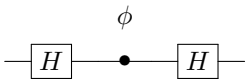
One, two and many qubits

Artur Ekert and Alastair Kay

I. SINGLE QUBIT INTERFERENCE

The optical Mach-Zehnder interferometer is just one way of performing a quantum interference experiment – there are many others. Atoms, molecules, nuclear spins and many other quantum objects can be prepared in two distinct states, internal or external, labelled as 0 and 1 and manipulated so that transition amplitudes between these states are the same as in a beam-splitter or in a phase shifter. However, there is no need to learn these technologies to understand quantum interference. You may conveniently forget about any specific experimental realisation (hardware) and refer to any quantum object with two distinct states labelled 0 and 1 as a quantum bit or a qubit. The interference of a single qubit can then be represented as a sequence of three elementary operations called quantum logic gates. The most common sequence is the Hadamard gate, followed by a phase shift gate, and followed by the Hadamard gate. We can represent it graphically as a network diagram



Quantum network diagrams are read from left to right. The horizontal line represents a quantum wire, which inertly carries a qubit from one quantum operation to another. The wire may describe translation in space, e.g. atoms travelling through cavities, or translation in time, e.g. between operations performed on a trapped ion. If we want to signify that a particular unitary evolution is to be enacted on our qubit, then we put a box with a symbol describing this unitary operation along the quantum wire. Each operation is described by its matrix of transition amplitudes. In particular, the two quantum logic gates shown in the diagram are

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

HADAMARD PHASE

The Hadamard gate plays the same role as a beam-splitter: it prepares an equally weighted superposition of $|0\rangle$ and $|1\rangle$ and it closes the interference by brining the interfering paths together.

All together the network effects the unitary operation

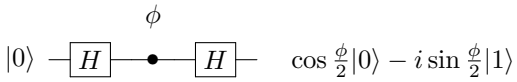
$$\begin{aligned} H\,P_\varphi\,H &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= e^{i\frac{\varphi}{2}}\begin{pmatrix} \cos\varphi/2 & -i\sin\varphi/2 \\ -i\sin\varphi/2 & \cos\varphi/2 \end{pmatrix}. \end{aligned}$$

The phase shift φ effectively controls the evolution and determines the output. The phase matrix $P_\varphi = \mathrm{diag}(1, e^{i\varphi})$ contains only the relative phase. This is because $\mathrm{diag}(e^{i\varphi_0}, e^{i\varphi_1})$ can be written as $e^{i\varphi_0}\mathrm{diag}(1, e^{i\varphi})$ with $\varphi = \varphi_1 - \varphi_0$, and we have already seen that it is the relative phase that really matters.

Given that our input state is almost always $|0\rangle$ it is easier to step through the execution of this network and follow the evolving state.The interference network effects the following sequence of transformations (we have dropped the normalisation factors)

$$\begin{aligned} |0\rangle &\overset{H}{\mapsto} (|0\rangle + |1\rangle) \\ &\overset{\phi}{\mapsto} |0\rangle + e^{i\phi}|1\rangle \\ &\overset{H}{\mapsto} \cos\frac{\phi}{2}|0\rangle - i\sin\frac{\phi}{2}|1\rangle. \end{aligned}$$

We represent the result of the computation performed by the interference network on state $|0\rangle$ as



The probabilities of detecting 0 or 1 are, respectively,

$$P_0(\phi) = \cos^2\frac{\phi}{2}, \quad P_1(\phi) = \sin^2\frac{\phi}{2}$$

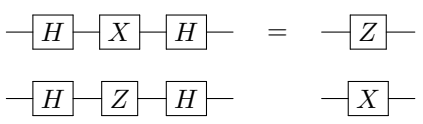
The interference network will be our starting point for discussing quantum algorithms.

II. SINGLE QUBIT GATES

Apart from the HADAMARD and PHASE, the most popular single qubit operations are the PAULI gates, described by the Pauli matrices $\sigma_x \equiv X$, $\sigma_y \equiv Y$, and $\sigma_z \equiv Z$,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Like the Hadamard gate, they square to the identity $X^2 = Y^2 = Z^2 = \mathbb{1}$. The Z gate is a special phase gate with $\varphi = \pi$ and the X gate is the logical NOT gate. The two gates, X and Z, are often referred to as the bit flip and the phase flip respectively. The Hadamard gate can turn the action of the X gate into Z and vice versa;

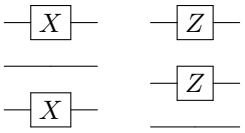


The network HXH is equivalent to the action of single Z and conversely $HZH \equiv X$.

