. Ain Nabihah Mohd Padaliah
2. Nur Ainin Sabrina Nor Efandi
3. Ricardo André González Gómez
4. Nur Amirah Hafizah Abdul Wahab
5. Nurul Aisyah Azhar

Workshop on quantum algorithms

Timetable

Day 1	**30 October 2025**
0800 - 0900	Registration
0900 - 1200	Introduction to quantum information and quantum computing
1200 - 1330	Lunch break
1330 - 1630	Deutsch-Jozsa algorithm
Day 2	**31 October 2025**
0900 - 1200	Shor's algorithm
1200 - 1500	Lunch break and prayer time
1500 - 1545	Yap Yung Szen: Control System for Superconducting Quantum Computers
1545 - 1630	Tomasz Paterek: Quantum Reservoir Processing: NISQ AI

Introduction to quantum information and computing

9.00am - 12.00pm GMT+8, 30 October 2025

Quantum computing

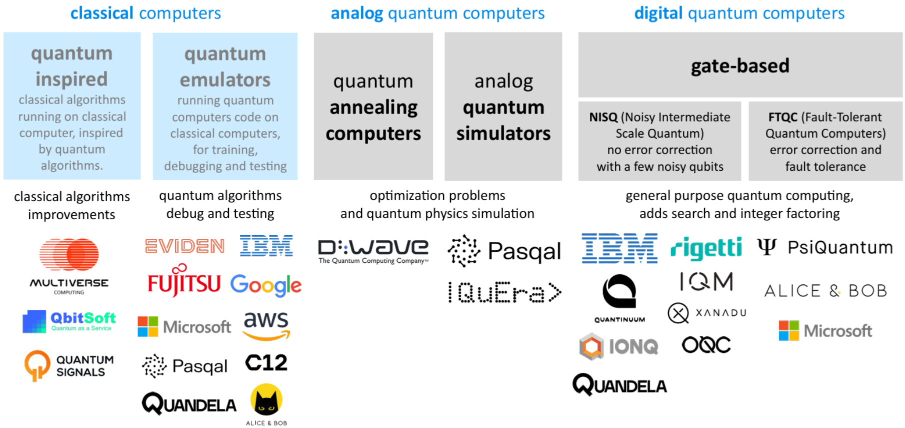


Figure 1: Different computing paradigms with quantum systems, hybrid systems and classical systems (Ezratty, 2025).

Quantum emulator

1. Classical software and hardware that can execute quantum algorithms which are designed to run on quantum computers.
2. This terminology coincides with the classical view of an emulator, which runs some software code on one machine that was designed for older hardware.

Quantum simulator

1. Quantum computing system that is used to simulate low temperature physics and many-body quantum physics, as envisioned by Richard Feynman.

Quantum-inspired algorithm

1. Classical algorithm that runs on classical hardware with new efficiencies inspired by quantum algorithm.

Quantum algorithm

1. Algorithm that runs on a realistic quantum computer and uses some essential quantum phenomena.

NISQ algorithm

1. Quantum algorithm that is designed for quantum processors in the noisy intermediate-scale quantum (NISQ) era.
2. Usually, some calculations are offloaded to classical processors.

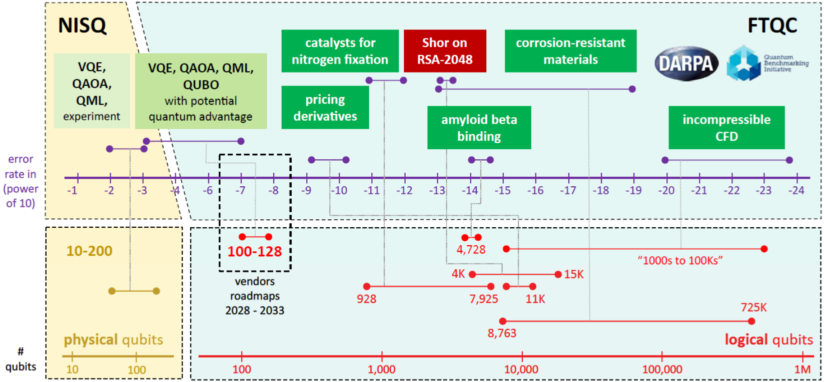


Figure 2: Algorithmic-level resource estimates for key algorithms which have some industry relevance (Ezratty, 2025).

Quantum communication

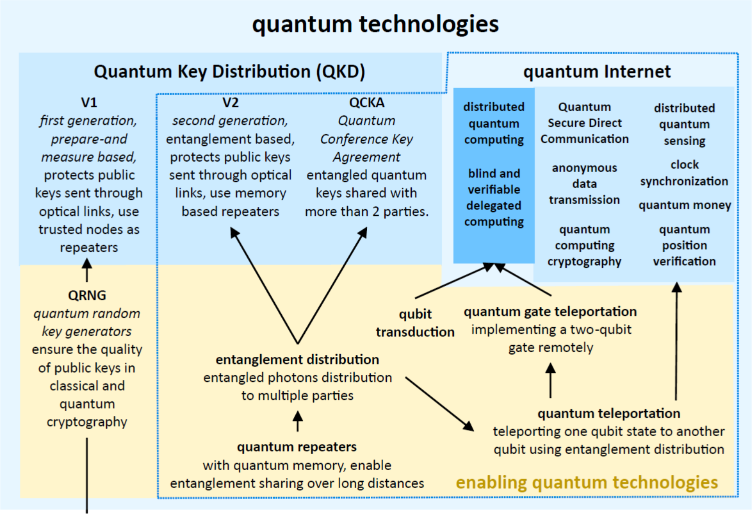


Figure 3: Various types of quantum communication and cybersecurity technologies (quantum) (Ezratty, 2025).

