Chapter 5

Quantum vs Classical Information

5.1 The qubit

Quantization proceeds by associating the two faces of a cebit two orthogonal vectors $|0\rangle$ and $|1\rangle$, say, in a two-dimensional Hilbert space. A quantum-mechanical entity whose Hilbert space is two-dimensional is called a **qubit**. The qubit is the elementary *carrier* of a novel type of information, called **quantum information**.[1] What kind of information this "is", and how it relates to "ordinary" information, is the subject of this lecture.

Possible states of the qubit are

$$|0\rangle \quad \text{or} \quad |1\rangle \qquad \text{but also} \qquad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \tag{5.1}$$

where complex α,β denote probability *amplitudes*. We recall that, for $|\psi\rangle$ normal-

[1] The *measure* of quantum information continues to be in bits, not qubits.

ized, the squares $|\alpha|^2$ and $|\beta|^2$ give the *probability* to detect the qubit in the state $|0\rangle$ and $|1\rangle$, respectively.

The normalization $|\alpha|^2 + |\beta|^2 = 1$ admits the parametrization $\alpha = \cos(\frac{\vartheta}{2})e^{i\gamma}$, $\beta = \sin(\frac{\vartheta}{2})e^{i\delta}$, and since the global phase of $|\psi\rangle$ has no observable effect, we may write

$$|\psi\rangle = \cos\tfrac{\vartheta}{2}\,|0\rangle + e^{i\varphi}\sin\tfrac{\vartheta}{2}\,|1\rangle\,. \tag{5.2}$$

The angles ϑ and φ define a point on the surface of a unit sphere – the *Bloch sphere*, see Fig. 5.1. The Bloch sphere, which in an optical context is called *Poincaré sphere*, provides an excellent tool to visualize the state vector of a qubit.

For the physical realization of the qubit one may take any two-state system, e. g.

- a two-level atom, with the the excited state $|e\rangle$ the logical $|1\rangle$, and the ground state the logical $|0\rangle$;
- a photon in a given spatial mode, a plane wave say, with any pair of two orthogonal polarizations playing the role of the two states;
- a cavity mode with one or zero photons;
- the spin degree of freedom of a spin-$\frac{1}{2}$ particle, like a neutron, or an atom, treating the translational degrees of freedom classically.

Each of these systems has its merits and specific flaws. Single photons, for example, are good for communication purposes, yet (i) it is still difficult to produce them "on demand", and (ii) it is still not possible to detect them one by one, i.e. with unit efficiency. Atoms – and spins for that matter – are good for computation purposes, but they are difficult (i) to prepare and to control, and (ii) to shield from their environment.

Example Consider an atom which at time $t = 0$ is prepared in its excited state $|e\rangle$. Due to the unavoidable coupling of the atom to the electromagnetic field, even if in the vacuum state, the atom will eventually emit a photon, thereby making a transition into the atom ground state $|g\rangle$. We can not predict exactly when this will happen. The only thing we know is that the probability to still find the atom in its excited state at a later time $t > 0$ decreases with time, $|\beta(t)|^2 = e^{-\gamma t}$.[2] Thus finding an atom in its ground state, we do not know whether (i) it in fact was prepared in the ground state, or (ii) whether it was, some time ago, prepared in the excited state but underwent spontaneous emission in the meantime. On long time scales spontaneous emission is clearly detrimental for any information processing, but on short time scales $t \ll \gamma^{-1}$ spontaneous emission is irrelevant.

To balance the merits and the short comings requires a detailed physical investigation. It must be dealt with in a system specific manner. In developing the foundations of the quantum information theory, however, we may ignore the specifics, and focus on the principles.

5.2 The power of linear superposition

The state vector on the right hand side of (5.1) is a *linear superposition*. The linear superposition is one of two key elements of quantum information. The other element – *entanglement* – will be introduced when we talk about composite systems which consist of several qubits. For the time being we shall be dealing with single qubits.

[2]According to Fermi's Golden Rule $\gamma/\omega_0 = (4/3)\alpha[a_0/\lambda\!\!\!^{-}_0]^2[d/(ea_0)]^2$, where ω_0 is the Bohr transition frequency, $\lambda\!\!\!^{-}_0 = c/\omega_0$ is the reduced wavelength of the emitted photon, a_0 is the Bohr radius, $\alpha \approx 1/137$ is the fine structure constant, and d is the dipole matrix element of the transition.

The quantum mechanical superposition, having no classical counterpart, allows to do things which are impossible with classical cebits. For example instead of using the naive code

$$b(|\mathtt{1}\rangle) = \mathtt{1}\,, \qquad b(|\mathtt{0}\rangle) = \mathtt{0}\,, \tag{5.3}$$

Alice and Bob could agree on the superposition code

$$b(|+\rangle) = \mathtt{1}, \qquad b(|-\rangle) = \mathtt{0}\,, \tag{5.4}$$

where $|\pm\rangle = (|\mathtt{0}\rangle \pm |\mathtt{1}\rangle)/\sqrt{2}$ is also a pair of orthogonal – that is fully distinguishable – state vectors. An eavesdropper (dt.: Lauscher), who is not aware of the agreement (5.4) but assumes the naive code (5.3) instead, would decode an intercepted qubit in state $|+\rangle$, say, as $\mathtt{0}$ or $\mathtt{1}$ with equal probability. Hence in contrast to Bob, who can read any of Alice's messages with one hundred percent reliability, the eavesdropper can not infer Alice's message from the intercepted qubit. This kind of *privacy protection*, which is impossible with cebits, is a nice pay-off of the quantum mechanical superposition principle.

