C. QUANTUM INFORMATION

C Quantum information

C.1 Qubits

C.1.a Single qubits

1. Qubit: Just as the bits 0 and 1 are represented by distinct physical states, so the quantum bits (or qubits) \(|0\rangle\) and \(|1\rangle\) are represented by distinct quantum states.

2. Computational or standard basis: We call \(|0\rangle\) and \(|1\rangle\) the computational or standard measurement basis.

3. Superposition: What distinguishes qubits from classical bits is that they can be in a superposition of states, \(a_0|0\rangle + a_1|1\rangle\), \(a_0, a_1 \in \mathbb{C}\), where \(|a_0|^2 + |a_1|^2 = 1\).

4. We will observe \(|0\rangle\) with probability \(|a_0|^2\) and likewise for \(|1\rangle\); henceforth the qubit is in the observed state.

5. I write this:

\[
a_0|0\rangle + a_1|1\rangle \xrightarrow{|a_0|^2} |0\rangle,
\]

\[
a_0|0\rangle + a_1|1\rangle \xrightarrow{|a_1|^2} |1\rangle.
\]

6. Sign basis: The following sign basis is often useful:

\[
|+\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),
\]

\[
|-\rangle \overset{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).
\]

7. Notice that \(|+\rangle\) is “halfway” between \(|0\rangle\) and \(|1\rangle\).
Likewise \(|-\rangle\) is halfway between \(|0\rangle\) and \(-|1\rangle\).

8. Draw them.

8. Note (exercise):

\[
|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle),
\]

\[
|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).
\]
To remember this, think 
\[(+x) + (-x) = 0\] and 
\[(+x) - (-x) = (+2x)\] (just a mnemonic).
Even though a quantum bit can be put in infinitely many superposition states, it is only possible to extract a single classical bit’s worth of information from a single quantum bit. The reason that no more information can be gained from a qubit than in a classical bit is that information can only be obtained by measurement. When a qubit is measured, the measurement changes the state to one of the basis states in the polarization experiment. As every measurement can result in one of two states, one of the basis vectors associated to the given measuring device, so, just as in the classical case, there are only two possible results. As measurement changes the state, one cannot measure the state of a qubit in two different bases. Furthermore, as shown in section 4.1.2, quantum states cannot be cloned so it is not possible to measure a qubit in two ways, even indirectly by, say, copying the qubit and measuring the copy in a different basis from the original.

3.1 Quantum Key Distribution

Sequences of single qubits can be used to transmit private keys on insecure channels. In 1984 Bennett and Brassard described the first quantum key distribution scheme [Bennett and Brassard 1987; Bennett et al. 1992]. Classically, public encryption techniques, e.g. RSA, are used for key distribution.

Consider the situation in which Alice and Bob want to agree on a secret key that they can communicate privately. They are connected by an ordinary bidirectional open channel and a unidirectional quantum channel both of which can be observed by Eve, who wishes to eavesdrop on their conversation. This situation is illustrated in the figure below. The quantum channel allows Alice to send individual particles (e.g. photons) to Bob who can measure their quantum state. Eve can attempt to measure the state of these particles and can resend the particles to Bob.

To begin the process of establishing a secret key, Alice sends a sequence of bits to Bob by encoding each bit in the quantum state of a photon as follows. For each bit, Alice randomly uses one of the following two bases for encoding each bit:

\[
\begin{align*}
0 & \rightarrow |\uparrow\rangle \\
1 & \rightarrow |\downarrow\rangle
\end{align*}
\]

Figure III.6: Quantum key distribution (from IQC).

Figure III.7: Example of QKD without interference. [fig. from wikipedia]

C.1.b QUANTUM KEY DISTRIBUTION

This section is based on Rieffel & Polak (2000), which is also the source for otherwise unattributed quotes.

¶1. In 1984 Bennett and Brassard showed how sequences of qubits could be used to distribute an encryption key securely. This is called the “BB84 protocol.” The idea was proposed initially by Stephen Wiesner in the 1970s, but he couldn’t get it published.

¶2. We are supposing that Alice is transmitting a key to Bob over two
channels, one classical and one quantum. Eve may eavesdrop on both channels and even replace the signals in them.

3. Over the quantum channel Alice will send the photons to Bob that encode the key bits in two different bases, $\{|\uparrow\rangle, |\rightarrow\rangle\}$ (the + basis) or $\{|\downarrow\rangle, |\leftarrow\rangle\}$ (the $\times$ basis), chosen randomly. See Fig. III.7.