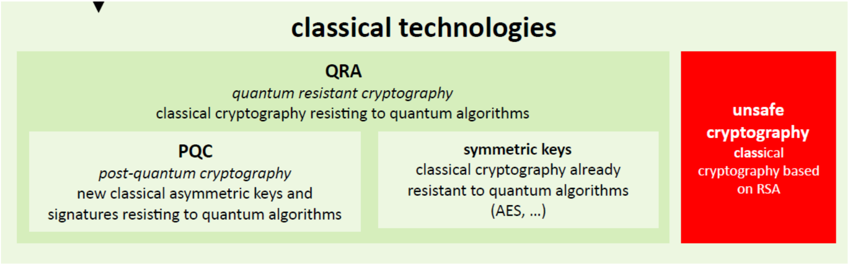


Figure 4: Various types of quantum communication and cybersecurity technologies (classical) (Ezratty, 2025).

Quantum key distribution: BB84

1. Alice creates a random bit (0 or 1) and randomly selects one of her two basis sets, ($Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$) to transmit her information to Bob using the quantum channel.
2. This process is repeated with Alice recording the state, basis and time of each photon sent.
3. As Bob does not know the basis the photons were encoded in, he randomly selects a basis (Z or X) to measure. He does this for each photon he receives, recording the time, measurement basis used and result.
4. After Bob has measured the photons, Alice broadcasts the basis each photon was in, and Bob broadcasts the basis each photon was being measured.
5. They discard the photons where Bob used a different basis (half on average).
6. If more than p bits differ, they abort the key and try again with a different quantum channel.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random qubit	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's random measuring basis	Z	X	X	X	Z	X	Z	Z
Bob's result	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$
Shared secret key	0		1			0		1

Table 1: Example of BB84.

Quantum sensing

Quantum sensing[1] is typically used to describe one of the followings:

1. Use of a quantum object to measure a physical quantity (classical or quantum). The quantum object is characterized by quantized energy levels.
2. Use of quantum coherence (wave-like spatial or temporal superposition states) to measure a physical quantity.
3. Use of quantum entanglement to improve the sensitivity or precision of a measurement, beyond what is possible classically.

[1] Degen, Reinhard & Cappellaro. Quantum sensing. Rev. Mod. Phys. 89, 035002, 2017.

In analogy to DiVincenzo criteria for quantum computing, a set of attributes for quantum sensing can be defined:

1. The quantum system has discrete, resolvable energy levels.
2. It must be possible to initialize the quantum system into a well-known state and to read out its state.
3. The quantum system can be coherently manipulated, typically by time-dependent fields.
4. The quantum system interacts with a relevant physical quantity, quantified by a coupling parameter, and will lead to a shift of the quantum system's energy levels or to transition between energy levels.

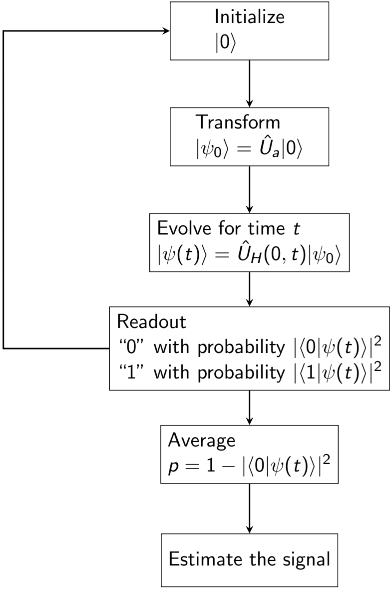
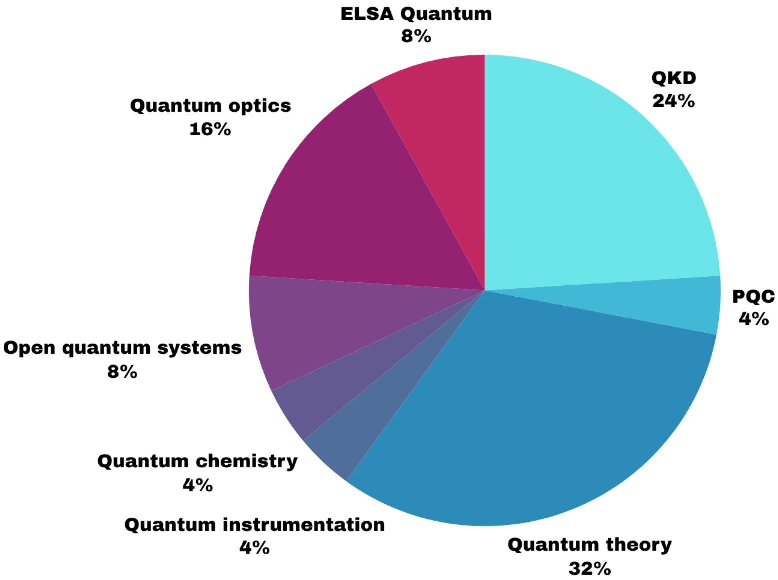


Figure 5: Basic steps of the quantum sensing process.