Eve's futile attempts to read Alices messages can also be viewed positively: measurement of a sequence of $|+\rangle$ qubits in the naive code, say, generates a completely random sequence of bits – the randomness being not "pseudo", i.e. due to some deterministic algorithm, but rather "perfect", i.e. fully unpredictable. Mother nature – being quantum – provides us with truly divine a perfect random number generator!

Another pay-off is in computation, where the superposition allows for a speed-up by an effect called *quantum parallelism*. Consider a binary function $f : \{|\mathtt{0}\rangle, |\mathtt{1}\rangle\} \to \{|f(\mathtt{0})\rangle, |f(\mathtt{1})\rangle\}$. Acting on a qubit in the superposition $|+\rangle$, we have $f : |+\rangle \mapsto |f(\mathtt{0})\rangle + |f(\mathtt{1})\rangle$, i.e. *both* values of f are computed in a *single* call – a sheer impossibility in classical computation.

5.3 The benefit of the impossible

The quantum mechanical superposition, while clearly offering additional possibilities, is not unlimited a source of magic tricks. There are ideas, which on first sight appear mind boggling, which on close scrutiny, however, turn out to be mere pipe dreams.

Example As the two angles ϑ and φ need infinitely many binary digits for their specification, one may speculate that a qubit may be used to transmit many, in fact infinitely many, bits of information. But this hope is void. Alice may well *encode* her PhD thesis into a superposition, but Bob can not *decode*: there is no device which – for a *single* qubit[3] – can measure the numbers α, β.[4] Even the most perfect measurement device only allows to decide on binary alternatives $|0\rangle$ or $|1\rangle$, say, or – with another device – $|+\rangle$ or $|-\rangle$. For a single qubit, the most one can extract is *one* bit of information. [5]

Important impossibilities are best memorized as *impossible machines*. The impossible machine underlying the previous example is the *universal quantum decoder*–a device which produces, for a *single* qubit, the numbers ϑ, φ.

[3]The notion of a *single* qubit refers to a situation where indeed you have only one shot in an experiment. Note that even in the context of a statistical theory like quantum mechanics, the single event still has its role to play. You may be given, for example, a *single* qubit which was either prepared in state $|0\rangle$ or – with equal probability – in state $|1\rangle$. In this case, the alternative may be unambiguously decided from the outcome of a single measurement.

[4]That is not to say that you can not determine these numbers. Indeed, if you have *many* qubits, all in the same state (drawn from the same ensemble) you may unambiguously determine these numbers from the outcomes of three different measurements (three different orientations of a Stern-Gerlach magnet, see below).

[5]On average. Recall the discussion on the number of Hartley bits carried by a single cebit. This number can be more than one, but it can not exceed one *on average*.

Despite their negative connotation, impossible machines often turn out to be quite useful. It is the impossibility of universal decoding, for example, which renders void the eavesdropper's attempt to silently listen in, i.e. without disturbing the channel and thereby revealing his (or her) attempt. And it is the fundamental randomness of quantum mechanics which gives us such powerful a device like a perfect random number generator.

5.4 The novel type of information

From our experience with ideal telephones we know that the transferral of information from sound wave to electrical currents back to sound waves is possible without "losing" (or adding, for that matter) any information.

Similarly the transferral of the numbers ϑ, φ from one quantum system to another is also possible. But it is impossible to faithfully extract these numbers in a single experiment. With respect to a faithful extraction, the classical to quantum coding is a perfect trap door – easy to fall in, but impossible to climb out. In contrast to a mathematical trap door functions like, say, factoring, this is a trap door which is based on a *physical law*, and until that law is proven to be wrong, the trap is perfect.

With perfect convertability of information between different *classical* carriers, and between different *quantum* carriers, but imperfect convertibility between quantum and classical carriers, the distinction of quantum and classical information makes sense. To be more specific

> Quantum information is that kind of information, which is carried by a quantum system from the preparation device to the measuring apparatus

in a quantum mechanical experiment.[6]

[6]quoted from: *Quantum Information Theory – an Invitation* by R. F. Werner, preprint (2000)

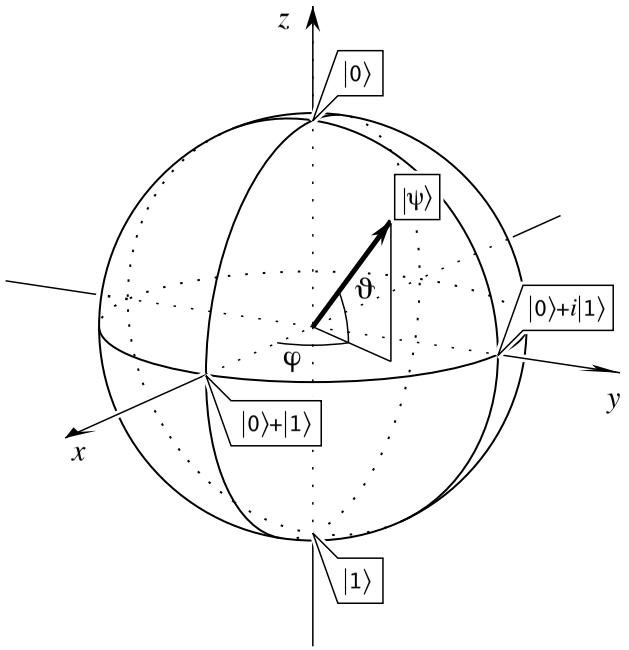

Figure 5.1: The Bloch sphere. Each pair of angles ϑ and φ represents a state vector of a qubit. Opposite points define a pair of orthogonal basis vectors.