4. Bob will measure the photons according to these two bases, also chosen randomly and independently of Alice.

5. After the transmission, Alice and Bob will communicate over the classical channel and compare their random choices; where they picked the same basis, they will keep the bit, otherwise they will discard it. (They will have agreed on about 50% of the choices.)

6. **Eavesdropping:** Suppose Eve is eavesdropping on the quantum channel, measuring the qubits and retransmitting them to Bob. See Fig. III.8.

7. About 50% of the time, she will guess the wrong basis.

8. She will also resend it in this same incorrect basis.

9. “So when Bob measures a resent qubit with the correct basis there will be a 25% probability that he measures the wrong value.”
50% of the time Eve picks the same basis as Alice, so she reads the bit correctly and transmits it to Bob correctly.
50% of the time Eve guesses the wrong basis. She will know this, if she is listening in on the classical channel.
However she has already transmitted it to Bob in the wrong basis.
If this is a case in which Alice and Bob used the same basis (and so Bob should get it correct), he will get it incorrect 50% of the time, since Eve transmitted it in the other basis.
So 25% of the bits that should be correct will be wrong.

¶10. This high error rate will be apparent to Alice and Bob if they have been using an error-detecting code for the key. (In effect Eve is introducing noise into the channel.)

¶11. Further, Eve’s version of the key will be about 25% incorrect.

¶12. This is only the most basic technique, and it has some vulnerabilities. Other techniques have been proposed.

¶13. State of the art:² “The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre)”

¶14. “As of March 2007 the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos National Laboratory/NIST using the BB84 protocol.”

¶15. “The distance record for free space QKD is 144 km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the Ekert scheme) in 2006,[7] and using BB84 enhanced with decoy states[8] in 2007.[9] The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes.”

¶16. Commercial: At least three companies offer commercial QKD.
“Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capitol in the national election occurring on October 21, 2007.”

§17. **QKD networks**: Four QKD networks have been in operation since mid-late 2000s.

§18. **SECOQD**: These include “[t]he world’s first computer network protected by quantum key distribution was implemented in October 2008, at a scientific conference in Vienna. The name of this network is SECOQ (Secure Communication Based on Quantum Cryptography) and EU funded this project. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west.”
C. QUANTUM INFORMATION

C.1.c Multiple qubits

1. We can combine multiple qubits into a *quantum register*.

2. **State space:** By Postulate 4, if \( \mathcal{H} \) is the state space of one qubit, then the tensor power \( \mathcal{H}^\otimes n \) will be the state space of an \( n \)-qubit quantum register.

3. **Computational or standard basis:** The computational basis of this space is the set of all vectors \( |b_1 b_2 \cdots b_n\rangle \) with \( b_k \in \{0, 1\} \).

4. Therefore the dimension of this space is \( 2^n \). The set of states is the set of normalized vectors in \( \mathbb{C}^{2^n} \).

5. For 10 qubits we are dealing with 1024-dimensional complex vectors (because each of the \( 2^{10} \) basis vectors has its own complex amplitude).

6. This is a huge space, exponentially larger than the \( 2^n \) classical \( n \)-bit strings. This is part of the origin of *quantum parallelism*, because we can compute on all of these qubit strings in parallel.

7. **500 qubits:** Consider a quantum computer with 500 qubits; it should be very small (e.g., 500 atoms).
   It is computing in a space of \( 2^{500} \) complex numbers.
   \( 2^{500} \) > the number of particles in the universe \( \times \) the age of the universe in femtoseconds!
   In effect, a universe-sized computer working at high speed since the Big Bang.

8. Whereas a normal direct product has dimension \( \dim(S \times T) = \dim S + \dim T \), a tensor product has dimension \( \dim(S \otimes T) = \dim S \times \dim T \). Hence if \( \dim S = 2 \), \( \dim S^{\otimes n} = 2^n \).

9. **Partial measurement:** Suppose we have a composite state

\[
|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,
\]

and we measure just the first bit.
\(10.\) We will get 0 with probability \(|a_{00}|^2 + |a_{01}|^2\) and it will collapse into the state \(a_{00}|00\rangle + a_{01}|01\rangle\), but we must renormalize it:

\[
|\psi'\rangle = \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.
\]

Do this by striking out all terms that have 1 in the first position.

\(11.\) That is:

\[
|\psi\rangle \xrightarrow{|a_{00}|^2 + |a_{01}|^2} \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.
\]