Malaysia's quantum research landscape



Classical bits

Imagine an unfair coin. The probability of getting a head is $P(C = H) = p$, the probability of getting a tail is $P(C = T) = 1 - p$.

It can be represented as a probability table:

	$P(C)$
H	p
T	$1 - p$

More compactly, one can represent it as a column matrix,

$$\begin{aligned} P(C) &= \begin{pmatrix} p \\ 1 - p \end{pmatrix} \\ &= p \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (1 - p) \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned} \tag{1}$$

If we want to transform into different physical systems with different probability vectors, we can apply stochastic matrices on the probability vectors. A stochastic matrix S satisfies the following conditions to preserve the properties of probability vectors:

1. Every matrix elements are non-negative;
2. The sum of every matrix elements in a column is equals to 1.

The matrix element S_{ij} represents the probability of moving from i to j, $P(j|i)$.

Example of a 2×2 stochastic matrix $S = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$, where $0 \leq p \leq 1$.

Consider two independent events, for example two coin tosses C_1 and C_2. The probability table of C_1 and C_2 can be given as follow.

	$P(C_1)$
H	p
T	$1-p$

	$P(C_2)$
H	q
T	$1-q$

The combined probability table of two coin tosses can be given as follows.

	$P(C_1 C_2)$
HH	pq
HT	$p(1-q)$
TH	$(1-p)q$
TT	$(1-p)(1-q)$

Or, written as a probability vector,

$$P(C_1 C_2) = \begin{pmatrix} pq \\ p(1-q) \\ (1-p)q \\ (1-p)(1-q) \end{pmatrix}. \tag{2}$$

Since C_1 and C_2 are independent events, $P(C_1|C_2) = P(C_1)$ and $P(C_2|C_1) = P(C_2)$, i.e. the outcome of event C_1 (C_2) is independent of event C_2 (C_1).

Also, note that $P(HH) \times P(TT) = P(HT) \times P(TH)$.

In other words, if C_1 and C_2 are not independent events, then $P(HH) \times P(TT) \neq P(HT) \times P(TH)$. C_1 and C_2 are correlated in this scenario.

One example of dependent events is drawing two cards from a deck without replacement.

We denote the symbol $i = \sqrt{-1}$ with the understanding that $i^2 = -1$ to represent imaginary unit.

Any constant c multiplying with the imaginary unit is called imaginary number. For example, $12i$.

The combination of real and imaginary number is called complex number.

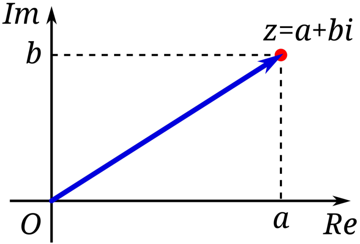


Figure 6: Argand diagram

The rectangular form, $z = a + bi$, can be rewritten into the polar form,

$$z = a + bi = r(\cos\theta + i\sin\theta) = re^{i\theta}. \tag{3}$$

Note that $Re(z) = a$ and $Im(z) = b$.

The complex conjugate of z is defined as $\bar{z} = a - bi = re^{-i\theta}$.

The modulus or absolute value of z is defined as $|z| = r = \sqrt{a^2 + b^2}$.

Hence, $|z| = \sqrt{z\bar{z}}$.

Linear algebra

A vector can be seen as a geometric entity (arrow in a coordinate system) or a set of numbers, with components relative to a coordinate system. Mathematically, a vector can be represented as a column matrix. For a two-dimensional vector $\vec{v}$,

$$\begin{aligned} \vec{v} &= \begin{pmatrix} x \\ y \end{pmatrix} && (4) \\ &= x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} && (5) \\ &= x\vec{e}_x + y\vec{e}_y && (6) \end{aligned}$$

We call $\vec{e}_x$ and $\vec{e}_y$ as the unit vectors along x and y directions respectively.

For complex vector spaces, x and y are complex numbers.

The conjugate transpose operation of a vector $\vec{v}$ is denoted by the dagger symbol $\dagger$ and defined by

$$\vec{v}^\dagger = \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \tag{7}$$

The inner product is defined as the multiplication between $\vec{v}^\dagger$ and $\vec{v}$, i.e.

$$\begin{aligned} \vec{v}^\dagger \vec{v} &= \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= |x|^2 + |y|^2 \end{aligned} \tag{8}$$

The outer product (or tensor product) is defined as the multiplication between $\vec{v}$ and $\vec{v}^\dagger$, i.e.

$$\begin{aligned} \vec{v} \otimes \vec{v}^\dagger &= \begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \\ &= \begin{pmatrix} |x|^2 & x\bar{y} \\ \bar{x}y & |y|^2 \end{pmatrix} \end{aligned} \tag{9}$$

More generally, tensor product is done with Kronecker product operation. For example,

$$\begin{aligned} \vec{v} \otimes \vec{v}^{\dagger} &= \begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \\ &= \begin{pmatrix} x \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \\ y \begin{pmatrix} \bar{x} & \bar{y} \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} |x|^2 & x\bar{y} \\ \bar{x}y & |y|^2 \end{pmatrix} \end{aligned}$$

Kronecker product is not the same as matrix multiplication. For example,

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} &= \begin{pmatrix} a \begin{pmatrix} e & f \\ g & h \end{pmatrix} & b \begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ c \begin{pmatrix} e & f \\ g & h \end{pmatrix} & d \begin{pmatrix} e & f \\ g & h \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix} \end{aligned}$$

Consider a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with complex entries.

