A quantum computer is a machine that can perform certain calculations much faster than a classical computer by using the laws of quantum mechanics. Quantum computers do not exist yet, because it is extremely difficult to control quantum mechanical systems to the necessary degree. What is more, we do at this moment not know which physical system is the best suited for making a quantum computer (although we have some ideas). It is likely that a mature quantum information processing technology will use (among others) light, because photons are ideal carriers for quantum information. These notes are an expanded version of the five lectures I gave on the possibility of making a quantum computer using light, at the Summer School in Theoretical Physics in Durban, 14–24 January, 2007. There are quite a few proposals using light for quantum computing, and I can highlight only a few here. I will focus on photonic qubits, and leave out continuous variables completely.\(^1\) I assume that the reader is familiar with basic quantum mechanics and introductory quantum computing.

1 Light and Quantum Information

Simply put, a quantum computer works by storing information in physical carriers, which then undergo a series of unitary (quantum) evolutions and measurements. The information carrier is usually taken to be a qubit, a quantum system that consists of two addressable quantum states. Furthermore, the qubit can be put in arbitrary superposition states. The unitary evolutions on the qubits that make up the computation can be decomposed in single-qubit operations and two-qubit operations. Both types of operations or gates are necessary if the quantum computer is to outperform any classical computer.

\(^1\) For a review on optical quantum computing with continuous variables, see Braunstein and Van Loock, Rev. Mod. Phys. 77, 513 (2005).
1.1 Photons as Qubits

We define the computational basis states of the qubit as some suitable set of states $|0\rangle$ and $|1\rangle$. An arbitrary single-qubit operation can take the form of a compound rotation parameterized by two angles $\theta$ and $\phi$:

$$
|0\rangle \rightarrow \cos \theta |0\rangle + ie^{i\phi} \sin \theta |1\rangle,
$$

$$
|1\rangle \rightarrow ie^{i\phi} \sin \theta |0\rangle + \cos \theta |1\rangle.
$$

This can be represented graphically in the Bloch or Poincaré sphere (see Fig. 1).

What type of light can be used as a qubit? The smallest excitation of the electromagnetic field is the photon. We cannot construct a standard wave function for the photon, but we can identify the different degrees of freedom that we can use as a qubit: a photon can have the choice between two spatially separated beams (or modes), or it can have two distinct polarizations [1]. These two representations are mathematically equivalent, as we will show below.

The emission and absorption of photons with momentum $k$ is described mathematically using creation and annihilation operators:

$$
\hat{a}(k)|n\rangle_k = \sqrt{n}|n-1\rangle_k \quad \text{and} \quad \hat{a}^\dagger(k)|n\rangle_k = \sqrt{n+1}|n+1\rangle_k.
$$

It is straightforward to show that $\hat{n}(k) \equiv \hat{a}^\dagger(k)\hat{a}(k)$ is the number operator $\hat{n}(k)|n\rangle_k = n|n\rangle_k$. The canonical commutation relations between $\hat{a}$ and $\hat{a}^\dagger$ are given by

$$
[\hat{a}(k), \hat{a}^\dagger(k')] = \delta(k - k'),
$$

$$
[\hat{a}(k), \hat{a}(k')] = \hat{a}(k') = 0.
$$

For the purposes of these notes, we use subscripts to distinguish the creation and annihilation operators for different modes, rather than the functional dependence on $k$. In photon language, we can define the logical qubit states on two spatial modes $a$ and $b$ as:

![Fig. 1 Graphic representation of the Bloch sphere](image-url)