III. QUANTUM REGISTERS

A collection of n qubits is called a *quantum register* of size n. We shall assume that information is stored in the registers in binary form. For example, the number 6 is represented by a register in state $|1\rangle \otimes |1\rangle \otimes |0\rangle$. In more compact notation: $|a\rangle$ stands for the tensor product $|a_{n-1}\rangle \otimes |a_{n-2}\rangle \ldots |a_1\rangle \otimes |a_0\rangle$, where $a_i \in \{0,1\}$, and it represents a quantum register prepared with the value $a = 2^0 a_0 + 2^1 a_1 + \ldots 2^{n-1} a_{n-1}$. There are 2^n states of this kind, representing all binary strings of length n or numbers from 0 to $2^n - 1$, and they form a convenient computational basis. In the following $a \in \{0,1\}^n$ (a is a binary string of length n) implies that $|a\rangle$ belongs to the computational basis.

In addition to the single-qubit Pauli operations, we can also define bit flips and phase flips on selected qubits, X_c and Z_c, where the binary string c indicates the location of the flip, for example $X_{101} = X \otimes \mathbb{1} \otimes X$, $Z_{110} = Z \otimes Z \otimes \mathbb{1}$.



For any x and any constant c in $\{0,1\}^n$ we can express the action of X_c and Z_c as

$$X_c|x\rangle = |x \oplus c\rangle, \quad Z_c|x\rangle = (-1)^{c\cdot x}|x\rangle,$$

where the product of $c = (c_{n-1}, \ldots, c_0)$ and $x = (x_{n-1}, \ldots, x_0)$ is taken bit by bit:

$$c \cdot x = (c_{n-1}x_{n-1} + \ldots c_1 x_1 + c_0 x_0).$$

IV. HADAMARD TRANSFORM

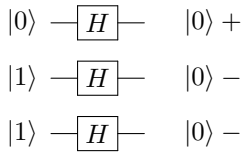
A quantum register of size three can store individual numbers such as 011 and 111,

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \equiv |011\rangle,$$
$$|1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |111\rangle,$$

but, it can also store the two of them simultaneously. For if we take the first qubit and instead of setting it to $|0\rangle$ or $|1\rangle$ we prepare a superposition $1/\sqrt{2}\,(|0\rangle + |1\rangle)$ then we obtain

$$\frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle \equiv \frac{1}{\sqrt{2}}\,(|011\rangle + |111\rangle)\,.$$

In fact we can prepare this register in a superposition of all eight numbers – it is enough to put each qubit into the superposition $1/\sqrt{2}\,(|0\rangle \pm |1\rangle)$. Such superpositions are usually prepared using the Hadamard gates. The Hadamard transform on n qubits is implemented by applying the Hadamard gate to each of the n qubit, e.g.



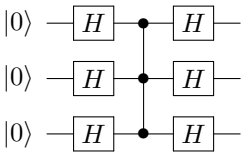
In general, if we start with a register in some state $|x\rangle$ ($x \in \{0,1\}^n$) then The Hadamard transform gives

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle.$$

Quantum computation usually starts with the main register in state $|0\rangle$ and the Hadamard transform $|0\rangle \mapsto \sum_x |x\rangle$, which prepares an equally weighted superposition of all possible inputs.

V. MULTIQUBIT INTERFERENCE

Quantum interference gets even more interesting when it involves several qubits. For example, the network



effects an interference of three qubits. The sequence of operations is essentially the same as in the single qubit case: the first Hadamard, followed by phase shifts and followed by another Hadamard transform. The input state, $|0\rangle$, evolves as

$$\begin{aligned}|0\rangle &\mapsto \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \\ &\mapsto \frac{1}{\sqrt{2^n}} \sum_x e^{i\phi(x)}|x\rangle \\ &\mapsto \frac{1}{2^n} \sum_y \left(\sum_x e^{i\phi(x)}(-1)^{x\cdot y} \right) |y\rangle\end{aligned}$$

where $x, y \in \{0,1\}^n$. The output state of the register is a superposition of binary strings y. If you choose to measure the register, bit by bit, you obtain one specific value of y, with probability that depends on the phase shifts.

$$P_y(\phi) = \frac{1}{2^{2n}} \left| \sum_x e^{i\phi(x)}(-1)^{x\cdot y}/2^n \right|^2$$

A quantum register, initially in the input state $|0\rangle$ can evolve into some final state $|y\rangle$ following 2^n different computational paths, labelled by x, and taking each of them with the probability amplitude $e^{i\phi(x)}(-1)^{x\cdot y}/2^n$. The total amplitude for this transition is the sum of all the contributing amplitudes (we sum over x) and the corresponding probability is the squared modulus of the sum.

The multiqubit interference is not equivalent to running several single qubit interferences in parallel. Take, for example, a two qubit interference and let the four states $|x\rangle$ acquire phase shits

$$|00\rangle + e^{i\alpha}|01\rangle + e^{i\beta}|10\rangle + e^{i\gamma}|11\rangle.$$

This interference can be viewed as two single qubit interferences only when $\alpha + \beta = \gamma$. Can you see it?