The transpose of a matrix A is given as

$$A^T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \quad (10)$$

A Hermitian matrix is defined as $A = (\bar{A})^T = A^\dagger$.

The inverse matrix of A is written as A^{-1}.

The matrix multiplication between a matrix with its inverse, $AA^{-1} = A^{-1}A = I$, where I is the identity matrix.

A unitary matrix is defined as $A^\dagger = A^{-1}$.

Quantum bits

We use a different notation for vectors. Let $|\psi\rangle$ be a vector in complex vector space $\mathbb{C}^2$,

$$|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle \tag{11}$$

$$= \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} \tag{12}$$

, where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, ψ_0 and ψ_1 are complex numbers called probability amplitudes.

$|\psi\rangle$ is called a ket vector. The dual is a bra vector,

$$\langle\psi| = \bar{\psi}_0\langle 0| + \bar{\psi}_1\langle 1| \tag{13}$$

$$= \begin{pmatrix} \bar{\psi}_0 & \bar{\psi}_1 \end{pmatrix} \tag{14}$$

, where $\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$ and $\langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$.

The probability of getting $|0\rangle$ is $|\psi_0|^2$, while the probability of getting $|1\rangle$ is $|\psi_1|^2$. Therefore,

$$|\psi_0|^2 + |\psi_1|^2 = \langle\psi|\psi\rangle = 1. \tag{15}$$

There are three orthonormal basis sets:

1. Z-basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
2. X-basis: $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
3. Y-basis: $|+i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$, $|-i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$

We use tensor product to describe composite quantum systems. For two qubits A and B, $|\psi\rangle$ and $|\phi\rangle$, the quantum state becomes

$$\begin{aligned}
|\Psi_{AB}\rangle &= |\psi\rangle \otimes |\phi\rangle \\
&= (\psi_0|0_A\rangle + \psi_1|1_A\rangle) \otimes (\phi_0|0_B\rangle + \phi_1|1_B\rangle) \\
&= \psi_0\phi_0|0_A\rangle \otimes |0_B\rangle + \psi_0\phi_1|0_A\rangle \otimes |1_B\rangle + \psi_1\phi_0|1_A\rangle \otimes |0_B\rangle \\
&\quad + \psi_1\phi_1|1_A\rangle \otimes |1_B\rangle \\
&= \psi_0\phi_0|00\rangle + \psi_0\phi_1|01\rangle + \psi_1\phi_0|10\rangle + \psi_1\phi_1|11\rangle && (16) \\
&= \begin{pmatrix} \psi_0\phi_0 \\ \psi_0\phi_1 \\ \psi_1\phi_0 \\ \psi_1\phi_1 \end{pmatrix} && (17)
\end{aligned}$$

In general, a two-qubit state can be written as

$$|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle. \tag{18}$$

Similarly, if $\psi_{00}\psi_{11} = \psi_{01}\psi_{10}$, the two-qubit state is separable. Otherwise, the two-qubit state is entangled.

Quantum gates

Quantum circuit reads from left to right. There are several common quantum gates:-

Pauli $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, equivalently the NOT (bit-flip) gate $-\boxed{X}-$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \tag{19}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{20}$$

Pauli $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, equivalently the phase-flip gate $-\boxed{Z}-$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{21}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle \tag{22}$$

Pauli $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, a combination of Pauli X and Z gates $\;-\!\boxed{Y}\!-$

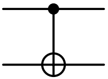
$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} |0\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle \tag{23}$$

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -i \begin{pmatrix} 1 \\ 0 \end{pmatrix} = -i|0\rangle \tag{24}$$

Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\;-\!\boxed{H}\!-$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle \tag{25}$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \tag{26}$$

CNOT gate 

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{27}$$

$$CNOT|00\rangle = |00\rangle \tag{28}$$
$$CNOT|01\rangle = |01\rangle \tag{29}$$
$$CNOT|10\rangle = |11\rangle \tag{30}$$
$$CNOT|11\rangle = |10\rangle \tag{31}$$

Deutsch-Jozsa algorithm

1.30pm - 4.30pm GMT+8, 30 October 2025

Constant and balanced functions

Let f be a function that maps the set $\{0,1\}$ into the set $\{0,1\}$, $f : \{0,1\} \to \{0,1\}$. There are two possibilities.
A constant function gives the same output regardless of the input, i.e. $f(0) = f(1)$.
A balanced function gives an equal number of 0 and 1 as output, i.e. $f(0) \neq f(1)$.

x	$f_0(x)$	$f_1(x)$
0	0	1
1	0	1

Table 2: Constant function

x	$f_2(x)$	$f_3(x)$
0	1	0
1	0	1

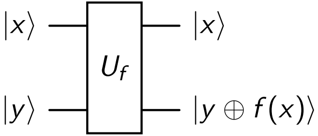
Table 3: Balanced function

Quantum oracle

A quantum oracle is a black-box that evaluates a function f. it is often represented as a unitary transformation U_f that acts on a bipartite system,

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle, \tag{32}$$

where $\oplus$ denotes addition modulo 2.



