C Quantum information

C.1 Qubits

C.1.a Single qubits

Just as the bits 0 and 1 are represented by distinct physical states in a conventional computer, so the *quantum bits* (or qubits) $|0\rangle$ and $|1\rangle$ are represented by distinct quantum states. We call $|0\rangle$ and $|1\rangle$ the *computational* or *standard* measurement basis. What distinguishes qubits from classical bits is that they can be in a superposition of states, $a_0|0\rangle + a_1|1\rangle$, for $a_0, a_1 \in \mathbb{C}$, where $|a_0|^2 + |a_1|^2 = 1$. If we measure this state in the computational basis, we will observe $|0\rangle$ with probability $|a_0|^2$ and likewise for $|1\rangle$; after measurement the qubit is in the observed state. This applies, of course, to measurement in any basis. I will depict the measurement possibilities this way:

$$\begin{aligned} a_0|0\rangle + a_1|1\rangle &\xrightarrow{|a_0|^2} |0\rangle, \\ a_0|0\rangle + a_1|1\rangle &\xrightarrow{|a_1|^2} |1\rangle. \end{aligned}$$

The following *sign basis* is often useful:

$$|+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{III.8}$$

$$|-\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{III.9}$$

Notice that $|+\rangle$ is "halfway" between $|0\rangle$ and $|1\rangle$, and likewise $|-\rangle$ is halfway between $|0\rangle$ and $-|1\rangle$. Draw them to be sure you see this. As a consequence (Exer. III.25):

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \\ |1\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \end{aligned}$$

To remember this, think $(+x) + (-x) = 0$ and $(+x) - (-x) = (+2x)$, which is nonzero (this is just a mnemonic).

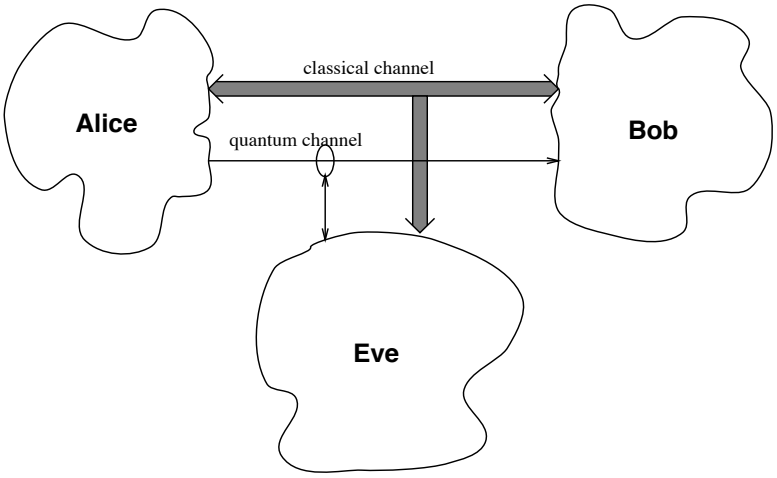

Figure III.6: Quantum key distribution [from Rieffel & Polak (2000)].

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

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

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Figure III.8: Example if QKD with eavesdropping. [fig. from wikipedia]

C.1.b Quantum key distribution

In 1984 Bennett and Brassard showed how sequences of qubits could be used to distribute an encryption key securely.[3] This is called the "BB84 protocol." Ironically, the idea was proposed initially by Stephen Wiesner in the 1970s, but he couldn't get it published.

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. Over the quantum channel Alice will send the photons to Bob that encode the key bits in two different bases, either $\{|\uparrow\rangle, |\rightarrow\rangle\}$, which I'll call the "+ basis," or $\{|\nearrow\rangle, |\searrow\rangle\}$ (the "× basis") (respectively 0, 1 in each basis). Alice chooses randomly the basis in which to encode her bits (see Fig. III.7). Bob will measure the photons according to these two bases, also chosen randomly and independently of Alice. 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.)

Suppose Eve is eavesdropping on the quantum channel, measuring the qubits and retransmitting them to Bob (see Fig. III.8). About 50% of the time, she will guess the wrong basis, and will also resend it in this same incorrect basis. If this is one of the times Alice and Bob chose the same basis, the bit will nevertheless be incorrect about half of the time (the times

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

Eve chose the wrong basis). That is, about 50% of the time Eve picks the same basis as Alice, so she reads the bit correctly and transmits it to Bob correctly. About 50% of the time Eve guesses the wrong basis. She will know this, if she is listening in on the classical channel, but 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. 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 significant, detectable noise into the channel.) Furthermore, Eve's version of the key will be about 25% incorrect. Therefore Bob knows that the key was not transmitted securely and Eve gets an incorrect key.

This is only the most basic technique, and it has some vulnerabilities, and so other techniques have been proposed, but they are outside the scope of this book. "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)"[4] "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." In Aug. 2015 keys were distributed over a 307 km optical cable, with 12.7 kbps key generation rate. "The distance record for free space QCD [quantum key distribution] 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." 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." Four QKD networks have been in operation since mid-late 2000s. Among them,

> [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 SECOQC (**Se**cure **Co**mmunication Based on **Q**uantum **C**ryptography) and

[4] `https://en.wikipedia.org/wiki/Quantum_key_distribution` (accessed 12-09-18).

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.1.c Multiple qubits

We can combine multiple qubits into a *quantum register*. 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. The computational basis of this space is the set of all vectors $|b_1 b_2 \cdots b_n\rangle$ with $b_k \in \mathbf{2}$. (I define $\mathbf{2} \stackrel{\text{def}}{=} \{0, 1\}$ to be the set of bits, and in general I use a boldface integer $\mathbf{N}$ for the set integers $\{0, 1, \ldots, N-1\}$.) Therefore the dimension of the space $\mathcal{H}^{\otimes n}$ is 2^n, and the set of states is the set of normalized vectors in $\mathbb{C}^{2^n}$. For 10 qubits we are dealing with 1024-dimensional complex vectors (because each of the 2^{10} basis vectors has its own complex amplitude). 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. Consider a quantum computer with 500 qubits; it could be very small (e.g., 500 atoms), but it is computing in a space of 2^{500} complex numbers. Note that 2^{500} is more than the number of particles in the universe times the age of the universe in femtoseconds! That is, a 500-qubit quantum computer is equivalent to a universe-sized computer working at high speed since the Big Bang.

Whereas an ordinary 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 $\dim S = 2$, $\dim S^{\otimes n} = 2^n$.

Measuring some of the qubits in a register causes partial collapse of the quantum state. 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. 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 in $|\psi\rangle$ that have 1 in the first qubit.

$$|\psi\rangle \stackrel{|a_{00}|^2+|a_{01}|^2}{\longrightarrow} a_{00}|00\rangle + a_{01}|01\rangle \cong \frac{a_{00}|00\rangle + a_{01}|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}.$$