$|x\rangle$ is called the input state, $|y\rangle$ is called the ancillary state.
Show that

$$U_f^2|x\rangle|y\rangle = |x\rangle|y\rangle. \tag{33}$$

State preparation

$$
\begin{aligned}
H \otimes H|00\rangle &= |++\rangle \\
&= \left(\frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]\right) \otimes \left(\frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]\right) \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2^2}} \sum_{x \in \{0,1\}^2} |x\rangle
\end{aligned}
$$

Here, $\{0,1\}^2 = \{00, 01, 10, 11\}$.
In general,

$$
H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle. \tag{34}
$$

Modulo 2 arithmetic

Modulo 2 addition, $\oplus$, is also known as the XOR operation, with the following truth table:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

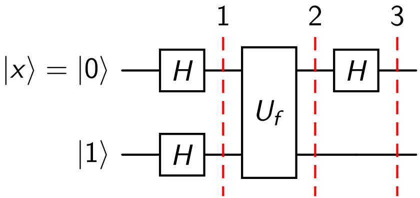
Table 4: Truth table of XOR

Let c be either 0 or 1. Find $0 \oplus c$.

Let $c_0 = 0$, $c_1 = 1$. Find $1 \oplus c_0$ and $1 \oplus c_1$. Will the result change if $c_0 = 1$, $c_1 = 0$?

Deutsch algorithm

Consider the following circuit.



Note that $|1\rangle = X|0\rangle$. For simplification, we initiate the two-qubit state as $|0\rangle|1\rangle$. At Step 1,

$$H \otimes H|0\rangle|1\rangle = |+\rangle|-\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{35}$$

At Step 2,

$$U_f \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right)$$
$$= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \quad (36)$$

Regardless of the value of x, if $f(x) = 0$, then

$$\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

If $f(x) = 1$, then

$$\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Combining both cases, we have

$$\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Hence, we can rewrite Equation (36) as

$$\begin{aligned}
&\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right) \\
&= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left[(-1)^{f(x)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] \\
&= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle|0\rangle - (-1)^{f(0)}|0\rangle|1\rangle + (-1)^{f(1)}|1\rangle|0\rangle - (-1)^{f(1)}|1\rangle|1\rangle\Big) \\
&= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad (37)
\end{aligned}$$

At Step 3, we apply a Hadamard gate on the first qubit, $|x\rangle$, from Equation (37),

$$
\begin{aligned}
& H \otimes I \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \left(\frac{(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)}{2} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \left(\frac{[(-1)^{f(0)} + (-1)^{f(1)}]|0\rangle + [(-1)^{f(0)} - (-1)^{f(1)}]|1\rangle}{2} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)
\end{aligned}
\tag{38}
$$

If f is a constant function, i.e. $f(0) = f(1)$, Equation (38) becomes

$$
\pm|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{39}
$$

If f is a balanced function, i.e. $f(0) \neq f(1)$, Equation (38) becomes

$$
\pm|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{40}
$$

Before we go into Deutsch-Jozsa algorithm, it is useful to know that

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|y\rangle, \tag{41}$$

where $x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_n y_n$.

For one qubit,

$$H|0\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{0\cdot y}|y\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right),$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{1\cdot y}|y\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right).$$

Example: Find $H^{\otimes 2}|10\rangle$.

Using Equation (41), we can rewrite Equation (38) as follow:

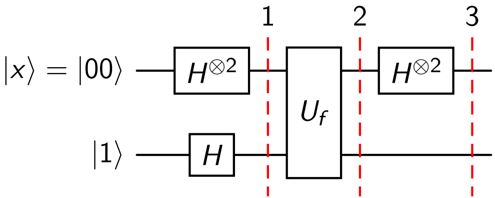
$$
\begin{aligned}
&H \otimes I \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{\sqrt{2}} H \otimes I \left(\sum_{x=0}^{1} (-1)^{f(x)} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{2} \left(\sum_{x=0}^{1} (-1)^{f(x)} \sum_{y=0}^{1} (-1)^{x \cdot y} |y\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{2} \left(\sum_{x=0}^{1} \sum_{y=0}^{1} (-1)^{f(x) + x \cdot y} |y\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \qquad (42)
\end{aligned}
$$

Verify that Equation (42) can be expanded into Equation (38), provided as follow:

$$
\left(\frac{[(-1)^{f(0)} + (-1)^{f(1)}]|0\rangle + [(-1)^{f(0)} - (-1)^{f(1)}]|1\rangle}{2} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)
$$

Deutsch-Jozsa algorithm

Consider the following example circuit.



The three-qubit state is initiated as $|00\rangle|1\rangle$. At Step 1,

$$H^{\otimes 2} \otimes H|00\rangle|1\rangle = \left(\frac{1}{2} \sum_{x \in \{0,1\}^2} |x\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{43}$$

At Step 2,

$$U_f\left(\frac{1}{2}\sum_{x\in\{0,1\}^2}|x\rangle\right)\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$
$$=\left(\frac{1}{2}\sum_{x\in\{0,1\}^2}(-1)^{f(x)}|x\rangle\right)\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \tag{44}$$

We know from Deutsch algorithm that the ancillary qubit is not important. Hence, we can focus only on the input state during Step 3.

At Step 3,

$$
\begin{aligned}
&H \otimes H \left(\frac{1}{2} \sum_{x \in \{0,1\}^2} (-1)^{f(x)} |x\rangle \right) \\
&= \frac{1}{2} H \otimes H \Big((-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle \Big) \\
&= \frac{1}{2} \Big((-1)^{f(00)}|++\rangle + (-1)^{f(01)}|+-\rangle + (-1)^{f(10)}|-+\rangle \\
&\qquad + (-1)^{f(11)}|--\rangle \Big) \\
&= \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) \Big((-1)^{f(00)}[|00\rangle + |01\rangle + |10\rangle + |11\rangle] \\
&\qquad + (-1)^{f(01)}[|00\rangle - |01\rangle + |10\rangle - |11\rangle] \\
&\qquad + (-1)^{f(10)}[|00\rangle + |01\rangle - |10\rangle - |11\rangle] \\
&\qquad + (-1)^{f(11)}[|00\rangle - |01\rangle - |10\rangle + |11\rangle] \Big)
\end{aligned} \tag{45}
$$

Verify that the following simplification can be expanded into Equation (45).

$$
\begin{aligned}
&\frac{1}{2^2}\left(\sum_{x\in\{0,1\}^2}\sum_{y\in\{0,1\}^2}(-1)^{f(x)+x\cdot y}|y\rangle\right)\\
&=\frac{1}{4}\Big([(-1)^{f(00)}+(-1)^{f(01)}+(-1)^{f(10)}+(-1)^{f(11)}]|00\rangle\\
&\quad+[(-1)^{f(00)}-(-1)^{f(01)}+(-1)^{f(10)}-(-1)^{f(11)}]|01\rangle\\
&\quad+[(-1)^{f(00)}+(-1)^{f(01)}-(-1)^{f(10)}-(-1)^{f(11)}]|10\rangle\\
&\quad+[(-1)^{f(00)}-(-1)^{f(01)}-(-1)^{f(10)}+(-1)^{f(11)}]|11\rangle\Big)
\end{aligned}
$$

If the function is constant, due to the constructive interference for $|00\rangle$, the probability of getting $|00\rangle$ is 1.

If the function is balanced, due to the destructive interference for $|00\rangle$, the probability of getting $|00\rangle$ is 0.

Shor's algorithm

9.00am - 12.00pm GMT+8, 31 October 2025

Eigenvalues and eigenvectors

Let $|\psi\rangle$ be a vector. An eigenvector is a vector that remains unchanged under a linear transformation. For a unitary transformation U, the eigenequation is given by

$$U|\psi\rangle = e^{2\pi i\omega}|\psi\rangle, \tag{46}$$

where $e^{2\pi i\omega}$ is the eigenvalue of the unitary transformation. ω is the phase of the eigenvalue.

Binary fraction

The decimal fraction allows us to express rational numbers as a fraction whose denominator is a power of ten. For example,

$$0.15625 = 1 \times 10^{-1} + 5 \times 10^{-2} + 6 \times 10^{-3} + 2 \times 10^{-4} + 5 \times 10^{-5}.$$

Similarly, the binary fraction allows us to represent the above rational number as a fraction whose denominator is a power of two,

$$0.00101 = 0 \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3} + 0 \times 2^{-4} + 1 \times 2^{-5}.$$

A binary representation is useful because we can encode it using qubits.

Modular exponentiation

Modular exponentiation is exponentiation performed over a modulus,

$$c = b^e \bmod m. \tag{47}$$

Example: Given $b = 4$, $e = 13$, $m = 497$, calculate c.

Note that b is only one digit, e is two digits, but the value b^e is eight digits in length.

While it is efficient to compute even for very large integers, it is difficult to compute e when given b, c, m. This is a one-way function suitable for cryptographic purposes.

Quantum Fourier Transform (qFT) can be thought of as a unitary transformation with the following unitary matrix,

$$\hat{U}_{qFT} = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} e^{\frac{2\pi ijk}{N}} |j\rangle\langle k|, \tag{48}$$

where $N = 2^n$.

Example: Let $\omega = e^{\frac{2\pi i}{N}}$. Write down the unitary matrix $\hat{U}_{qFT}$ for $N = 2^2 = 4$.

$\hat{U}_{qFT}$ acts on a quantum state $|x\rangle = \sum_{k=0}^{N-1} x_k |k\rangle$ and maps it to $|y\rangle = \sum_{j=0}^{N-1} y_j |j\rangle$, where

$$y_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi ijk}{N}} x_k. \tag{49}$$

For a single qubit, $n = 1$. $\hat{U}_{qFT}$ becomes

$$\begin{aligned}
\hat{U}_{qFT} &= \frac{1}{\sqrt{2}} \sum_{j,k=0}^{1} e^{\pi ijk} |j\rangle\langle k| \\
&= \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + e^{\pi i} |1\rangle\langle 1|) \\
&= \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)
\end{aligned}$$

Therefore,

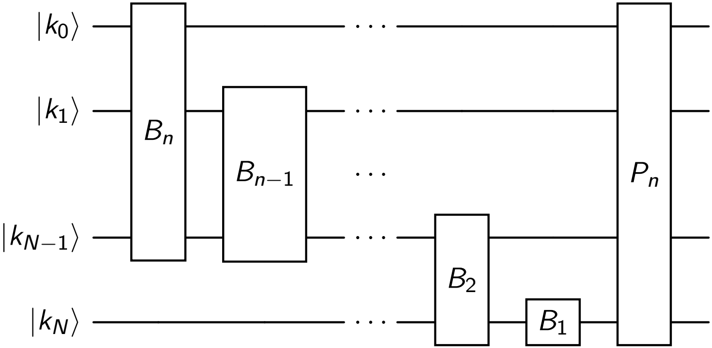
$$\begin{aligned}\hat{U}_{qFT}|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle,\end{aligned}$$

$$\begin{aligned}\hat{U}_{qFT}|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle,\end{aligned}$$

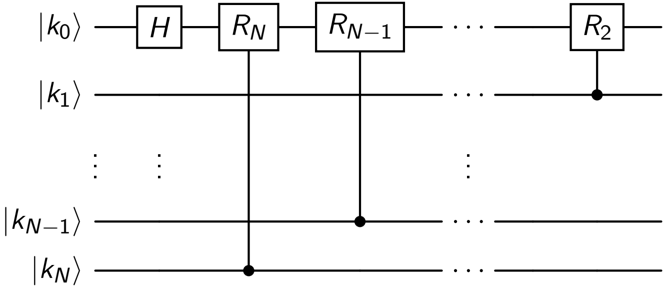
Example: Identify the general form of qFT for two qubits based on Equation (48). Hence, find the qFT of $|00\rangle$ and $|01\rangle$.

Since qFT is a unitary transformation, there exists an inverse qFT that maps $|y\rangle$ into $|x\rangle$.

In general, the qFT circuit looks like



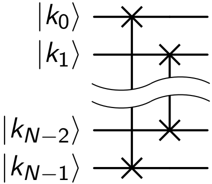
The gate $-\boxed{B_n}-$ means



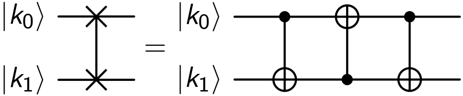
where $-\boxed{R_n}-$ is the unitary rotation,

$$R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{pmatrix} . \tag{50}$$

The gate $-\boxed{P_n}-$ means a set of permutations of (i)-th qubit to $(N - i - 1)$-th qubit,

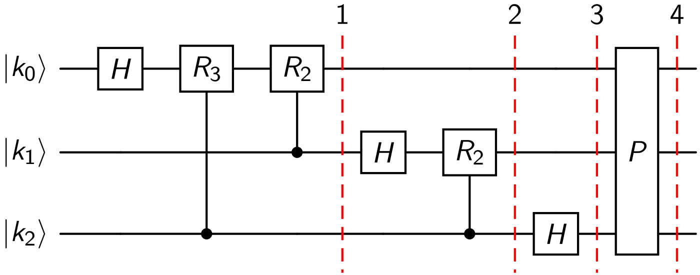


where the permutation between two qubits can be executed through 3 CNOT gates,



Note that the permutation P_n depends on how the hardware orders the qubits and sometimes it is not necessary to perform P_n.

Example: Three-qubit quantum Fourier transform



The rotation matrices are given by

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^2}} \end{pmatrix}, \; R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^3}} \end{pmatrix}.$$

We note that

$$
\begin{aligned}
H|k_j\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{k_j}|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{\pi i})^{k_j}|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{\pi i k_j})|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i \frac{k_j}{2}})|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i [0.k_j]})|1\rangle\right) \qquad (51)
\end{aligned}
$$

Also,

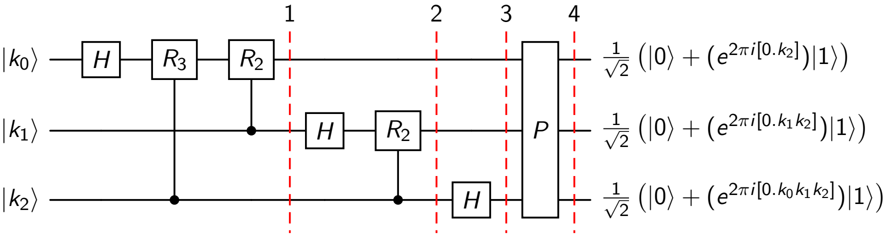
$$R_n|0\rangle = |0\rangle, \qquad (52)$$

$$R_n|1\rangle = e^{\frac{2\pi i}{2^n}}|1\rangle. \qquad (53)$$

We can view each step from the example as the consequence of the B_n gates. If we understand how B_n works, we can generalize for every B_n gates. For step 1,

$$
\begin{aligned}
|k_0\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0]})|1\rangle\right) \\
&\xrightarrow{C-R_3} \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0]}e^{2\pi i\frac{k_2}{2^3}})|1\rangle\right) \\
&\xrightarrow{C-R_2} \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0]}e^{2\pi i\frac{k_2}{2^3}}e^{2\pi i\frac{k_1}{2^2}})|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0]}e^{2\pi i[0.00k_2]}e^{2\pi i[0.0k_1]})|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0k_1k_2]})|1\rangle\right)
\end{aligned}
$$

Hence,


1
2
3
4
$|k_0\rangle$
$|k_1\rangle$
$|k_2\rangle$
H
R_3
R_2
H
R_2
H
P
$\frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_2]})|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_1 k_2]})|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + (e^{2\pi i[0.k_0 k_1 k_2]})|1\rangle\right)$

Quantum phase estimation

The purpose of quantum phase estimation is to estimate the eigenvalue $e^{2\pi i\omega}$ of a unitary operator,

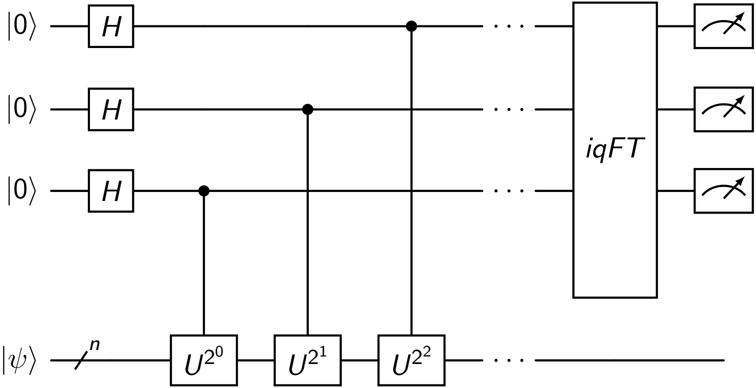
$$U|\psi\rangle = e^{2\pi i\omega}|\psi\rangle, \tag{54}$$

by preparing a quantum circuit to transform

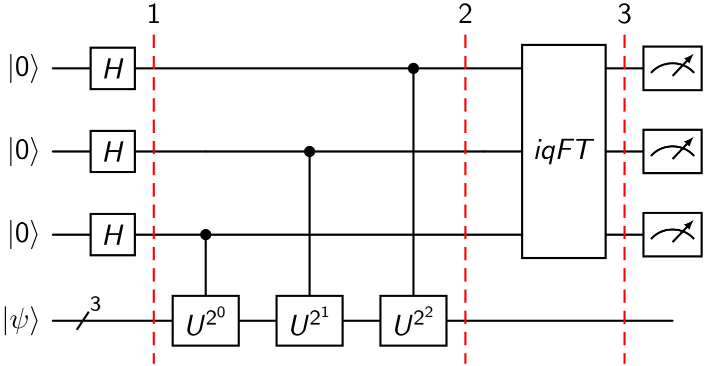
$$|\psi\rangle|0\rangle \to |\psi\rangle|\phi\rangle \tag{55}$$

and then obtaining the phase estimation by measuring $|\phi\rangle$.

A general quantum phase estimation algorithm looks like the following:



Example: Three-qubit quantum phase estimation



The unitary matrix U^{2^k} introduces the phase,

$$U^{2^k}|\psi\rangle = e^{2\pi i\omega 2^k}|\psi\rangle. \tag{56}$$

After the first step, we have

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle. \tag{57}$$

At step 2, the first control-U^{2^0} will introduce a phase to $|\psi\rangle$,

$$|+\rangle^{\otimes 2} \otimes \frac{|0\rangle|\psi\rangle + e^{2\pi i[\omega]}|1\rangle|\psi\rangle}{\sqrt{2}} = |+\rangle^{\otimes 2} \otimes \frac{|0\rangle + e^{2\pi i[\omega]}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle. \tag{58}$$

Following the same logic, the final state at step 2 is

$$\frac{|0\rangle + e^{2\pi i[2^2\omega]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[2\omega]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[\omega]}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \tag{59}$$

If we let $\omega = 0.k_0k_1k_2$, then the final state at step 2 becomes

$$\begin{aligned}
&\frac{|0\rangle + e^{2\pi i[2^2\omega]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[2\omega]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[\omega]}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \\
&= \frac{|0\rangle + e^{2\pi i[k_0k_1.k_2]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[k_0.k_1k_2]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[0.k_0k_1k_2]}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle \\
&= \frac{|0\rangle + e^{2\pi i[0.k_2]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[0.k_1k_2]}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i[0.k_0k_1k_2]}|1\rangle}{\sqrt{2}} \otimes |\psi\rangle
\end{aligned} \tag{60}$$

We note that the integers in front of the binary representation in the first equality is ignored in the second equality, because $e^{2\pi ij} = 1$ for any integer j.

This is the quantum Fourier transform that we have seen just now! By applying the inverse quantum Fourier transform, the measurement of the three qubits $|k_0k_1k_2\rangle$ will tell us the phase of $|\psi\rangle$.

Shor's algorithm

To factor $N = pq$, Shor's algorithm performs the following steps:

1. Select any number $1 < a < N$ and find the greatest common divisor (gcd) of a and N.
2. If gcd $\neq 1$, then the it is a nontrivial common factor of a and N, hence we found one of the factors of N, $p = \text{gcd}(a, N)$. The other factor will be $q = \frac{N}{p}$.
3. If gcd $= 1$, we find the period r of $a^r \bmod N$.
4. If r is odd, we go back to step 1 and pick a different a; If $a^{\frac{r}{2}} \bmod N = N - 1$, we go back to step 1 and pick a different a.
5. Now, $a^r = 1 \bmod N$. Subtract 1 from both sides, $a^r - 1 = 0 \bmod N$. This means that $a^r - 1 = kN = kpq$.
6. Factoring the left hand side, we have $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) = kpq$.
7. Hence, $a^{\frac{r}{2}} - 1 = cp$, $a^{\frac{r}{2}} + 1 = dq$. Since each term $a^{\frac{r}{2}} - 1$ and $a^{\frac{r}{2}} + 1$ share a non-trivial factor with $N = pq$, we have thus factored N.

The quantum circuit of Shor's algorithm looks like the following: