QUANTUM INFORMATION May 8, 2023

In the 1920s quantum mechanics was discovered, by *Heisenberg, Born, Schrödinger,* and others. It was found to involve probability theory in an intimate way. But classical probability theory was still in a primitive state. *Kolmogorov* gave a proper axiomatization of probability theory in the 1930s. *Shannon* introduced information theory in the 1940s. In the following decade the theory of stochastic processes saw great developments. So did operator theory, the work of *Stinespring* being especially important. In the 1970s the time had come to update the probabilistic structure of quantum mechanics. Thus the subject of quantum information was born, in the hands of *Holevo, Kraus, Lindblad*, and a few others. A new ingredient was introduced when the idea of quantum computers was put on the table, by *Benioff*, *Deutsch*, and others. The subject grew dramatically in the 1990ies largely because experimentalists caught up with it, enabling theorists like *Bennett* and *Shor* to assume that the theory deals with things you can actually do. At the moment it is one of the main growth points of physics. It will take some time before we know where it leads.

Quantum mechanics has many successes to its credit, such as enabling us to understand the wave-particle nature of light, the structure of atoms, and the stability of matter. Here we take a lightning tour through quantum information theory, assuming as little as possible in the way of prerequisites. The course falls into four separate parts:

- Lengthy introduction
- Open systems
- Information theory
- Quantum computation

To support you, and keep you company in the evenings, you have the book by Stenholm and Suominen, and these lecture notes. Since the book starts with a quote, I do so too: "*it would be contrary to ... the perfection of things, if there were no chance events*". The source is the same as Stig's and Kalle-Antti's.

LENGTHY INTRODUCTION

Throughout the lectures I will stress the connection to classical probability theory rather more than the book does. The book on the other hand stresses the connection to experiments in quantum optics much more than I will do.

The set of classical probabilities

Probability theory is simple to define mathematically if we stick to probability distributions over a finite number n of mutually exclusive events. Then we need n non-negative numbers summing to 1,

$$p_i \geq 0 \ , \qquad \sum_{i=1}^{n} p_i = 1 \ . \tag{1}$$

We can collect these numbers into a vector $\vec{p}$ and refer to any such vector as a probability vector, as a *probability distribution* P, or—in analogy to the quantum states that we will introduce later—as a *classical state*.

It is an embarrassment that the question what it *means* to assign the number $p_1 = 0.561$ (say) is controversial. Is it an objective statement about frequencies? Or a measure of rational belief? Or what? Things are simple only as long as we don't ask.

A bit of extra notation is helpful. A *random variable* is defined as a function that assigns real numbers to events. The random variable A takes values a_i with probabilities

$$p_i = P(A = a_i) \ . \tag{2}$$

If we have several random variables we can define the *joint probability* $p_{i,j} = P(A = a_i, B = b_j)$, which is the probability that A takes the value a_i and B takes the value b_j, and the *conditional probability* $P(A = a_i|B = b_j)$, which is the probability that A takes the value a_i given that B is known to take the value b_i. Joint and conditional probabilities are connected by *Bayes*'s formula. In short hand notation

$$P(A, B) = P(A|B)P(B) = P(B|A)P(A) \ . \tag{3}$$

If there are n outcomes for the first and m for the second, the joint probability vector carries a collective index and has nm components. We require

$$p_i = P(A = a_i) = \sum_{j=1}^{m} p_{i,j} \ , \qquad q_j = P(B = b_j) = \sum_{i=1}^{n} p_{i,j} \ . \tag{4}$$

Probability vectors that arise in this way from a joint probability distribution are known as *marginal* distributions.

The random variables may or may not be correlated. If not, they are *independent*, and the probability vector for the joint event can be written as

$$p_{i,j} = P(A = a_i, B = b_j) = P(A = a_i)P(B = b_j) = p_i q_j \ . \tag{5}$$

I stress that this equation is *not* true in general. Indeed, suppose $n = m = 2$, and order the components of the joint probability vector lexicographically:

$$P_0 = p_{0,0} \ , \quad P_1 = p_{0,1} \ , \quad P_2 = p_{1,0} \ , \quad P_3 = p_{1,1} \ . \tag{6}$$

Now suppose that the random variables are independent, as in eq. (5). Then the probability vectors that actually occur (the frequencies that will actually be observed, if you look at it that way) are constrained by[1]

$$P_0 P_3 = P_1 P_2 \ . \tag{7}$$

If the observed frequencies do not obey this condition, you conclude that the two random variables must be correlated.

The set of probability vectors form a *convex set*. What this means is that given two probability vectors $\vec{p}_{(1)}$ and $\vec{p}_{(2)}$ and a number $x \in (0, 1)$, the combination

$$\vec{p} = x\vec{p}_{(1)} + (1 - x)\vec{p}_{(2)} \tag{8}$$

is a probability vector too. Conversely, given a probability vector $\vec{p}$ we can ask if it can be formed as a mixture of two distinct probability vectors in this way. If no such decomposition is possible the vector $\vec{p}$ is said to be *pure*. Geometrically, you can think of a convex set as a set of points such that the straight line between any pair of points in the set also belongs to the set. Of course this assumes that we have a rule for adding points, and for drawing

[1]Exercise: Prove this. Note that it is an 'if and only if' statement.

straight lines between them. But this we have, because we regard our points as vectors in a vector space of a fixed dimension n. Given a set of points you can form the minimal convex set that contains them. This is known as their *convex hull*.

The set of probability vectors is a convex set of a special kind. When $n = 3$ there are three pure vectors, and every probability vector $\vec{p}$ can be written as a convex combination of these pure vectors,

$$\vec{p} = p_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + p_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + p_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad , \qquad p_i \geq 0 \ , \quad p_1 + p_2 + p_3 = 1 \ . \tag{9}$$

Geometrically this is a triangle, or a *simplex* if we keep the number of outcomes n arbitrary.[2] A convex combination, also known as a *mixture*, is a quite special case of a linear combination, because the coefficients are required to be non-negative and sum to one. For simplices the decomposition of a point into a convex combination of pure points is unique, but this is a special feature of simplices. A square is also a convex set, but there is no unique way of decomposing an interior point as a mixture of the four pure points at the corners. The same is true for a circular disk, which has infinitely many pure points. This last observation will become relevant when we come to the quantum case.

If you find the story so far too abstract for your taste you can use your physical intuition on an equivalent problem. Consider n points in space, or in the plane, distribute a fixed amount of mass over them, and ask for all possible positions of the centre of mass that can arise in this way. The answer is: the convex hull of the n points. You can also ask the converse question: if you know the position of the centre of mass, can you decide how the mass was distributed over the n points? The answer to this will depend on the set of n points was to begin with.

Dynamics and distinguishability

[2]Exercise: When $n = 4$ the simplex is a tetrahedron, and eq. (7) describes a surface inside a tetrahedron. Draw it! You should be able to see that it is formed from straight lines obtained by keeping either $\vec{p}$ or $\vec{q}$ constant.

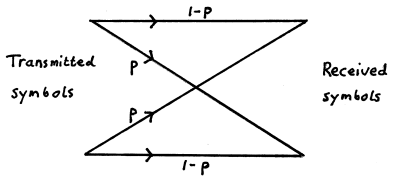


Figure 1: We illustrate the stochastic map (11). In information theory stochastic maps are called 'channels', and this is the 'binary symmetric channel'.

If you want to introduce dynamics on a probability simplex, the options are rather limited. You can use *stochastic maps*, given by matrices S such that the vector $\vec{q}$ defined by

$$\vec{q} = S\vec{p} \tag{10}$$

is a probability vector for every probability vector $\vec{p}$.[3] An example of a stochastic map is the 'bit flip' matrix

$$S = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}, \tag{11}$$

which may describe the degrading noise acting on a bit in a computer memory. If we also require the stochastic maps to take pure states into pure states, then the matrix is a permutation matrix. General stochastic maps tend to shrink the simplex towards some fixed point, and can be combined into *Markov chains*.[4] A *Markov process* is a special kind of stochastic time development in which what happens in a given step depends only on the result of the previous step. To see if a real physical phenomenon—like the Brownian motion studied by *Einstein*—is a Markov process, one needs a careful study of the relevant time scales.

This is a natural point to introduce the notion of *distance* between states, in this case between probability vectors. The first attempt is to say that the distance is defined using the recipe of Euclidean geometry, so that

[3]Exercise: What conditions on the matrix elements of S ensure that this holds? How do you prove that the product of two stochastic matrices is stochastic?

[4]Exercise: Apply the bit flip map (11) N times, and see what happens to the (one dimensional) probability simplex.

$$D^2(\vec{p},\vec{q}) = \sum_{i=i}^{n}(p_i - q_i)^2 \ . \tag{12}$$

The triangle becomes an equilateral flat triangle. But this turns out to be unsatisfactory from two points of view. From the first point of view one asks how easy it would be to *distinguish* two probability assignments from each other using a finite number N of observations or *samplings*. You may have two competing theories predicting the probability distributions $\vec{p}$ and $\vec{q}$, respectively. You perform N measurements and obtain a frequency vector $\vec{\nu}$, which does not agree exactly with either prediction because of statistical fluctuations. How many measurements do you have to perform before you can sit judgment between the two theories? If that number is large, the predictions are 'close', and we want a notion of distance that encodes this idea. The second point of view suggests that the notion of distance should have the property that

$$D(S\vec{p},S\vec{q}) \leq D(\vec{p},\vec{q}) \ . \tag{13}$$

This means that one requires *monotonicity* under arbitrary stochastic maps S. Either way, we insist that a notion of distance must mean something. This is the *operational* point of view, which pervades the whole subject.

Let us look at a special example of a stochastic matrix:

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \ . \tag{14}$$

This is a *coarse graining* of the outcomes. We have decided not to keep track of the distinction between the second and the third outcome, so certainly distinguishability goes down if we perform the map $\vec{p} \to \vec{q} = S\vec{p}$. But Euclidean distances on a flat simplex can increase under this map, as you can see in Figure 2. One way to handle this is to write

$$x_i = \sqrt{p_i} \geq 0 \quad \Rightarrow \quad \sum_i p_i = \sum_i x_i^2 = 1 \ . \tag{15}$$

If we think of the x_i as Cartesian coordinates in space the probability simplex looks like the positive octant of a sphere. We define the *Fisher–Rao distance* $D_{\rm FR}$ between two probability vectors as the length of the shortest curve

connecting them on the sphere that we just defined. It is well known that the shortest curve between two points on the sphere is always an arc of a great circle on the sphere, and you can easily convince yourself that if we connect two points on an octant of the sphere with such an arc, then the entire arc will lie within the octant. The distance D_{FR} between two probability distributions $\vec{p}$ and $\vec{q}$ then becomes simply the angle between the two unit vectors they define, which is implicitly given by the formula

$$\cos D_{\mathrm{FR}} = \sum_i \sqrt{p_i}\sqrt{q_i} \ . \tag{16}$$

This should be a familiar property of the unit sphere.

This notion of distance behaves nicely under all stochastic maps. It cannot decrease. We omit the proof, but Figure 2 shows how things work out for the coarse graining map (14). On the round octant the transformation goes along an arc of constant latitude, and distances stay constant.

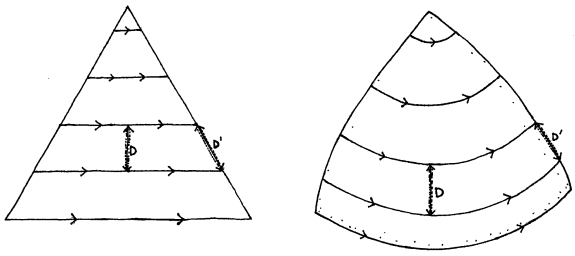


Figure 2: Coarse graining collapses the entire simplex onto one of its edges. Euclidean distances can increase under this operation—two points at distance D from each other will find themselves at a distance $D' > D$. On a round octant (one eighth of the surface of a sphere) this never happens.

The Fisher-Rao metric does have an operational meaning in terms of how well one can distinguish between two probability distributions based on the frequencies observed in a finite but large number of trials. Suppose that there are only two outcomes, and that one of them happens with probability p. The probability to see it happening m times if we do N samplings is

$$P(m) = \binom{N}{m} p^m (1-p)^{N-m} \ . \tag{17}$$

We get a frequency vector $\vec{\nu}$ with components $(m/N, (N-m)/N)$. If N is large we expect this to be a fair approximation of the probability vector $(p_1, p_2) = (p, 1-p)$. Indeed, after 20 years of work, *Jakob Bernoulli* proved an important theorem:[5]

Law of Large Numbers. For every $\epsilon > 0$ and $\delta > 0$ the probability $\mathcal{P}$ to obtain the first outcome m times in N trials obeys

$$\mathcal{P}\left(\left|\frac{m}{N} - p\right| < \epsilon\right) > 1 - \delta \ , \tag{18}$$

provided that $N > N_0$ for some sufficiently large N_0.

Information theory, to which we will arrive later, relies heavily on this.

It is possible to make the Law of Large Numbers into a more quantitative statement by bringing in Stirling's formula

$$n! \sim \chi(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \ . \tag{19}$$

This formula turns up whenever large numbers are to be counted.[6] The sign '$\sim$' means that

$$\lim_{n\to\infty} \frac{n!}{\chi(n)} = 1 \ , \tag{20}$$

and the approximation is accurate to within a percent already for $n = 10$.

Assuming that the number of samplings is large and using Stirling's formula we can rewrite (17) as

$$P(m) \sim \frac{1}{\sqrt{2\pi Npq}}\left(\frac{Np}{m}\right)^{m+\frac{1}{2}}\left(\frac{Nq}{N-m}\right)^{N-m+\frac{1}{2}} \ , \tag{21}$$

where $q = 1 - p$. We now introduce the variable

$$\lambda = \frac{m - Np}{\sqrt{Npq}} = \frac{m/N - p}{\sigma} \ , \tag{22}$$

[5]Exercise: Look in a textbook on probability theory for a proof that takes less than 20 years to do.

[6]Exercise: Derive an approximation for $\ln n!$ by rewriting it as a sum and then approximately as an integral. Compare to Stirling's formula.

where σ is the standard deviation. The parameter λ measures the deviation of the observed frequency from its expected value, in units of the standard deviation. Using λ to replace m we find after some calculations, and Taylor expansions, that

$$P(m) \sim \frac{1}{\sqrt{2\pi Npq}} e^{-\frac{\lambda^2}{2}} \ . \tag{23}$$

This is a famous result, due to *De Moivre*.

We can rewrite it in an interesting way by introducing

$$\left.\begin{array}{l} \Delta p_1 = \nu_1 - p_1 \\ \Delta p_2 = \nu_2 - p_2 \end{array}\right\} \quad \Rightarrow \quad \lambda^2 = N\left(\frac{\Delta p_1^2}{p_1} + \frac{\Delta p_2^2}{p_2}\right) \ . \tag{24}$$

We conclude that if N is large then the probability to observe the frequency $\vec{\nu}$ in N samplings is governed by the probability distribution

$$\mathcal{P}(\vec{\nu}) \sim \sqrt{\frac{N}{2\pi p_1 p_2}} e^{-\frac{N}{2}\sum_{i=1}^{2}\frac{(\Delta p_i)^2}{p_i}} \ , \qquad \Delta p_i = \nu_i - p_i \ . \tag{25}$$

What we are driving at now is that the sharpness of the peak of the Gaussian varies as you move around the probability simplex. As you can see in Figure 3, two probability assignments close to the edges of the interval will be easy to distinguish with a modest number of samplings, and hence we should regard them as far apart. The opposite holds for two probability assignments close to the centre. Quantifying this leads directly to the Fisher-Rao distance.

To see how, go back to (16) and suppose that $q_i = p_i + \Delta p_i$ where the Δp_i are small (and sum to zero). Taylor expanding on both sides (16) becomes

$$1 - \frac{1}{2} D_{\mathrm{FR}}^2 \approx \sum_i \sqrt{p_i}\sqrt{p_i}\sqrt{1 + \frac{\Delta p_i}{p_i}} \approx 1 - \frac{1}{4}\sum_i \frac{\Delta p_i^2}{p_i} \ . \tag{26}$$

From this we see that the expression that governs the sharpness of the peak in (25) is the Fisher–Rao distance squared. When we allow a large number of samplings this provides a justification of the Fisher–Rao distance, at least if the distances are small. Since we do not expect stochastic maps to increase distinguishability, we do indeed expect that metrics quantifying the latter notion must be monotone.

If we do not know what probability vector to assign to a choice between N outcomes, we expect that the likelihood to find the probability vector in a

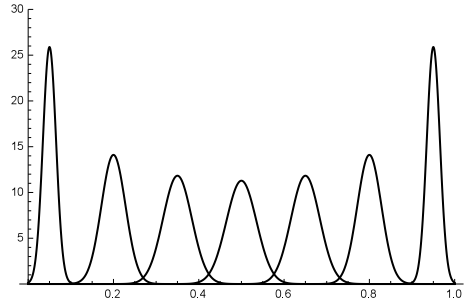


Figure 3: The broader the Gaussian, the harder it is to decide if the observed frequency matches the probability assignment we are assuming. Here $N = 200$, and we have one component of the probability vector on the horizontal axis.

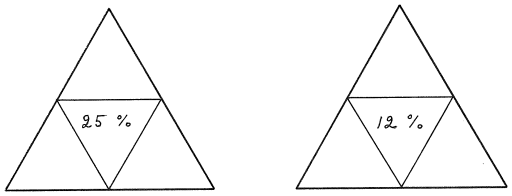


Figure 4: It might seem as if 25 percent of all probability distributions lie in the triangle in the middle. However, using the round metric on the simplex only 12 percent of them do.

given region on the probability simplex is proportional to the volume of that region. Here it clearly matters whether the simplex is flat or round. If we use the volume element provided by the Fisher-Rao metric for the purpose, we find that most of the volume is concentrated near the edges and vertices of the simplex. We can take this as a reason why, in real life, most things happen in a fairly predictable way. Random events that are evenly poised are quite rare.[7]

There are other notions of distance that are operationally meaningful, such as the 'taxi cab' l_1-distance

$$||\vec{p} - \vec{q}||_1 = \sum_{i=0}^{n-1} |p_i - q_i| \ . \tag{27}$$

[7]Exercise: Verify the calculation that goes into Figure 4.

On a two dimensional probability simplex 'circles' at constant distance from a given point will then appear as suitably oriented hexagons.[8] The taxi cab distance is monotone under stochastic maps, and its operational meaning has to do with how reliably two probability distributions can be distinguished by means of a single sampling.

The quantum generalization

To generalize classical probability theory we first rewrite the definitions in terms of diagonal matrices. We replace all probability vectors with matrices

$$P = \begin{pmatrix} p_1 & 0 & 0 \\ 0 & p_2 & 0 \\ 0 & 0 & p_3 \end{pmatrix} , \quad P \geq 0 , \quad \mathrm{Tr}P = 1 . \tag{28}$$

A random variable A is an otherwise unrestricted diagonal matrix,

$$A = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} . \tag{29}$$

The expectation value of a random variable, given a state, is then

$$\langle A \rangle = \mathrm{Tr}PA . \tag{30}$$

There is a fairly obvious generalization of all this. We replace the diagonal matrices with 'diagonalizable', and more particularly Hermitian, matrices. This still leaves it open whether they should be real or complex matrices, but it will turn out that complex numbers are the preferred choice, so let us make it right away. A state is now a positive (and therefore Hermitian) matrix,

$$\rho = \rho^\dagger , \qquad \rho \geq 0 , \qquad \mathrm{Tr}\rho = 1 . \tag{31}$$

The notation $\rho \geq 0$ means that all the eigenvalues are greater than or equal to zero. A matrix obeying all these conditions is known as a *density matrix*, or as

[8] Exercise: Draw such 'circles' around a few selected points in the simplex. Argue that this distance is monotone under the map (14).

a *quantum state*. A random variable is an otherwise unrestricted Hermitian matrix,

$$A = A^\dagger \ . \tag{32}$$

For expectation values, we keep the classical formula (30).

Since positive operators are so important, let us state three equivalent definitions:

$$\begin{aligned} &\rho \text{ is Hermitian with non-negative eigenvalues} \quad \Leftrightarrow \\ \Leftrightarrow \quad &\langle v|\rho|v\rangle \geq 0 \text{ for every vector } |v\rangle \quad \Leftrightarrow \\ \Leftrightarrow \quad &\rho = X^\dagger X \text{ for some bounded operator } X \ . \end{aligned} \tag{33}$$

This will make it easier to check if a given operator ρ is positive. It is also good to know that if A and B are positive operators then $\mathrm{Tr}AB \geq 0$, even though AB is not Hermitian unless A and B commute.

The quantum generalization is a significant one. The random variables, and the states, now belong to a non-commutative algebra. If the matrices act on a d dimensional Hilbert space the $d-1$ dimensional classical state space is turned into a $d^2-1 = (d-1)(d+1)$ dimensional one.[9] The set of density matrices is again a convex set. To see this we must prove that if ρ_1 and ρ_2 are density matrices then so is ρ, where ρ is the convex combination

$$\rho = x\rho_1 + (1-x)\rho_2 \ , \quad 0 \leq x \leq 1 \ . \tag{34}$$

The proof is easy given one out of the three equivalent definitions of a positive operators.[10] So the density matrices form a convex set, just as the probability vectors do.

A remark on the Dirac notation

[9] Exercise: Verify that a general matrix subject to (31) depends on d^2-1 real parameters, where d is the dimension of the complex Hilbert space.

[10] Exercise: Verify that this is, indeed, easy.

We will be dealing with vectors in Hilbert space, and operators acting on them. The Hilbert space will have a finite dimension d, and an orthonormal basis consisting of d unit vectors $|e_i\rangle$. In fact it has infinitely many different orthonormal bases. Having chosen one, we can write every vector in the form

$$|\psi\rangle = \sum_{i=0}^{d-1} z^i |e_i\rangle \ , \tag{35}$$

and every operator in the form

$$A = \sum_{i,j=0}^{d-1} |e_i\rangle A^i{}_j \langle e^j| \ . \tag{36}$$

Frequently this is on the pedantic side, and we will often regard vectors and operators as ordered arrays of numbers in the usual way (so that an operator becomes a matrix). Having said this, there are situations where things become conceptually more clear if we remember that this is just a shorthand. And it is important to know what properties depend only on the operator itself, and what properties depend also on the chosen basis. Being positive is an example of the first kind, and being diagonal is an example of the second. A Hermitian operator defines its own preferred eigenbasis, but if you are interested in two Hermitian operators that do not commute you will have to make the choice yourself.

The qubit

To understand what we have, set $d = 2$ so that we deal with two-by-two matrices. The most general Hermitian two-by-two matrix with unit trace can be written as

$$\rho = \frac{1}{2} \begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} = \frac{1}{2}(\mathbf{1} + x\sigma_x + y\sigma_y + z\sigma_z) \ , \tag{37}$$

where Pauli's sigma-matrices were introduced in the last step. Think of the triple (x, y, z) as a real vector. We call it the *Bloch vector*. When the Bloch vector is zero we have what we call the *maximally mixed* state. Its eigenvalues are clearly positive. We calculate that

$$\det \rho = \frac{1}{4}(1 - x^2 - y^2 - z^2) \ . \tag{38}$$

So the determinant vanishes if and only if the length of the Bloch vector equals unity. The set of positive matrices is determined by the condition

$$\det \rho \geq 0 \quad \Leftrightarrow \quad x^2 + y^2 + z^2 \leq 1 \ . \tag{39}$$

We call it the *Bloch ball*. Its surface is the *Bloch sphere*. The pure states sit at the surface. States in the interior are known as *mixed*, because they can be obtained as mixtures of pure states—in a highly non-unique fashion.

To see what goes on at the surface we note that every Hermitian matrix can be decomposed into its eigenvectors. That is, we can write

$$\rho = \lambda_0 |\psi_0\rangle\langle\psi_0| + \lambda_1 |\psi_1\rangle\langle\psi_1| \ , \qquad \langle\psi_i|\psi_j\rangle = \delta_{ij} \ , \quad \lambda_0 + \lambda_1 = 1 \ . \tag{40}$$

The eigenvectors are orthonormal, and the eigenvalues sum to 1 because $\mathrm{Tr}\rho = 1$. At the surface of the Bloch ball $\det\rho = 0$, and one of the eigenvalues vanish. Hence we have

$$\rho = |\psi\rangle\langle\psi| \ , \tag{41}$$

for some unit vector $|\psi\rangle$. Conversely, for every unit vector $|\psi\rangle$ we will obtain a density matrix lying on the Bloch sphere in this way. Let us consider the most general case. Since an overall phase factor of the vector can be chosen freely we can make things completely definite by insisting that the first non-vanishing component is real and positive, and then we get

$$|\psi\rangle = \cos\frac{\theta}{2}|e_1\rangle + \sin\frac{\theta}{2}e^{i\phi}|e_2\rangle \ , \qquad 0 \leq \theta \leq \pi \ , \quad 0 \leq \phi < 2\pi \ . \tag{42}$$

We have chosen to parametrize the state vector with angles θ and ϕ with the idea that these parameters should, in the end, serve as coordinates on a sphere.

Putting eqs. (41) and (42) together we find

$$\rho = \begin{pmatrix} \cos^2\frac{\theta}{2} & \cos\frac{\theta}{2}\sin\frac{\theta}{2}e^{-i\phi} \\ \sin\frac{\theta}{2}\cos\frac{\theta}{2}e^{i\phi} & \sin^2\frac{\theta}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \sin\theta e^{-i\phi} \\ \sin\theta e^{i\phi} & 1-\cos\theta \end{pmatrix} \ . \tag{43}$$

We can now read off the Bloch vector that describes an arbitrary pure state $|\psi\rangle$, namely

$$(x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) \ . \tag{44}$$

And we can draw a picture of the Bloch sphere, with some states of interest placed where they should be.

Let us think about the basis that was implicit in the discussion. By agreement the *computational basis* consists of the vectors

$$|e_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ \leftrightarrow \ \theta = 0 \ , \qquad |e_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ \leftrightarrow \ \theta = \pi \ . \tag{45}$$

(No pedantry here.) We place them at the north and south poles of our sphere. Another pair of orthogonal states are

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \ \leftrightarrow \ (\theta, \phi) = (\frac{\pi}{2}, 0) \ , \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \ \leftrightarrow \ (\theta, \phi) = (\frac{\pi}{2}, \pi) \ . \tag{46}$$

Orthogonal pure states always sit on antipodal points on the sphere, as far from each other as they can be. Note also that every state in the interior can be created as a mixture of pure states in infinitely many ways.

Let us draw the map of the Bloch sphere in a slightly different way. We begin with a general vector in the two dimensional Hilbert space $\mathbf{C}^2$. We are interested in vectors only up to an overall normalization and an arbitrary phase factor. It is quite convenient to remove the ambiguity by insisting that its first componenent equals 1. This works for all vectors except for those whose first component vanish. In $\mathbf{C}^2$ we miss only one state in this way, and this can be added in later. Taking the sign '$\sim$' to mean 'equal up to an overall complex factor' we write

$$|\psi\rangle \sim z_0|e_0\rangle + z_1|e_1\rangle \sim |e_0\rangle + \frac{z_1}{z_0}|e_1\rangle = |e_0\rangle + z|e_1\rangle \ . \tag{47}$$

The equality defines an arbitrary complex number z. In terms of the angles we used before we would have

$$z = \tan\frac{\theta}{2}e^{i\phi} \ . \tag{48}$$

The one-to-one correspondence between pure qubit states and the surface of a sphere now turns into the well known correspondence between the complex plane and the surface of a sphere. The 'extra' number ∞ will have to be added to the complex plane in order to ensure that the correspondence becomes one-to-one.

We write down the corresponding density matrix, normalizing as we go, and read off the Bloch vector:

$$\frac{1}{1+|z|^2}\begin{pmatrix}1\\ z\end{pmatrix}\begin{pmatrix}1 & \bar{z}\end{pmatrix}=\frac{1}{1+|z|^2}\begin{pmatrix}1 & \bar{z}\\ z & |z|^2\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1+x_3 & x_1-ix_2\\ x_1+ix_2 & 1-x_3\end{pmatrix}. \tag{49}$$

The components of the Bloch vector are denoted x_i. Clearly

$$x_1+ix_2=\frac{2z}{1+|z|^2}\qquad x_3=\frac{1-|z|^2}{1+|z|^2}\ . \tag{50}$$

The condition $x_1^2+x_2^2+x_3^2=1$ is built in, because we started from a pure state. This is the famous *stereographic projection* from the sphere to the complex plane.[11]

We have now provided two useful maps of the Bloch sphere, and we just have to fill in some physics.

Polarization states of a photon

We have just described the *qubit*, the smallest information carrying unit in quantum information theory. Many physical systems are as simple as this. However, it is often difficult to give a physical interpretation of the full set of qubit states. An example where we can do it is given by the polarization states of a photon.

The word 'photon' is a dangerous one. *Lamb* suggested that it should not be used by anyone who does not have a special license to do so. Some people *define* a photon as 'a click in a detector'. We may, however, think of a monochromatic electromagnetic plane wave travelling in the z-direction. While this is a rather different thing, the possible polarization states of the

[11] Exercise: Why do I call it a "projection"? What am I projecting from? Explain the geometric construction behind this.

two things agree, and this is what we want to parametrize. A polarization state of a plane wave is an ellipse swept out by an electric field vector orthogonal to that direction. The magnetic field sweeps out a similar ellipse. The ellipse degenerates to a line for a linearly polarized state. Why is the set of such polarization states equal to a sphere? The answer was given by *Stokes*. We will give a sketch of the details.

Keeping things quantum mechanical, imagine that you have bought a source producing 10^6 photons per second and a very expensive detector with 90 % efficiency. You also buy two Glan–Thompson prisms, at only 1000 Swedish crowns apiece. You can now prepare and measure *linear* polarization states. You arrange the source, the two prisms, and the detector along a straight line. The source and the first prism serve to *prepare* the state. The second prism together with the detector serves as a *measuring device*. Let us say that the detector clicks 10^6 times every second whenever the two prisms have the same vertical orientation. Now change the preparation by rotating the first prism an angle α away from the vertical. An accuracy of about 5 arcseconds can be achieved with a suitable goniometer. You will observe that the number of clicks go down with a factor of $\cos^2 \alpha$. When you rotate the prism through the angle π you prepare the same polarization state as the one we started out with. Evidently we have a circle's worth of linear polarization states. It is convenient to replace α with an angle that runs from 0 to 2π, so we define a one parameter family of states $\psi(e^{i\phi})$ where

$$e^{i\alpha} = \sqrt{e^{i\phi}} = \pm e^{\frac{i\phi}{2}} \ . \tag{51}$$

Now α and $\alpha + \pi$ correspond to the same state. We place this one parameter family of states on the equator of a sphere, using the stereographic coordinate $z = e^{i\phi}$.

How do we interpret the remaining points on the sphere? There should be two orthogonal *circular* polarization states, obtained as equal weight superpositions of any two orthogonal linear polarization states. (You will have to buy some more equipment in order to prepare and measure them.) We place them on the poles of our sphere. In between we have *elliptical* polarization. These can be understood by first correlating ellipses with pairs of positions on an auxiliary sphere, and again using a square root to obtain a one-to-one correspondence between oriented ellipses and points on the final Bloch sphere, with coordinates θ and ϕ. Consult Figure 5 for the idea. The

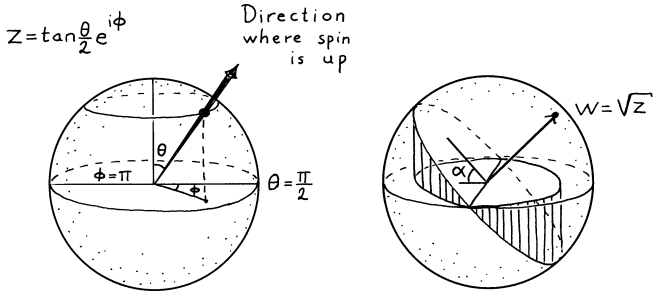


Figure 5: The physical geography of the Bloch sphere. To the left, for a spin one half silver atom. To the right, we show the first of the two steps needed to define the Stokes parameters for photon polarization states. Each oriented ellipse in the equatorial plane can be obtained by projecting two distinct great circles on the sphere down to the equatorial plane. This means that it is associated to two distinct points on that auxiliary sphere, which is coordinatized by a complex number w.

components of the resulting Bloch vector are known in optics as the *Stokes parameters*. They are indispensable for serious optics, but here we skip over the fairly complicated details of the calculation. Notice though that the specific one-to-one correspondence we have set up here is not God given. We can (and people sometimes do) change coordinates so that linear polarization states lie on the Greenwich meridian, where they are described by real state vectors. What is always true is that the linear polarization states lie on a great circle on the sphere, with pairs of physically orthogonal states (for which the relative angle of linear polarization is 90°) sitting at antipodal points.

Dynamics and distances on the qubit

In the classical theory dynamics is given by stochastic maps, degenerating to permutation matrices if pure states always evolve into other pure states. In quantum theory the general case is difficult enough to merit a chapter of its own, 'Open systems'. But we can understand those transformations that take pure states to pure states. They are simply rotations of the Bloch sphere. We

obtain them by acting with a *unitary* matrix on the pure state vectors. To see this it is enough to observe that we can obtain scalar products between Bloch vectors by turning the set of operators acting on $\mathbf{C}^d$ into a Hilbert space in its own right. The scalar product between operators is defined by

$$A \cdot B = \mathrm{Tr} A^\dagger B \ . \tag{52}$$

Notice the dagger, guaranteeing that

$$||A||^2 = \mathrm{Tr} A^\dagger A \geq 0 \ . \tag{53}$$

Clearly this scalar product is left invariant by

$$A \to UAU^\dagger \ , \quad B \to UBU^\dagger \ . \tag{54}$$

The complex dimension of the Hilbert space of operators acting on a complex Hilbert space of dimension d is d^2. This is an important idea that we will use again.

So far things do not really depend on the Hilbert space dimension d. For $d = 2$ we check that if

$$A = \frac{1}{2} \begin{pmatrix} x_3 & x_1 - ix_2 \\ x_1 + ix_2 & -x_3 \end{pmatrix} \ , \qquad B = \frac{1}{2} \begin{pmatrix} y_3 & y_1 - iy_2 \\ y_1 + iy_2 & -y_3 \end{pmatrix} \ , \tag{55}$$

then

$$\mathrm{Tr} A^\dagger B = \frac{1}{2} \vec{x} \cdot \vec{y} \ . \tag{56}$$

It follows that, in $\mathbf{C}^2$, unitary transformations can be thought of as rotations of the Bloch ball. Moreover every rotation of the Bloch ball can be obtained in this way, but this is a special feature of the qubit.

The scalar product that we have introduced defines a notion of distance between quantum states that reduces to the ordinary Euclidean distance on the Bloch ball, and on the probability simplex spanned by a set of diagonal density matrices. There is no disputing the usefulness of this, but we have already argued that if a distance is to capture the notion of statistical distinguishability it must be defined differently. If we restrict ourselves to pure states and qubits, another notion of distance between quantum states

suggests itself, namely the length of an arc of a great circle connecting the two points on the Bloch sphere. This is known as the *Fubini–Study distance*, and denoted $D_{\rm FS}$. It is an exercise to show that it is given by the formula

$$\cos^2 D_{\rm FS} = \frac{|\langle\psi|\phi\rangle|^2}{\langle\psi|\psi\rangle\langle\phi|\phi\rangle} \ , \tag{57}$$

where the vectors are not necessarily normalized.[12] It is an interesting exercise because it brings home the fact that the Bloch sphere does not sit *in* Hilbert space. A point on the Bloch sphere corresponds to an equivalence class of vectors in Hilbert space (all unit vectors differing only by a phase). So do quantum states. The formula turns out to be useful, in the same sense as the Fisher–Rao distance is useful, and it can be used regardless of the dimension of Hilbert space.

Higher dimensions

Many of the formulas for the qubit generalize immediately to Hilbert spaces of dimensions higher than two. Nevertheless the qubit is a misleadingly simple example in many ways. The set of quantum states, that is positive matrices with trace one, has d^2-1 dimensions. A general density matrix can be obtained from a diagonal one by means of a unitary transformation

$$\rho \to U\rho U^\dagger \ . \tag{58}$$

Because an overall phase does not matter it is the $SU(d)$ subgroup that acts effectively on the states. You can still think of this as a rotation in d^2-1 dimensions, but now it is a quite special rotation. This is so because the set of density matrices is no longer a sphere. In fact the surface of a sphere in d^2-1 dimensions has, in itself, d^2-2 dimensions. But the pure states can be described by vectors in $\mathbf{C}^d$, with one of the d complex numbers being irrelevant. So the set of pure states has only $2d-2$ dimensions, far less than the dimension of the surface of a sphere. The set of all states is the

[12] Exercise: Do the exercise referred to in the text. You may have to adjust the size of the sphere. Can you see why the same formula will work in every dimension?

convex hull of the pure states, and is therefore only a subset of the ball. It is well-nigh impossible to visualize the set of density matrices for $d > 2$.[13]

When $d = 2$ we expanded an arbitrary state in terms of the Pauli matrices. A Pauli matrix has eigenvalues ± 1, which means that it is both Hermitian and unitary. There are two ways to generalize the Pauli matrices to arbitrary dimensions, because you can regard them either as a basis for the set of all Hermitian matrices, or as a basis for the set of all unitary matrices in the d^2 dimensional Hilbert space of d by d matrices equipped with the trace inner product (59). Saving the second way for later, we observe that for any d one can find a set of $d^2 - 1$ Hermitian traceless matrices such that

$$\mathrm{Tr}\lambda_i\lambda_j = d\delta_{ij} \ . \tag{59}$$

Any $d \times d$ density matrix can then be written as[14]

$$\rho = \frac{1}{d}\left(\mathbf{1} + \sum_{i=1}^{d^2-1} x_i\lambda_i\right) \ . \tag{60}$$

This defines a generalized Bloch vector with components x_i, although the conditions one has to impose on this vector to ensure that ρ is positive are distinctly unpleasant.

A couple of useful facts, that you can prove by first diagonalizing ρ: A density matrix lies at the boundary of the set of density matrices if and only if it has a vanishing eigenvalue. A density matrix is pure if and only if $\mathrm{Tr}\rho^2 = 1$. This quantity obeys

$$1 \geq \mathrm{Tr}\rho^2 \geq \frac{1}{d} \ . \tag{61}$$

It is sufficiently important to have a name, *purity*.[15]

From now on we will be a bit vague about the dimension of the Hilbert space in this 'Introduction'. The dimension is arbitrary but finite when this causes no extra trouble, but you may think in terms of qubits if you so prefer.

[13]Exercise: Let ρ be a Hermitian matrix obeying $\mathrm{Tr}\rho^3 = \mathrm{Tr}\rho^2 = 1$. (In this exercise nothing else is assumed about ρ.) Prove that ρ is a pure state.

[14]Exercise: Find such a set of Hermitian matrices for $d = 3$. What instructions would you give to the computer, if you want it to produce such a set in some very high dimension?

[15]Exercise: Prove these inequalities. Also write down a formula connecting $\mathrm{Tr}M$, $\mathrm{Tr}M^2$, and $\det M$ for an arbitrary two-by-two matrix M.

A preliminary theory of measurements

In classical theory it is fairly obvious what a measurement is, and what it measures. Not so in quantum theory, and most of the discussion has to wait until we come to 'Open systems'. But we can make a start. Choose any quantum random variable, that is to say a Hermitian matrix. It has a complete set of orthonormal eigenvectors $\{|e_i\rangle\}_{i=0}^{d-1}$, and they correspond to the d mutually exclusive outcomes of an experiment. Given that the state of the system is defined by a particular density matrix ρ, the probability that a particular outcome occurs is declared to be

$$p_i = \mathrm{Tr}|e_i\rangle\langle e_i|\rho = \langle e_i|\rho|e_i\rangle \ . \tag{62}$$

These numbers are non-negative because $\rho \geq 0$ is a positive matrix, and they sum to unity because

$$\sum_i p_i = \sum_i \mathrm{Tr}|e_i\rangle\langle e_i|\rho = \mathrm{Tr}\sum_i |e_i\rangle\langle e_i|\rho = \mathrm{Tr}\rho = 1 \ . \tag{63}$$

Note carefully the steps in this calculation, which made use first of the linearity of the trace, then of the completeness of the basis, and finally of the normalization of the density matrix. The density matrix is not a probability distribution, but it stands prepared to give one for every orthonormal basis that you choose to introduce.

It is important to notice that the result of a quantum measurement cannot tell you what the state of a qubit was before the measurement, not even if you are assured that it was in some pure state. The measurement is associated to an eigenbasis unrelated to the state. If you observe the outcome associated to $|e_1\rangle$, all you can say with certainty is that the state was *not* one of the those orthogonal to $|e_1\rangle$. Every other pure state would yield that outcome with some probability.

The situation improves if you are given a large number N of qubits, and an assurance that their states are identical. Then you will obtain a probability distribution $\vec{p}$ over the eigenstates of the observable. A look at the Bloch sphere tells you that this outcome is consistent with any state lying on a certain circle at the surface of the Bloch sphere. If you have no assurance that the state ρ you are trying to determine is pure, you can only conclude that ρ lies on a disk in the Bloch ball. (The disk has a normal vector parallel

to the line that connects the two eigenstates.) In order to pin down the state exactly you will need not only a supply of many identically prepared qubits, you will also need to perform quantum measurements associated to more than one eigenbasis.[16]

There remains the question about the state of the system after the measurement. The answer depends. A photon detected as a click in a detector does not exist after the measurement. In a *projective* or *von Neumann measurement* corresponding to some Hermitian matrix, the state after the measurement is one of the eigenstates $|e_i\rangle$ of that matrix. The system 'collapses' to one of the eigenstates, with probabilities given by (62). Some more detail will be added when we come to 'Open systems', but for now it is enough to know that the notion of von Neumann measurements is useful in the lab.

Nice error bases

Let us return to the Pauli matrices, and look at them as unitary operators. We even give them new names:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{64}$$

There is one more, but we can regard it as a derived quantity because

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ . \tag{65}$$

The action on the computational basis is

$$X|0\rangle = |1\rangle , \quad X|1\rangle = |0\rangle , \qquad Z|0\rangle = |0\rangle , \quad Z|1\rangle = -|1\rangle . \tag{66}$$

X is sometimes called the *bit flip*, and Z is called the *phase flip*. Another interesting operator in this connection is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{67}$$

[16]Exercise: If your Hilbert space has dimension d, how many different measurements would you need to determine an arbitrary state ρ, given an infinite supply of identically prepared systems so that each measurement may be repeated to give a frequency?

It interchanges X and Z,

$$H^2 = \mathbf{1} \ , \qquad HXH^\dagger = Z \ , \qquad HZH^\dagger = X \ . \tag{68}$$

It is called the *Hadamard gate*, where 'gate' means 'unitary operator' in discussions of quantum computers.[17]

An important property of the set $\{\mathbf{1}, X, Z, XZ\}$ is that it forms a *unitary operator basis*. This is also known as a *nice error basis* in quantum computing, because such bases play a role in quantum error correction. What it means is that there exists a *group* with d^2 elements g_i, $g_0 = e$ being the identity element, and a set of unitary operators U_g acting on $\mathbf{C}^d$, such that

$$U_e = \mathbf{1} \ , \qquad g_i \neq e \quad \Rightarrow \quad \mathrm{Tr} U_{g_i} = 0 \ , \qquad U_{g_i} U_{g_j} \sim U_{g_i g_j} \ . \tag{69}$$

Here the sign '$\sim$' means 'equal up to a phase factor'. It follows that $U_{g_i}^\dagger = U_{g_i^{-1}}$. But then it also follows that

$$\mathrm{Tr} U_{g_i}^\dagger U_{g_j} = \begin{cases} d & \text{if} \quad i = j \\ 0 & \text{if} \quad i \neq j \ . \end{cases} \tag{70}$$

But this means that this set of unitary operators forms an orthonormal basis in the d^2-dimensional Hilbert space of all operators acting on $\mathbf{C}^d$, equipped with the natural inner product (52). Hence the name. Every operator, whether Hermitian or unitary or none of those, can be expanded as

$$A = \frac{1}{d} \sum_g U_g \mathrm{Tr} U_g^\dagger A \ , \tag{71}$$

where the sum runs over the elements in the operator basis. In the qubit example, there are four terms.

Nice error bases exist in all dimensions. One of many possibilities goes as follows: Introduce a basis $\{|i\rangle\}_{i=0}^{d-1}$ in Hilbert space, and treat the labels as integers modulo d (that is to say that $i + d = i$). Let

$$\omega = e^{\frac{2\pi i}{d}} \ . \tag{72}$$

Define two unitary operators Z and X by

[17] Exercise: How do X, Z, and H rotate the Bloch sphere? For each of them you have to find an axis of rotation and an angle.

$$Z|i\rangle = \omega^i|i\rangle \ , \qquad X|i\rangle = |i+1\rangle \ . \tag{73}$$

One can now prove that

$$X^d = Z^d = \mathbf{1} \ , \qquad ZX = \omega XZ \ . \tag{74}$$

The resulting group is called the *Weyl–Heisenberg group*. Up to phase factors it has d^2 group elements X^iZ^j, and it can be shown that these group elements form a nice error basis in dimension d.[18]

Composite systems

If, in classical probability theory, we look for the combined outcomes of n events that can be either true or false, then there are two outcomes per event but 2^n possible outcomes altogether. If n is large this gives a probability simplex of a high dimension. Quantum mechanics shows a similar exponential growth in the dimension of Hilbert space if you put several qubits together. The idea is that if you have a system composed of two parts, so that you can choose to do observations either on only one of the parts or on the whole, then the Hilbert space is the *tensor product* of the Hilbert spaces of the parts. One way of constructing the tensor product is to introduce orthonormal bases in each *factor*, say $\{|e_i\rangle\}_{i=0}^{d_1-1}$ and $\{|f_j\rangle\}_{j=0}^{d_2-1}$, and use the d_1d_2 vectors $|e_i\rangle \otimes |f_j\rangle$ as an orthonormal basis for the combined system. This is a somewhat clumsy way of expressing things, but it will do. It does not imply that every vector in the larger space is a product vector, because we can have superpositions such as

$$|\psi\rangle = \sum_{i,j} c_{ij}|e_i\rangle \otimes |f_j\rangle \ . \tag{75}$$

This is not a product vector in general.[19] You can put n qubits together by iterating the idea, and you will end up with a Hilbert space of dimension 2^n.

[18] Exercise: Write the operators X and Z as matrices for $d = 2, 3, 4$. Write out all the operators X^iZ^j for $d = 3$, and check that they form a nice error basis.

[19] Exercise: For two qubits, write down the condition that this be a product vector and compare to (7).

We can define operators of a special form, called *local* operators and denoted $A \otimes B$. They act on the basis states according to

$$A \otimes B|e_i\rangle \otimes |f_j\rangle = A|e_i\rangle \otimes B|f_j\rangle \ . \tag{76}$$

They obey obvious rules such as

$$A \otimes (B + C) = A \otimes B + A \otimes C \ , \qquad (A \otimes B)(C \otimes D) = AC \otimes BD \ . \tag{77}$$

Operators of the form $A \otimes \mathbf{1}$ and $\mathbf{1} \otimes B$ commute.

When working with components in a product basis we adopt a lexicographical ordering of the basis vectors. Thus

$$|\psi_1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \ , \quad |\psi_2\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \quad \Rightarrow \quad |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{pmatrix} \ , \tag{78}$$

$$\begin{gathered} A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \ , \quad B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} \quad \Rightarrow \\ A \otimes B = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix} \ . \end{gathered} \tag{79}$$

We frequently abbreviate $|\psi_1\rangle \otimes |\psi_2\rangle$ to $|\psi_1\rangle|\psi_2\rangle$. More drastic abbreviations are sometimes used, especially for qubits where one often abbreviates $|0\rangle \otimes |1\rangle$ and $X \otimes Z$ (say) to $|01\rangle$ and XZ.

By inspection we see that it may be useful to index the components of the density matrix, and other matrices, by a pair of indices. Thus we write

$$\rho = \sum_{i,j=0}^{d_1-1} \sum_{\alpha,\beta=0}^{d_2-1} |e_i\rangle|f_\alpha\rangle \rho^{i\alpha}{}_{j\beta} \langle e^j|\langle f^\beta| \ , \tag{80}$$

where we used both Latin and Greek indices to emphasize that the factor Hilbert spaces may have different dimensions (although the dimensions

would be the same for the two-qubit case). Here I am using the "upstairs–downstairs" notation for indices, but I will not be very consistent about it. You can think of it as just a way of keeping track of which pair of indices that label the rows, and which pair of indices that label the columns. You may prefer to have all indices down, and use a notation like $U_{i\alpha;j\beta}$, with a semicolon to separate the pairs. Whatever notation we choose we can do the same for every operator. For local operators the expressions take a quite special form. In particular

$$(A \otimes \mathbf{1})^{i\alpha}{}_{j\beta} = A^i{}_j \delta^\alpha_\beta \ , \qquad (\mathbf{1} \otimes B)^{i\alpha}{}_{j\beta} = \delta^i_j B^\alpha{}_\beta \ . \tag{81}$$

We have constructed the Hilbert space $\mathbf{C}^{d_1 d_2} = \mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$. Sometimes we will write this as $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Starting from the other end, a Hilbert space with a dimension that is a composite number can always be decomposed into a tensor product, but there are many different ways of doing so. A particular way may be preferred by the physics. Suppose that Hilbert space is four dimensional, and that we are able to identify two sets of mutually commuting operators, each of them as rich as the set of operators on a qubit. Then we declare them to be local operators of the special form that guarantee that they commute, relative to a tensor product structure defined especially for the purpose. Thus operators of the form $A \otimes \mathbf{1}$ and $\mathbf{1} \otimes B$ may be applied at opposite ends of an optical table, while non-local operators may have been applied to the system at an earlier stage. For instance, the system may be a pair of photons created in a special two-photon state by a non-linear crystal. In some experiments pairs of photons have been distributed by satellite to locations that are very far apart, and it seems obvious that whatever is done at one of the locations 'commutes' with what is done at the other location. This explains why we refer to 'local' operators, because then we really mean 'local in space'.

We have a general formula for the expectation value of any Hermitian operator A given that the state is ρ, namely

$$\langle A \rangle = \mathrm{Tr}(A\rho) \ . \tag{82}$$

But there are many situations, many more than those hinted at in the preceding paragraph, where we are only concerned with expectation values of local operators of the form $A \otimes \mathbf{1}$. Inspection of the formulas (81) suggests that there may be many complexities of ρ that do not come into play when

we calculate such expectation values. We are therefore looking for a *reduced state* density matrix ρ_1, acting only on the first factor in the tensor product, such that

$$A = A_1 \otimes \mathbf{1}_2 \quad \Rightarrow \quad \mathrm{Tr}(A\rho) = \mathrm{Tr}(A_1\rho_1) \ , \tag{83}$$

where the matrices and the trace at the end are those relevant for the factor Hilbert space $\mathcal{H}_1$. This is achieved by taking the *partial trace* of ρ, written

$$\rho_1 = \mathrm{Tr}_2\rho \ , \qquad \rho_2 = \mathrm{Tr}_1\rho \ . \tag{84}$$

The definition of the partial trace is conveniently given in the matrix representation (80), as

$$(\mathrm{Tr}_2\rho)^i{}_j = \sum_{\alpha=0}^{d_2-1} \rho^{i\alpha}{}_{j\alpha} \ , \qquad (\mathrm{Tr}_1\rho)^\alpha{}_\beta = \sum_{i=0}^{d_2-1} \rho^{i\alpha}{}_{i\beta} \ . \tag{85}$$

Clearly $\mathrm{Tr}\rho = \mathrm{Tr}_1\mathrm{Tr}_2\rho$. One can show that ρ_1, so defined, is the unique linear operator that meets the requirement (83). The importance of the reduced states ρ_1 and ρ_2 is that they encode all the information about the state ρ that can be extracted by means of operations acting only on one of the factors of the Hilbert space. Formulated in this way it sounds abstract, but it is in fact what may be going on in the lab, and elsewhere.[20]

In calculations it is often preferable to use the Dirac notation for the trace. Using the product basis we write

$$\mathrm{Tr}\rho = \sum_{i,j} {}_1\langle i|{}_2\langle j|\rho|i\rangle_1|j\rangle_2 \ , \ \ \mathrm{Tr}_2\rho = \sum_j {}_2\langle j|\rho|j\rangle_2 \ , \ \ \mathrm{Tr}_1\rho = \sum_i {}_1\langle i|\rho|i\rangle_1 \ . \tag{86}$$

Note carefully that $\mathrm{Tr}\rho$ is a number, while $\mathrm{Tr}_2\rho$ is an operator acting on $\mathcal{H}_1$. The notation has to carry quite a bit of information, eg. ${}_2\langle j|$ is a basis vector for the bra-space in the second factor of the composite Hilbert space, while $|i\rangle_1|j\rangle_2$ is a basis vector for the latter. Checking that eqs. (86) are equivalent to eqs. (85) is a good exercise.

The story does not stop at two. We can construct tensor products of an arbitrary number of Hilbert spaces, such as $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$, and trace out whatever factors we are not controlling, to obtain density matrices like

[20] Exercise: Compute the two partial traces of the matrix $A \otimes B$ given in (79).

$$\rho_{12} = \mathrm{Tr}_{34}\rho \ , \tag{87}$$

where ρ acts on the four partite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$ in this particular example.

Entanglement

The term 'entanglement' was coined by *Schrödinger*, in a far-seeing series of papers in the 1930ies. We begin by considering a pure state in a bipartite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, and ask what one can do with it using local operators only. For simplicity we assume that both the factors have the same dimension d. A general pure state can be written as

$$|\Gamma\rangle = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \Gamma_{ij} |e_i\rangle \otimes |e_j\rangle \ . \tag{88}$$

Keeping the distinction between upstairs and downstairs indices requires some sophistication when we encounter notions like the transpose of a matrix, as we soon will. The easy way out is to have all the indices in downstairs position. The tensor product sign will be omitted when it is not needed for absolute clarity.

The vector $|\Gamma\rangle$ is a product vector if there exist vectors $\vec{\alpha}$ and $\vec{\beta}$ such that

$$\Gamma_{ij} = \alpha_i \beta_j \ . \tag{89}$$

The state is then said to be *separable*. If it is not separable it is said to be *entangled*, but entanglement is (as we will see) a question of degree. Now let us act on the state with a local unitary $U \otimes V$. The result, using the notation we just introduced, is[21]

$$U \otimes V |\Gamma\rangle = \frac{1}{\sqrt{d}} \sum_{i,j,k,l} U_{ik} V_{jl} \Gamma_{kl} |e_i\rangle |e_j\rangle = |U \Gamma V^{\mathrm{T}}\rangle \ . \tag{90}$$

This is alarming at first sight. Let us choose $\Gamma_{ij} = \delta_{ij}$. This gives the *Jamiołkowski state* $|\delta\rangle$,

[21] Exercise: Perform the calculation, using Dirac notation very carefully.

$$|\delta\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i\rangle|e_i\rangle \ . \tag{91}$$

We see that

$$U \otimes \mathbf{1}|\delta\rangle = |U\rangle \ , \qquad \mathbf{1} \otimes V|\delta\rangle = |V^{\mathrm{T}}\rangle \ . \tag{92}$$

Everything that Alice can do acting with $U \otimes \mathbf{1}$ can be done by Bob as well, if he acts with $\mathbf{1} \otimes U^{\mathrm{T}}$. Does this means that information can be transmitted by the state in a non-local way?

Recall that all the information that Alice can extract from the state must come from the partial trace of the density matrix, and similarly for Bob. For any state $|U\rangle$ for which U is a unitary matrix (this includes the Jamiołkowski state) we can calculate

$$\rho_1 = \mathrm{Tr}_2|U\rangle\langle U| = \frac{1}{d}\mathbf{1} \ , \qquad \rho_2 = \mathrm{Tr}_1|U\rangle\langle U| = \frac{1}{d}\mathbf{1} \ . \tag{93}$$

In both cases this is the maximally mixed state for dimension d.[22] It means that neither Alice nor Bob can make any useful prediction about the experiments that they carry out on their own, using operators of the form $A \otimes \mathbf{1}$ and $\mathbf{1} \otimes B$ respectively. This is true for Bob regardless of what Alice does to the state, and conversely. Alice and Bob will have to cooperate, and use non-local operations, if they want something more specific to come out of the Jamiołkowski state. No information was transmitted in (92).

The Schmidt decomposition

We will now introduce one of the working horses of entanglement theory, the *Schmidt decomposition*. It concerns bipartite Hilbert spaces that are tensor products of the form $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$, where we may as well assume that $d_1 \leq d_2$. We start out with any choice of bases $\{|e_i^{(1)}\rangle\}_{i=1}^{d_1}$ and $\{|e_i^{(2)}\rangle\}_{i=1}^{d_2}$ in the two factors, and consider an arbitary pure state $|\Psi\rangle$ in the composite Hilbert space. Then the claim is that we can introduce new bases in the two factor Hilbert spaces, adapted to the state and denoted by $\{|e_i\rangle\}$ for both factors, such that

[22] Exercise: Perform the calculation. Also try the two qubit state $|\psi\rangle = z_0|00\rangle + z_1|11\rangle$.

$$|\Psi\rangle = \sum_{i=1}^{d_1}\sum_{j=1}^{d_2}\Gamma_{ij}|e_i^{(1)}\rangle|e_j^{(2)}\rangle = \sum_{i=1}^{d_1}\sqrt{p_i}|e_i\rangle|e_i\rangle \ . \tag{94}$$

Here the p_i are non-negative numbers, and so are their square roots. The double sum has been converted to a single sum. Some important consequences follow immediately, but first we have to prove that this can always be made to work.

Here we can rely on the *singular value decomposition* of the matrix Γ_{ij}, but we can also do it directly. What we need to know is that for any matrix A the matrix $AA^\dagger$ is Hermitean with non-negative eigenvalues, hence that $\sqrt{AA^\dagger}$ can be defined in a natural way, and finally that there always exist a unitary matrix U such that

$$A = \sqrt{AA^\dagger}U \ . \tag{95}$$

I hope this looks plausible.[23] For 1×1 matrices it is the usual way of writing a complex number as $z = re^{i\phi}$.

Now we apply this to the matrix Γ that occurs in equation (94). We also decide to use unitary operators to diagonalize the Hermitean matrix we encounter. Hence

$$\Gamma = \sqrt{\Gamma\Gamma^\dagger}U = U_1 D U_1^\dagger U = U_1 D U_2 \ , \tag{96}$$

where D is a diagonal matrix whose eigenvalues we denote by $\sqrt{p_i}$. We can then show that

$$|\Psi\rangle = \sum_{i,j,k,l} U_{1ik}D_{kl}U_{2lj}|e_i^{(1)}\rangle|e_j^{(2)}\rangle = \sum_{i,j,k,l} D_{kl}\left(|e_i^{(1)}\rangle U_{1ik}\right)\left(|e_j^{(2)}\rangle U_{2jl}^{\mathrm{T}}\right) \ . \tag{97}$$

The adapted bases that we are going to introduce are then

$$|e_k\rangle = |e_i^{(1)}\rangle U_{1ik} \ , \qquad |e_l\rangle = |e_j^{(2)}\rangle U_{2jl}^{\mathrm{T}} \ . \tag{98}$$

We use the same notation for both bases, even if the basis in $\mathbf{C}^{d_2}$ may have more members than that in $\mathbf{C}^{d_1}$. Then we finish the calculation with

[23] Exercise: Prove the three claims I made, perhaps under the simplifying assumption that all the eigenvalues of $\sqrt{AA^\dagger}$ are non-zero. Also look up "singular value decomposition" to see what it is.

$$|\Psi\rangle = \sum_{k,l} D_{kl}|e_k\rangle|e_l\rangle = \sum_{k,l} \sqrt{p_k}\delta_{kl}|e_k\rangle|e_l\rangle = \sum_k \sqrt{p_k}|e_k\rangle|e_k\rangle \ . \qquad (99)$$

It is done.

We can now prove[24] that the reduced density matrices take a transparent form when we use the adapted basis:

$$\rho_1 = \mathrm{Tr}_2|\Psi\rangle\langle\Psi| = \begin{pmatrix} p_1 & & \\ & \ddots & \\ & & p_{d_1} \end{pmatrix} = \mathrm{Tr}_1|\Psi\rangle\langle\Psi| = \rho_2 \ . \qquad (100)$$

This reveals that the bases we introduced in order to write the basis in the Schmidt form are precisely the bases in which the reduced density matrices are diagonal.

We also learn that the reduced density matrices have the same spectrum, except that if $d_2 > d_1$ there are additional zero eigenvalues in ρ_2. Let us ignore the latter complication. The eigenvalues p_i are *entanglement invariants* in the sense that they cannot be changed by local unitary operations. A pure state is separable if one eigenvalue equals 1 and the rest are zero. A state is *maximally entangled* if all the eigenvalues are equal, that is to say if the reduced states are maximally mixed.

Entanglement theory

Entanglement theory offers a new analogue of the venerable complementarity between position and momentum. If we place a particle in a position eigenstate we can make no prediction about its momentum. If we place a system in a maximally entangled state we can make no prediction about the outcomes of local measurements. All our information is about their correlations.

There is much more to the story. It is usually told from the perspective of *local operations and classical communication*. Then the operations are unitary transformations and measurements associated to operators like $A\otimes\mathbf{1}$ and $\mathbf{1}\otimes B$. The parties are allowed to communicate with each other, so that Alice can suggest to Bob which particular operation he should apply. The theory treats local operations as if they were for free, while entangling

[24]Exercise: Do it!

operations are expensive. Separable states can be transformed into each other for free, and pure states with isospectral reduced density matrices can be transformed into each other for free, but it is expensive to turn a separable state into an entangled one. We can define the *entanglement cost* of a state ρ as the minimum number m of maximally entangled states needed to create n copies of ρ, or more precisely as the quotient m/n in the limit of large n. We can define the *distillable entanglement* of a state ρ similarly, in terms of the number of maximally entangled states one can create from a number of copies of ρ. (Curiously, these are not equal.)

And we can generalize bipartite entanglement to tripartite or multipartite entanglement. Let me just say that this is not easy. One reason is that the Schmidt decomposition works only in the bipartite case.

The no-cloning property

Here is a simple observation one should know about: It is impossible to construct a machine that inputs an arbitrary quantum state and outputs two copies of the same state. Let us prove this for pure states. Our machine effects some unitary transformation. We need a unitary transformation in a two-particle Hilbert space $\mathcal{H} \otimes \mathcal{H}$, so that

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \ , \tag{101}$$

for every state $|\psi\rangle$. Let $|e_1\rangle$ and $|e_2\rangle$ be two orthogonal states in $\mathcal{H}$. It must be the case that

$$U(|e_1\rangle \otimes |0\rangle) = |e_1\rangle \otimes |e_1\rangle \ , \qquad U(|e_2\rangle \otimes |0\rangle) = |e_2\rangle \otimes |e_2\rangle \ . \tag{102}$$

Now consider the state $|\psi\rangle = z_1|e_1\rangle + z_2|e_2\rangle$. By linearity

$$\begin{aligned} U(|\psi\rangle \otimes |0\rangle) = U(z_1|e_1\rangle \otimes |0\rangle + z_2|e_2\rangle \otimes |0\rangle) = \\ = z_1 U(|e_1\rangle \otimes |0\rangle) + z_2 U(|e_2\rangle \otimes |0\rangle) = z_1|e_1\rangle \otimes |e_1\rangle + z_2|e_2\rangle \otimes |e_2\rangle \ . \end{aligned} \tag{103}$$

But

$$z_1|e_1\rangle \otimes |e_1\rangle + z_2|e_2\rangle \otimes |e_2\rangle \neq (z_1|e_1\rangle + z_2|e_2\rangle) \otimes (z_1|e_1\rangle + z_2|e_2\rangle) \ . \tag{104}$$

And what we have on the right hand side here is $|\psi\rangle \otimes |\psi\rangle$. End of proof.

Note that were it possible to clone an unknown state, we could perform a large number of measurements on a large number of copies, and in this way determine the state. But this way is blocked.

The no-cloning theorem is not the end of the story. We can still ask for a unitary operator that minimizes the maximal copying error over all possible states. The answer is known, but we go on to other matters.[25]

Quantum teleportation

It is time to introduce Alice and Bob, the pair that does all the quantum communication so far discussed in the literature. Alice is in possession of a system in an unknown quantum state. She wants to transmit this state to Bob without moving her actual system. The idea is that she simply reaches for a classical telephone and sends instructions enabling Bob to put a system of his in the same state. Given that unknown quantum states cannot be copied, and given that Alice does not know what state $|\psi\rangle$ her system is in—indeed, by the quantum theory of measurement, she cannot find it out—this sounds like a tall order.

I will first present the solution in complete generality, and afterwards specialize to qubits to make sure that we understand what is going on. The starting point is a nice error basis. Suppose that $\{U_I\}_{I=0}^{d^2-1}$ is a nice error basis (or, more generally, a unitary operator basis—since we are not doing quantum error correction yet, it does not have to form a group). Using one of these unitaries to replace the matrix Γ in (88) gives a maximally entangled state, as you can check by taking the partial trace of $|U_I\rangle\langle U_I|$. To be explicit about it,

$$|U\rangle\langle U| = \frac{1}{d}\left(\sum_{i,j} U^{ij}|i\rangle|j\rangle\right)\left(\sum_{k,l}\langle k|\langle l|U^*_{kl}\right) = \frac{1}{d}\sum_{i,j,k,l}|i\rangle|j\rangle U^{ij}U^*_{kl}\langle k|\langle l| \ . \tag{105}$$

[25]Exercise: Suppose there is a unitary such that $U|\psi\rangle\otimes|0\rangle \approx |\psi\rangle\otimes|\psi\rangle$ and $U|\phi\rangle\otimes|0\rangle \approx |\phi\rangle\otimes|\phi\rangle$ for two different states $|\psi\rangle$ and $|\phi\rangle$, leaving the meaning of 'approximately' a little vague. Argue that it must hold that $\langle\phi|\psi\rangle$ is close to either 0 or 1.

Now take the partial traces following the recipe (85), remembering that U is a unitary matrix. We asssumed that the matrices form a unitary operator basis, which means that

$$\langle U_I|U_J\rangle = \frac{1}{d}\mathrm{Tr}U_I^\dagger U_J = \delta_{IJ} \ . \tag{106}$$

To sum up, from a unitary operator basis we have created an orthonormal basis consisting solely of maximally entangled states.[26] Alice must be sophisticated enough so that she can perform a von Neumann measurement using this basis.

Next Alice and Bob create a Jamiołkowski state, and share it out between them. The total Hilbert space is a tensor product of three factors (of equal dimension). Alice controls the first two factors, Bob (situated elsewhere) controls the third. The shared entangled state sits in the tensor product of the last two factors. The state to be teleported, $|\psi\rangle$, is in the first factor.

When the teleportation is about to start, the state is

$$|\psi\rangle_1|\delta\rangle_{23} = \mathbf{1}_{12}\otimes\mathbf{1}_3|\psi\rangle_1|\delta\rangle_{23} = \left(\sum_{I=0}^{d^2-1}|U_I\rangle_{12}\langle U_I|\otimes\mathbf{1}_3\right)|\psi\rangle_1|\delta\rangle_{23} \ . \tag{107}$$

The equality here is just an odd way to rewrite the expression for the state, using a special basis for the $\mathcal{H}_{12}$ factor. It is an exercise to show that this rewriting can be continued to[27]

$$|\psi\rangle_1|\delta\rangle_{23} = \frac{1}{d}\sum_{I=0}^{d^2-1}|U_I\rangle_{12}|U_I^\dagger\psi\rangle_3 \ . \tag{108}$$

So far nothing has happened. But now Alice performs her von Neumann measurement. After looking at the outcome, she finds that the state has collapsed to an eigenstate in $\mathcal{H}_{12}$, namely, one of the states in the unitary operator basis. At this point Alice reaches for the classical phone, and tells

[26] Exercise: Write down the basis obtained from the nice error basis provided by the Pauli matrices, and for the one provided by the Weyl–Heisenberg group for $d = 3$, in fully explicit form. You should see a *Latin square* and the matrix that gives rise to the *discrete Fourier transform* in front of you.

[27] Exercise: Do this exercise.

Bob to apply one out of the d^2 unitary operators to the state he controls. As a result of this two-step process

$$|\psi\rangle_1|\delta\rangle_{23} \quad \rightarrow \quad |U_I\rangle_{12}U_I^\dagger|\psi\rangle_3 \quad \rightarrow \quad |U_I\rangle_{12}|\psi\rangle_3 \ . \tag{109}$$

The transfer of the unknown qubit state $|\psi\rangle$ from Alice to Bob is complete. Alice ends up with all the entanglement. Neither of them have gained any information about what the state $|\psi\rangle$ is.

Now let us specialize to qubits. We start with the state

$$\begin{aligned} |\psi\rangle|\delta\rangle &= \frac{1}{\sqrt{2}}(z_0|0\rangle + z_1|1\rangle)(|00\rangle + |11\rangle) = \\ &= \frac{z_0}{\sqrt{2}}|00\rangle|0\rangle + \frac{z_0}{\sqrt{2}}|01\rangle|1\rangle + \frac{z_1}{\sqrt{2}}|10\rangle|0\rangle + \frac{z_1}{\sqrt{2}}|11\rangle|1\rangle \ . \end{aligned} \tag{110}$$

We introduce the maximally entangled *Bell basis*

$$\begin{aligned} |U_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ , \qquad |U_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \ , \\ |U_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \ , \qquad |U_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \ . \end{aligned} \tag{111}$$

A quick calculation shows that

$$\begin{aligned} \langle U_0|00\rangle &= \frac{1}{\sqrt{2}} = \langle U_0|11\rangle \ , \qquad \langle U_1|00\rangle = \frac{1}{\sqrt{2}} = -\langle U_1|11\rangle \ , \\ \langle U_2|01\rangle &= \frac{1}{\sqrt{2}} = \langle U_2|10\rangle \ , \qquad \langle U_3|01\rangle = \frac{1}{\sqrt{2}} = -\langle U_3|10\rangle \ . \end{aligned}$$

The remaining scalar products vanish. We can now take the step from (107) to (108), and obtain

$$\begin{aligned} |\psi\rangle|\delta\rangle = \frac{1}{2}|U_0\rangle(z_0|0\rangle + z_1|1\rangle) + \frac{1}{2}|U_1\rangle(z_0|0\rangle - z_1|1\rangle) + \\ + \frac{1}{2}|U_2\rangle(z_0|1\rangle + z_1|0\rangle) + \frac{1}{2}|U_3\rangle(z_0|1\rangle - z_1|0\rangle) \ . \end{aligned} \tag{112}$$

A Bell measurement by Alice will not tell her what the amplitudes z_0 and z_1 are, but it does tell her what action Bob must take to transform his state into a copy of the original. The choice is between four possibilities, so the message she sends contains exactly two classical bits, in the language we will introduce later.[28]

The BB84 protocol

This introduction would be incomplete if we did not give an example of a quantum communication protocol that one can actually buy on the market. It concerns cryptography. Readers of *Poe* and *Conan Doyle* will know that encrypted messages can be cracked by statistical analysis. But there is a way of encrypting messages that will never yield to such methods. Suppose Alice wishes to encrypt a message to be sent in binary digits, such as 000111000 (or preferably something longer, to which statistical analysis can be applied). Suppose that Alice and Bob share a sequence of random digits of the same length, such as 101101100. (I constructed this sequence by flipping a coin. This is not a very good method. In fact, since random sequences are valuable, constructing them by quantum mechanical means is another useful application of quantum mechanics.) Alice now adds the two sequences digit by digit, and sends the sequence 101010100 to Bob. Bob subtracts the random sequence from the sequence he received, and obtains the sequence that Alice wanted to convey. This way of encrypting a message is known as the *Vignère* cipher, and it is in principle unbreakable because the sequence being sent shares complete randomness with the key. The catch with the idea is that it assumes that Alice and Bob do share copies of the same random sequence. The BB84 protocol offers a way of sending such a random sequence over an open channel, with a built-in guarantee that Alice and Bob can detect whether an eavesdropper has been listening in.

Alice starts with a secret sequence of 0s and 1s, rather longer in fact than the one needed to encrypt the message. She selects, at random and in secret, either X or Z, and encodes a binary digit by preparing a qubit in an

[28]Exercise: Alice creates a pair of maximally entangled photons, and Bob does likewise. Each of them sends one of their photons to Charlie. Design a measurement that Charlie can do, which forces the photons kept by Alice and Bob to be in a maximally entangled state (even though these two photons have never interacted with each other).

eigenstate of the gate she selected. She sends the qubit to Bob, who selects either X or Z and measures the outcome. If they made the same choices, the binary digit has been successfully transferred (because we are ignoring all practical difficulties with noise in the communication channel). If not, Bob's digit is not at all determined by Alice's. After doing this many times, Alice announces, over a telephone line that anyone can listen in to, what choices she made in the preparation. Bob replies with a list of those measurements he made where his choice agrees with Alice's. They both delete those elements of the sequence for which their choices disagreed. Having done so, they share identical random sequences, selected at random from the longer sequence that Alice started out with.

The claim is that this is an absolutely safe way to transmit a random sequence. To see why this is so, suppose an eavesdropper (called Eve) tries to listen in. Since no information about the actual digits has been sent over the telephone line, she must inform herself about the state of the qubits that were sent. This means that she must intercept and measure a qubit. But should she measure in the X or in the Z basis? She has to make a choice. Sometimes her choice will not be the same as Alice's, and then Alice's preparation is undone. When Eve sends the qubit on to Bob (to hide the fact that she is listening in) she destroys the perfect correlation between Alice and Bob that should have been there whenever they made the same choices between X and Z.

This means that Alice and Bob can test whether Eve has been listening. Alice sends a part of the shared random sequence to Bob over the public telephone line. Bob examines it and if it agrees with what he has, he knows that no-one has tampered with the qubit transmission. He informs Alice accordingly, and the secretive pair can use the remainder of the shared random sequence to encipher their messages using the unbreakable Vignère cipher.

It remains to add that companies that sell hardware for quantum key distribution are making excellent profits. Before being carried away by this, notice that this is in some ways a very simple application of quantum information theory because it does not involve any actual processing of quantum states, and it does not require us to store quantum states in memories.

Bell inequalities

Bell inequalities were introduced in the 1960ies by *Bell* to show that quantum mechanics gives predictions that cannot be obtained from any 'hidden variable' theory. We do not discuss hidden variables here, but it is to be noted that the inequalities arise in classical probability theory. The quantum part of the story is precisely that they do not hold, in situations where you might have expected them to hold.

We begin by defining a few *correlation polytopes*. A polytope is the convex hull of a finite set of points, and is bounded by a finite set of faces (called *facets* if their dimension is larger than two). A simple correlation polytope is obtained by first choosing three events a_i, each of which may occur in some experiment. We can make a truth table for the events, as follows

$$\begin{array}{c|cccccccc} a_1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ a_2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ a_3 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} \tag{113}$$

The first column covers the case when none of the events happen, the second when only a_1 happens, and so on. Each column can be regarded as a vector in a three-dimensional space, and together these vectors form the corners of a cube—which is a polytope. If the experiment is repeated N times each event will occur n_i times, and is hence associated with a frequency $\nu_i = n_i/N$. The argument to follow applies directly to the observed frequencies as well as to the probabilities that emerge in the limit. This means that when you have done the experiment N times you will have obtained three non-negative numbers p_i, none of which can be larger than 1. They do not have to sum to 1 because the events are not mutually exclusive.

So we have found that the possible outcomes of the N experiments taken together can be labelled by three numbers p_i, which by construction obey the inequalities

$$0 \leq p_1 \leq 1 \ , \quad 0 \leq p_2 \leq 1 \ , \quad 0 \leq p_3 \leq 1 \ . \tag{114}$$

This is related to a dual description of the cube in terms of these six inequalities, each of which says that the cube lies on one side of some two-dimensional plane. Every compact convex set admits two dual descriptions along these lines, one of which describes the body as the convex hull of a set of pure points, and one of which describes it as the intersection of a set

of half-spaces. In both cases we are looking for a minimal description of its kind.

Things get more interesting if there are logical connections between the events. For instance, we can assume that the three events are mutually exclusive, so that exactly one of the events happens in each run of the experiment. Only three columns of the truth table survives, there are only three pure points left, and the observed frequencies necessarily obey the condition

$$p_1 + p_2 + p_3 = 1 \ . \tag{115}$$

This is the case we started out with.

Another interesting restriction is to impose the logical condition that $a_3 = a_1 \& a_2$, that is to say that the event a_3 is that both a_1 and a_2 happen. This gives the truth table

$$\begin{array}{r|cccc} a_1 & 0 & 1 & 0 & 1 \\ a_2 & 0 & 0 & 1 & 1 \\ a_1 \& a_2 & 0 & 0 & 0 & 1 \end{array} \tag{116}$$

The convex hull of the four column vectors is a polytope inscribed in the cube. Its dual description in terms of inequalities describing the faces of the polytope is

$$p_3 \geq 0 \ , \quad p_1 \geq p_3 \ , \quad p_2 \geq p_3 \ , \tag{117}$$

$$p_1 + p_2 - p_3 \leq 1 \ . \tag{118}$$

The last of these may be a little hard to see, but—like the other three faces—it defines a face passing through exactly three of the vertices, namely in this case the last three of the columns of the truth table. See Fig. 6. Slightly more involved examples of this last kind of inequality are known as *Bell inequalities*. We will see that they may fail to hold in quantum theory, and must try to understand why.

To get an interesting Bell inequality, consider eight events a_1, a_2, a_3, a_4, $a_1 \& a_3, a_1 \& a_4, a_2 \& a_3, a_2 \& a_4$. The truth table will produce vectors with eight components, in fact 16 vectors altogether, and we do not write it out here. The inequalities of interest to us are

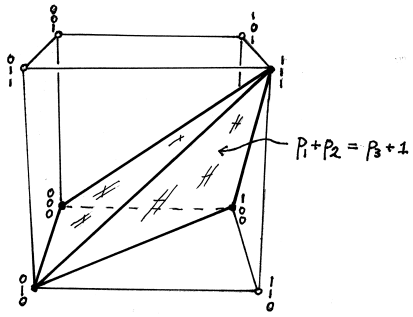


Figure 6: A correlation polytope for three logically connected events.

$$-1 \leq p_{1,3} + p_{1,4} + p_{2,4} - p_{2,3} - p_1 - p_4 \leq 0 \tag{119}$$

$$-1 \leq p_{2,3} + p_{2,4} + p_{1,4} - p_{1,3} - p_2 - p_4 \leq 0 \tag{120}$$

$$-1 \leq p_{1,4} + p_{1,3} + p_{2,3} - p_{2,4} - p_1 - p_3 \leq 0 \tag{121}$$

$$-1 \leq p_{2,4} + p_{2,3} + p_{1,3} - p_{1,4} - p_2 - p_3 \leq 0 \ . \tag{122}$$

You can check that they hold by making all possible truth assignments to the four events a_1, a_2, a_3, a_4.[29]

To each event a_i there will correspond an observable α_i taking values $+1$ if the event happens, 0 if it does not. There will be corresponding expectation values

$$p_i = \langle \alpha_i \rangle \ , \qquad p_{i,j} = \langle \alpha_i \alpha_j \rangle \ . \tag{123}$$

It is customary to introduce observables $A_i = 2\alpha_i - 1$, and to rewrite the inequalities in terms of

$$\langle A_i A_j \rangle = \langle 4\alpha_i \alpha_j - \alpha_i - \alpha_j + 1 \rangle = 4p_{i,j} - 2p_i - 2p_j + 1 \ . \tag{124}$$

Finally we rename A_3 as B_1 and A_4 as B_2. Inequality (119) then takes the form

[29]Exercise: Do it. Also rewrite (119) in the form (125).

$$-2 \leq \langle A_1 B_1 + A_1 B_2 + A_2 B_2 - A_2 B_1 \rangle \leq 2 \ . \tag{125}$$

Written in this form it is known as the *Clauser–Horne–Shimony–Holt* inequality. It has to hold for the individual outcomes and for the observed frequencies in any experiment measuring these random variables.

Now let A_1, A_2 be operators corresponding to measurements that can be made by Alice, while B_1, B_2 can be made by Bob. The possible outcomes are ± 1 in all cases. In a single run of the experiment only one of $A_1 \otimes B_1$, $A_1 \otimes B_2$, $A_2 \otimes B_1$, $A_2 \otimes B_2$, can be measured. But many measurements of each kind will be made, and it seems reasonable to assume that, once the statistics is collected, it will be true that

$$\langle A_1 B_1 + A_1 B_2 + A_2 B_2 - A_2 B_1 \rangle = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_2 \rangle - \langle A_2 B_1 \rangle \ . \tag{126}$$

In quantum mechanics the left and right hand side are necessarily equal to each other, and both can be computed once we know what state the system is in. The argument for the CHSH inequality applies to the left hand side. The right hand side will be measured. Its first term is evaluated by collecting the statistics from those instances of the experiment in which the settings were made so that $A_1 \otimes B_1$ was measured, and so on. The system, in most experiments, consists of a pair of photons in a carefully prepared entangled state. In the best experiments the choice of settings is done when the pair of photons are well on their way, and every effort is made to ensure that the choice is made in a random fashion on both sides. But now we do have a problem, namely Problem 1.

Problem 1: To test the CHSH inequality Alice and Bob use

$$\begin{gathered} A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \mathbf{1} \ , \qquad A_2 = \begin{pmatrix} 0 & e^{-i\alpha} \\ e^{i\alpha} & 0 \end{pmatrix} \otimes \mathbf{1} \ , \\ B_1 = \mathbf{1} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \qquad B_2 = \mathbf{1} \otimes \begin{pmatrix} 0 & e^{-i\alpha} \\ e^{i\alpha} & 0 \end{pmatrix} \ . \end{gathered} \tag{127}$$

They can vary α. What do these measurements correspond to if they are measuring photon polarization? What is the largest value they can obtain for the quantity in the CHSH inequality? What quantum state gives this value?

Problem 2: Consider two quantum states, anywhere on the Bloch sphere. Choose a Hermitian matrix A, and expand the two states in its eigenbasis. Calculate the Fisher–Rao distance between the two states, in terms of the expansion coefficients, for the two-outcome measurement corresponding to A. Prove that by varying A this distance can be made equal to the Fubini–Study distance, but that it cannot be made larger.

OPEN SYSTEMS

The theory of open systems deals with situations where the system of interest is not fully isolated from its environment. It regards the world as divided into a 'system' and a 'reservoir', where the latter is not controlled by the experimentalist. Sometimes the reservoir is useful when one wants to manipulate the system, and then it may be called an 'ancilla'. If the system becomes entangled with the reservoir the split of the whole into its parts becomes a subtle matter. The brief account here is mostly concerned with the theory of quantum measurements.

The chicken and the egg

Let us summarize the message of the Schmidt decomposition (94):

- Let ρ_{12} be a pure state on $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Then the reduced states $\rho_1 = \mathrm{Tr}_2\rho_{12}$ and $\rho_2 = \mathrm{Tr}_1\rho_{12}$ have the same non-zero eigenvalues.
- Given a state ρ_1 on $\mathcal{H}_1$ there exists a Hilbert space $\mathcal{H}_2$ and a pure state $|\psi\rangle$ in $\mathcal{H}_{12}$ such that $\rho_1 = \mathrm{Tr}_2|\psi\rangle\langle\psi|$.

In these notes density matrices were introduced first, and Hilbert space vectors were added almost as an afterthought. Many accounts start at the other end, density matrices appearing only when the state of the system has not been specified as completely as it could be. What is the correct starting point? The Schmidt decomposition turns this into a chicken-and-egg question because any mixed state can be *purified*, and regarded as a pure state in a larger Hilbert space partly outside our control.

Either way we have a concrete question concerning time evolution to discuss. Were the system isolated it would evolve *unitarily* according to

$$\rho \quad \rightarrow \quad U\rho U^\dagger \ . \tag{128}$$

If the unitary is of the form $U = e^{-iHt}$ this becomes the differential equation

$$\frac{d\rho}{dt} = i[\rho, H] \ . \tag{129}$$

We will want to know how the density matrix on $\mathcal{H}_1$ evolves if we extend it to a state on the larger Hilbert space $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$, evolve that state with a unitary, and take the partial trace down to $\mathcal{H}_1$ at the end.

CP maps

It is convenient to assume that there are no correlations between the state and its environment to begin with. In fact we assume that the initial state is

$$\rho_S \otimes \rho_R^0 \ , \tag{130}$$

where the initial state ρ_R^0 of the reservoir is pure

$$\rho_R^0 = |R_0\rangle\langle R_0| \ . \tag{131}$$

The second assumption is harmless because we can consider a Hilbert space large enough so that it holds. The assumption that we start out with a product state is not harmless, but it is an interesting one to make. It holds if the environment has no memory of any past interactions with the system. To see whether this is so requires a detailed analysis of the physics. For instance, it seems plausible that it holds if the reservoir consists of photons that come from afar and then quickly disappear to very large distances.

We now evolve the state (130) with a unitary U acting on the full Hilbert space, and then take the partial trace using an orthonormal basis $\{|i_R\rangle\}$ for $\mathcal{H}_R$. We find

$$\rho_S \to \mathrm{Tr}_R U \left(\rho_S \otimes \rho_R^0\right) U^\dagger = \sum_i \langle i_R|U|R_0\rangle \rho_S \langle R_0|U^\dagger|i_R\rangle \ . \tag{132}$$

The sum will have to include all non-zero terms. Whatever their number is, the answer has an interesting form.

We define the *Kraus operators* A_i by

$$A_i = \langle i_R|U|R_0\rangle \ . \tag{133}$$

If you remember that U operates on the Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_R$, it will be

obvious that this is an operator on the Hilbert space of the system.[30] By construction

$$\sum_i A_i^\dagger A_i = \sum_i \langle R_0|U^\dagger|i_R\rangle\langle i_R|U|R_0\rangle = \langle R_0|U^\dagger U|R_0\rangle = \mathbf{1}_S \ . \tag{134}$$

Conversely, it can be shown that every set of operators A_i obeying the last equality can be obtained in this way from some unitary U.

We have arrived at the notion of a *completely positive map*, which is the quantum version of the linear maps (10) that take probability vectors to probability vectors. A map Φ taking density matrices to density matrices is completely positive if and only if there exists a set of Kraus operators A_i such that

$$\rho \to \Phi(\rho) = \sum_i A_i \rho A_i^\dagger \quad \text{where} \quad \sum_i A_i^\dagger A_i = \mathbf{1} \ . \tag{135}$$

This is clearly a linear map,

$$a_1\rho_1 + a_2\rho_2 \to a_1 \sum_i A_i\rho_1 A_i^\dagger + a_2 \sum_i A_i \rho_2 A_i^\dagger \ . \tag{136}$$

If you rearrange the density matrix so that it forms a vector with d^2 components, the CP map Φ becomes a $d^2 \times d^2$ matrix. If you like, it is a *superoperator* acting on operators. The trace and the positivity of ρ is preserved by the map, so it takes density matrices to density matrices.[31] But positivity is not enough. There is more to it. The extra ingredient leading to complete positivity and to the Kraus form comes about in a rather strange way, as we will see.

Positive maps and entangled states

A linear map from matrices to matrices is said to be *positive* if it takes positive matrices to positive matrices. It is very difficult to describe positive

[30] Exercise: Expand U in a product basis for the composite Hilbert space (letting $|R_0\rangle$ be one of the basis vectors in one of the factors). Then calculate the Kraus operators. Note that many different Us correspond to the same set of A_i.

[31] Exercise: Prove this.

maps in general, but a simple example of a positive map is $\rho \to \rho^{\mathrm{T}}$. The transposed matrix has the same spectrum as the original, so this is clearly a trace preserving positive map. But suppose our Hilbert space is $\mathbf{C}^2 \otimes \mathbf{C}^2$. As usual, Alice controls only the first factor, so she performs a *partial transpose* of the density matrix. That is, using the notation (80), she performs the map

$$\rho^{i\alpha}{}_{j\beta} \to \rho^{j\alpha}{}_{i\beta} \ . \tag{137}$$

A little more abstractly, this is

$$\rho \to \rho^{\mathrm{T}_A} \ . \tag{138}$$

(It is understood that Alice 'performs' the map using pen and paper only. It does not correspond to a physical transformation, as we will see.) Let us take it that the density matrix is pure,

$$\rho = |\psi\rangle\langle\psi| \ , \qquad |\psi\rangle = \sqrt{p_0}|0\rangle|0\rangle + \sqrt{p_1}e^{i\nu}|1\rangle|1\rangle \ , \quad p_0 + p_1 = 1 \ . \tag{139}$$

The problem is that when the partial transposition is performed the spectrum of the density matrix changes according to

$$(1,0,0,0) \to (p_0, p_1, \sqrt{p_0 p_1}, -\sqrt{p_0 p_1}) \ . \tag{140}$$

Unless the state vector is a product vector negative eigenvalues appear. The matrix is not a density matrix any more.[32]

The definition of completely positive maps avoids this difficulty. Let us represent positive maps as $d^2 \times d^2$ matrices Φ. The density matrices, on which the maps are acting, act in their turn on a Hilbert space $\mathcal{H}_S$. This Hilbert space can be enlarged to a Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_R$, but let us agree that the second factor is irrelevant, so that we perform only positive maps of the form $\Phi \otimes \mathbf{1}$. The partial transposition is of this form. By definition the map Φ is said to be completely positive if $\Phi \otimes \mathbf{1}$ is positive for all possible extensions $\mathcal{H}_S \to \mathcal{H}_S \otimes \mathcal{H}_R$.

Stinespring's dilation theorem: A map is completely positive and trace preserving if and only if it can be written in the Kraus form (135).

[32]Exercise: Do this calculation. Do the same for the case when Bob takes the partial transpose.

The extra ingredient leads to the Kraus form. We quote the theorem without proof, not because the proof is difficult but because it takes a little time to organize. The point to notice is how simple and easy to use the result is.

It took some twenty years for physicists to understand *Stinespring*'s theorem, and *Kraus* was one of the first to do so. Once you know the result, it is easy to remember and to use. Moreover every completely positive map can be performed in a hypothetical lab equipped to perform every unitary transformation, in Hilbert spaces whose dimension is at most the square of that of the Hilbert space of the physical system being studied.

There is another interesting aspect of this story. We can ask: when is a quantum state entangled? If the state is pure the answer is simple: if its partial trace is a mixed state. But what if the state itself is mixed? There can be classical correlations present, and in fact there will be whenever the state is *not* of the form $\rho^A \otimes \rho^B$. A suitable definition of a separable quantum state, whether mixed or pure, should allow for classical correlation between the two subsystems, but no more than that. Mathematically this means that the separable state lies in the convex hull of uncorrelated states:

Definition: A state ρ is separable if and only if it can be written as

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B \ , \tag{141}$$

for some density matrices ρ_i^A, ρ_i^B acting on the factors.

This definition is due to *Werner*.

A direct check whether a given state ρ obeys this condition is prohibitively difficult, since we have to try all possible decompositions of this type. It is therefore helpful to know that a state is entangled if and only if there exists a positive but not completely positive map Φ such that $\Phi \otimes \mathbf{1}$ turns the state ρ into a matrix with at least one negative eigenvalue. This is still a hard condition to check when the dimensions involved are large. In fact it is an **NP** complete problem, in the language of complexity theory that we will introduce later. But for two qubits it settles things.

We have the following useful theorem:

Theorem: A state ρ is entangled if ρ^{T_A} has a negative eigenvalue. For two qubits, and for one qubit and one qutrit, this is an if-and-only-if statement.[33]

Measurements

Let us agree that an isolated quantum system always evolves unitarily, while an open system—perhaps the system is coupled to a measurement apparatus—evolves with completely positive trace preserving maps. In the first step (135) applies, for some choice of Kraus operators A_i. But in a measurement the wave function must collapse to an outcome. Rushing in where angels fear to tread, we resolve the measurement problem with a postulate:

Let there be n possible measurement outcomes. Then there are n Kraus operators A_i. In a non-selective measurement the system changes its state according to the CP map generated by the A_i. In a selective quantum measurement the system changes its state from ρ to one of the n states

$$\rho_i = \frac{A_i \rho A_i^\dagger}{\mathrm{Tr}(A_i \rho A_i^\dagger)} \ . \tag{142}$$

The transition $\rho \to \rho_i$ happens with probability

$$p_i = \mathrm{Tr} A_i \rho A_i^\dagger \ . \tag{143}$$

All the ρ_i are legitimate density matrices and the Kraus operators A_i obey a condition ensuring that the probabilities sum to unity.[34]

We now have two kinds of time evolution, the linear time evolutions effected by CP maps, and the non-linear time evolution $\rho \to \rho_i$ described by the measurement postulate. An important special case is that of a *projective* or *von Neumann* measurement. Then we choose the measurement operators to be mutually orthogonal projection operators,

$$A_i = P_i = A_i^\dagger \ , \qquad P_i P_j = \delta_{ij} P_i \ . \tag{144}$$

[33]Exercise: Consider the two qubit state $\rho = \frac{p}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) + \frac{1-p}{4}\mathbf{1}$. For what values of p is this an entangled state?

[34]Exercise: Check this.

The completeness property of the measurement operators implies that

$$\sum_i P_i = \mathbf{1} \ . \tag{145}$$

Sets of projection operators like this are obtained by choosing a Hermitian operator, now called an 'observable', and performing a *spectral decomposition*

$$A = \sum_i \lambda_i P_i \ . \tag{146}$$

For simplicity, suppose that all eigenvalues are non-degenerate. In a non-selective von Neumann measurement of the 'observable' A the state changes according to

$$\rho \to \rho' = \sum_{i=1}^{d} P_i \rho P_i \ . \tag{147}$$

The state has been forced to commute with A. This is in fact a CP map effected by the d Kraus operators P_i. In a selective von Neumann measurement the state collapses, and the outcome labelled λ_i occurs with probability p_i,

$$\rho \to \rho_i = \frac{P_i \rho P_i}{\mathrm{Tr}(P_i \rho P_i)} \ , \qquad p_i = \mathrm{Tr}(P_i \rho P_i) = \mathrm{Tr}(\rho P_i) \ . \tag{148}$$

This measurement is repeatable.[35] It is also highly idealized. Still the von Neumann measurement is much beloved by people who have the task of actually measuring things in the lab. The picture to have in mind is that of a photon encountering a Glan–Thompson prism that lets through linearly polarized photons only.

What is happening here? First we pause to reflect on classical probability theory. If a probability vector counts as a classical state, the classical state can collapse too. A classical probability distribution $P(A)$ can collapse to a conditional probability distribution $P(A = a_i | B = b_j)$ depending on the outcome observed for the random variable B. But the non-selective

[35] Exercise: In classical statistics the expectation value is $\langle A \rangle = \sum_i p_i \lambda_i$. Show that $\langle A \rangle = \mathrm{Tr}(A\rho)$. Also show that if you repeat the same von Neumann measurement you get the same result, and verify that ρ' commutes with A.

measurement does not have a classical analogue. In a non-selective classical measurement nothing happens since

$$\sum_j P(A = a_i|B = b_j)P(B = b_j) = P(A = a_i) \ . \tag{149}$$

The analogy breaks down because the quantum state ρ' obtained in (147) may be significantly different from the state ρ. Very special cases excepted a quantum measurement always disturbs the state, and the classical notion of 'conditional probability' is no longer with us. At the same time we should note that CP map that describes the non-selective measurement can in principle be reversed by an experimentalist who is able to perform arbitrary unitary transformations of the whole system including the 'reservoir' that describes the measurement apparatus. Then the non-selective measurement is an event that can be made to un-happen.

This is an important conceptual point, so let us say it in a different way. Suppose a pure quantum state evolves under a unitary transformation,

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle = z_0(t)|0\rangle + z_1(t)|1\rangle \ . \tag{150}$$

If, at time t, we perform a measurement in this basis we find the outcome $|0\rangle$ with probability $|z_0(t)|^2$. But what is the probability to get this outcome at time $t = 1$ given the outcome at $t = 0$? We cannot talk about the outcome at $t = 0$ unless a measurement was performed at that time. But if so the state at $t = 0$ changed according to

$$|\psi(0)\rangle\langle\psi(0)| = \begin{pmatrix} |z_0|^2 & z_0\bar{z}_1 \\ z_1\bar{z}_0 & |z_1|^2 \end{pmatrix} \quad \rightarrow \quad \rho(0) = \begin{pmatrix} |z_0|^2 & 0 \\ 0 & |z_1|^2 \end{pmatrix} \ . \tag{151}$$

The off-diagonal elements have disappeared, and

$$U(1)\rho(0)U^{-1}(1) \neq |\psi(1)\rangle\langle\psi(1)| \ . \tag{152}$$

So we get into a muddle if we use equation (150) to talk about the probability that the system 'was' in one of the states $|0\rangle$ and $|1\rangle$ at two different times. The notion of history is not that easily reconciled with quantum theory.

POVMs

We leave these questions open, and return to general measurements. The idea to use Kraus operators to guarantee that there is some larger Hilbert space behind us has led us to claim that a given outcome occurs with probability

$$p_i = \mathrm{Tr}\left(\rho A_i^\dagger A_i\right) \ , \qquad \sum_i A_i^\dagger A_i = \mathbf{1} \ . \tag{153}$$

The Kraus operators describe how the state of the system changes in a measurement. But maybe we are only interested in the result of the measurement, and therefore we define a general measurement by saying that there exists a number of positive operators E_i, called *effects*, such that

$$E_i \geq 0 \ , \qquad \sum_{i=1}^{n} E_i = \mathbf{1} \ . \tag{154}$$

The collection of effects is known as a *POVM*, which can be spelt out as 'positive operator valued measure'. The POVM allows us to extract a probability distribution from any density matrix,[36]

$$p_i = \mathrm{Tr}(\rho E_i) \ . \tag{155}$$

There is no requirement that $\mathrm{Tr}E_iE_j = 0$, which means that this is not a probability distribution over mutually exclusive events, nor is there any guarantee that we can choose a state for which p_1 (say) equals 1.[37] Moreover, unless the effects are one-dimensional projectors they can be written in terms of Kraus operators in many different ways.

Coming back to the chicken-and-egg question, following *Naimark* we can regard any POVM as a von Neumann measurement by adding an ancilla Hilbert space to the Hilbert space of the system. Let us consider the special case of a *rank one* POVM, in which each of the $n > d$ effects is of the form $E_i = |x_i\rangle\langle x_i|$ for some vector $|x_i\rangle$ obeying $\langle x_i|x_i\rangle \leq 1$, with equality only if the effect actually is a projector. Then form the *generator matrix*

[36] Exercise: Show that the following equation defines a probability distribution.

[37] Exercise: For the qubit, choose projectors that project onto states forming a regular triangle on the equator. Rescale them so that they form a POVM. What probability distributions over three events can you obtain in this way?

$$X = \begin{pmatrix} |x_1\rangle & |x_2\rangle & \dots & |x_n\rangle \end{pmatrix}_{d\times n} = \begin{pmatrix} \langle u_1| \\ \langle u_2| \\ \vdots \\ \langle u_d| \end{pmatrix}_{d\times n} . \tag{156}$$

We have arranged things so that we can think of X either as n columns or as d rows. You can check that

$$XX^\dagger = \sum_{i=1}^{n} |x_i\rangle\langle x_i| = \sum_{i=1}^{n} E_i = \mathbf{1}_{d\times d} . \tag{157}$$

But when you think in terms of the rows, this means that you have a set of d n-dimensional vectors obeying

$$\langle u_i|u_j\rangle = \delta_{ij} . \tag{158}$$

Here $1 \le i, j \le d$. You can extend this set of d orthonormal row vectors to n orthonormal row vectors by adding more rows to X, so that it becomes a unitary matrix. We interpret it as a set of n column vectors,

$$U = \begin{pmatrix} |x_1\rangle & |x_2\rangle & \dots & |x_n\rangle \\ |y_1\rangle & |y_2\rangle & \dots & |y_n\rangle \end{pmatrix}_{n\times n} . \tag{159}$$

Because the matrix is unitary, the column vectors are mutually orthogonal unit vectors $\{|z_i\rangle\}_{i=1}^n$, yielding n projection operators $\{P_i\}_{i=1}^n$, where

$$|z_i\rangle = \begin{pmatrix} |x_i\rangle \\ |y_i\rangle \end{pmatrix} , \qquad P_i = |z_i\rangle\langle z_i| . \tag{160}$$

This defines a von Neumann measurement in the large Hilbert space, related by a simple projection to the POVM we started out with.[38]

POVMs provide an interesting perspective on quantum states, but we hasten on to the next topic.

The Lindblad equation

[38] Exercise: Do this construction explicitly for the POVM in the preceding footnote.

A system may fail—and will always fail, more or less—to be isolated because it interacts with some 'environment' or 'thermal reservoir'. In this situation unitary time evolution is at best an approximation to what is observed. We round off this brief introduction to the theory of open systems by giving the generalization to quantum mechanics of the classical Markov process. If the evolution of the system is a continuous unfolding of completely positive maps it is described by the *Lindblad equation*

$$\frac{d\rho}{dt} = \mathcal{L}(\rho) = i[\rho, H] + \sum_i \left(L_i \rho L_i^\dagger - \frac{1}{2}(L_i^\dagger L_i \rho + \rho L_i^\dagger L_i) \right) \ . \tag{161}$$

The L_i are the *Lindblad* operators, and $\mathcal{L}$ stands for *Liouville*. The Hamiltonian H typically has contributions also from the terms that couple the system to the reservoir in the evolution of the composite system. The equation applies when the system dynamics is slow compared to the correlation time scale of the reservoir, so that equation (130) is a reasonable approximation for each step.

For a careful derivation you have to look elsewhere, but to see where the various terms come from consider a CP map

$$\mathcal{E}(\rho) = A_0 \rho A_0^\dagger + \sum_i A_i \rho A_i^\dagger = \rho + \delta\rho \ , \tag{162}$$

$$A_0 = \mathbf{1} + (L_0 - iH)\delta t \ , \quad A_i = L_i \sqrt{\delta t} \ . \tag{163}$$

One of the Kraus operators is close to the identity, while the others are close to zero. Then

$$\delta\rho = (-i[H, \rho] + L_0 \rho + \rho L_0 + \sum_i L_i \rho L_i^\dagger)\delta t \ . \tag{164}$$

To ensure that the trace is preserved we must have $\mathrm{Tr}\delta\rho = 0$ for all choices of ρ. This forces

$$L_0 = -\frac{1}{2} \sum_i L_i^\dagger L_i \ . \tag{165}$$

Dividing through by δt we arrive at the Lindblad equation.

To see a possible issue with the equation it is helpful to consider a familiar classical problem, namely that of Brownian motion. A pollen grain is immersed in a liquid, and moves under the influence of collisions with molecules coming from random directions. Now you may worry that when the pollen grain has been around for some time correlations will be set up between the grain and the molecules, so that the collisions do not come from random directions any more. Close investigation of the physics suggests that this worry is unfounded. So we make the *Markov assumption* that such correlations can be ignored, and the resulting theory works splendidly. In quantum theory there is a Markow assumption too, since we assume that equation (130) holds at each stage of the discretized process.

What we can say is that the Lindblad equation has fared brilliantly in quantum optics, where any correlations with the radiation field leak away quickly. But we do not go into this any further here.

Problem 3: Consider the unitary operator

$$U = \mathbf{1} \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| \tag{166}$$

acting on a two qubit Hilbert space (where $X = \sigma_x$). Choose the initial state to be $\rho \otimes |R_0\rangle\langle R_0|$, where

$$|R_0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \ . \tag{167}$$

Construct the Kraus operators acting on ρ. What happens to the Bloch vector of ρ when we perform the resulting CP map? To what surface in the Bloch ball of the first qubit does the Bloch sphere of the first qubit go?

INFORMATION THEORY

Shannon created information theory in two papers entitled *A Mathematical Theory of Communication*, later reissued as a book under the more accurate title *The Mathematical Theory of Communication*. The key to his work is to realize that it ignores the *meaning* of the message. Rather, the significant aspect of a message is that it has been *selected* from a set of possible messages. To quantify information the theory uses a quantity called 'entropy'. Following *Boltzmann* it was denoted by the letter H. Generalizing *Shannon*'s theory to the quantum case is a subtle thing.

Information

Shannon worked at the Bell Telephone Laboratories, and his interest in communication was very practical. A message is being sent, using some alphabet of n letters. The theory (as presented here) assumes that the letters are *i.i.d.*, spelt out as 'independent and identically distributed'. That is, the probability that the ith letter will be sent is p_i, every time. We want to compress the message as much as possible before sending it, and the first goal is to determine how much data compression that can be achieved.

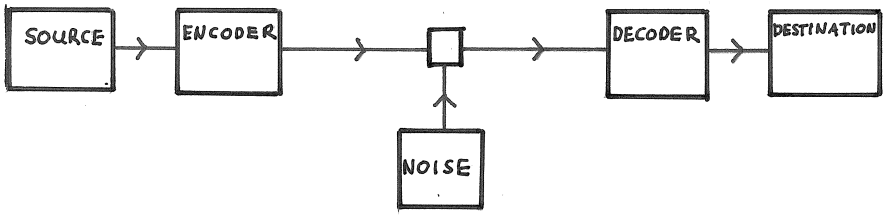


Figure 7: The problem considered by Shannon. The message is compressed at an encoder before it is sent through a possibly noisy communication channel.

Shannon began by asking for a measure of how much 'choice' is involved in the selection of a letter, or how uncertain we are of the outcome of the event. Equivalently, this is the amount of information produced when the event happens. The measure he arrived at is a function of the probability

distribution associated to some random variable. From now on then *information* is quantified by the *Shannon entropy*

$$H(\vec{p}) = -\sum_{i=1}^{n} p_i \log p_i \ . \tag{168}$$

It is understood that $0 \log 0 = 0$. The logarithm is usually taken to be with base 2, and then the information is measured in *bits*. We will slip back to natural logarithms at some stage.[39]

We can argue for this measure as follows. We regard $-\log p_i$ as an additive measure of the 'surprise' we feel in receiving the ith letter. Then $H = \langle -\log p \rangle$ is the information received per letter, when averaged over a long message. The interpretation makes more sense if we remember the psychophysical law that says that human response is proportional to the logarithm of the stimulus. (This is why the Greeks measured the luminosity of stars using logarithmic magnitudes.) But the real justification for the definition lies in the theorems that *Shannon* proved. Let us place an informal version of his *noiseless coding theorem* on the table right away. Then you will see that these lecture notes carry a certain amount of information, and that Shannon's definition of information is the relevant one if you want to convert them to JPEG format.

To introduce the theorem we first note that when we use the logarithm with base 2 we assume that the length of the message is measured in terms of the number of binary digits you need to encode it. This length will clearly depend on the coding. Recall that the Morse alphabet uses dashes and dots, with the number of dashes and dots used to encode the letter being lower if that particular letter is in frequent use. The theorem is concerned with the length of a message that has been encoded in an optimal way. Ignoring some fine print, it says that *if a message contains N letters chosen with probabilities p_i from an alphabet consisting of n symbols, then it can be transmitted in the form of a string of bits of length $NH(\vec{p})$, but it cannot be compressed further.*

To see how the theorem comes about, consider the kind of sequences that can arise. In particular, consider the number of sequences that contains N_1 instances of the first letter in the alphabet, N_2 of the second, and so on. This

[39] Exercise: For $p_1 = p, p_2 = 1 - p$, plot $H(p)$. Then maximize the function for arbitrary n. Also check what happens if you change the base of the logarithm to e.

number is

$$\frac{N!}{N_1!N_2!\ldots N_n!} \ . \tag{169}$$

Using Stirling's formula we can approximate this number, or more conveniently its logarithm, by

$$\begin{aligned} &\log \frac{N!}{N_1!N_2!\ldots N_n!} \approx \\ &\approx N\log N - N - \sum_{i=1}^{n}(N_i \log N_i - N_i) = -\sum_{i=1}^{n} N_i \log \frac{N_i}{N} \ . \end{aligned} \tag{170}$$

Now comes the trick. N_i/N is the frequency with which a certain letter occurs in a sequence. It then follows from the Law of Large Numbers that, with overwhelming probability, in the sequences that we need to encode we have

$$\frac{N_i}{N} = p_i \ . \tag{171}$$

Inserting this in (170) we conclude that the Law of Large Numbers allows us to say that, with overwhelming probability, the sequence that we need to encode can be regarded as having been chosen from a set of

$$2^{NH(\vec{p})} \tag{172}$$

typical sequences. For large N, and unless all letters are equally likely, this is a small fraction of the number of all possible sequences (equal to n^N).[40]

We see that the compression of the message is possible because at the encoder we can assume that we are dealing with a typical message. We do not have to encode all the 2^N messages. It is enough if the signal carries information about which out of all the typical messages is being sent. This is how the noiseless coding theorem arises. We also see that some fine print

[40]Exercise: Consider a string of 10 binary digits. How many such strings are there altogether? How many of them contain at least 7 zeroes? If the probability of choosing a zero is 9/10, what is the probability of obtaining a string of the latter type? Use your result to make a comment on the idea of typical sequences.

must be added to the statement of the theorem, because there is a small probability that the message is, in fact, not typical. If so we must declare an error. However, the Law of Large Numbers guarantees that the probability that this happens can be made as small as we please by making the message long enough.

Some limitations are apparent here. Let us raise some of them. To begin with, the i.i.d. assumption may be too strong. If the message is in English, or in any other natural language, there will in fact be strong correlations between the various letters in the message. We could compress the message by, say, removing all the vowels, and chances are that it would still be decodable. Entire books have been written in this way. (Incidentally, a theory taking the redundancies in the English language into account shows that the amount of information present in my notes would increase if its letters were reordered in a random way.) A second limitation of the theorem is that it is non-constructive. It tells us that compression is possible, but it does not provide a recipe for how to do it. Finally we notice that the encoding cannot even start until the encoder has received a string of letters long enough to ensure that the string is typical. Still the noiseless coding theorem provided information theory with a very good start.

Some properties of the Shannon entropy

The Shannon entropy is a continuous and nowhere negative function of a probability distribution $\vec{p}$, taking the value zero if and only if the probability vector is pure. It also obeys a recursion property that we illustrate in Figure 8. To see what it means, suppose that we coarse grain the data so that we do not distinguish between all of the N individual outcomes. We choose some partition $N = k_1 + k_2 + \ldots + k_r$ and obtain a new probability distribution with only r components,

$$q_1 = \sum_{i=1}^{k_1} p_i \ , \quad q_2 = \sum_{i=k_1+1}^{k_2} p_i \ , \quad \ldots \ , \quad q_r = \sum_{i=N-k_r+1}^{k_r} p_i \ . \tag{173}$$

Then it holds that

$$H(\vec{p}) = H(\vec{q}) + q_1 H\left(\frac{p_1}{q_1}, \ldots, \frac{p_{k_1}}{q_1}\right) + \ldots + q_r H\left(\frac{p_{N-k_r+1}}{q_r}, \ldots, \frac{p_N}{q_r}\right) \ . \quad (174)$$

Applied to the example in Figure 8 this gives the formula

$$\begin{aligned} &H\left(\frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}\right) = \\ &= H\left(\frac{3}{8}, \frac{3}{8}, \frac{1}{4}\right) + \frac{3}{8} H\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right) + \frac{3}{8} H\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right) + \frac{1}{4} H\left(\frac{1}{2}, \frac{1}{2}\right) \ . \end{aligned} \quad (175)$$

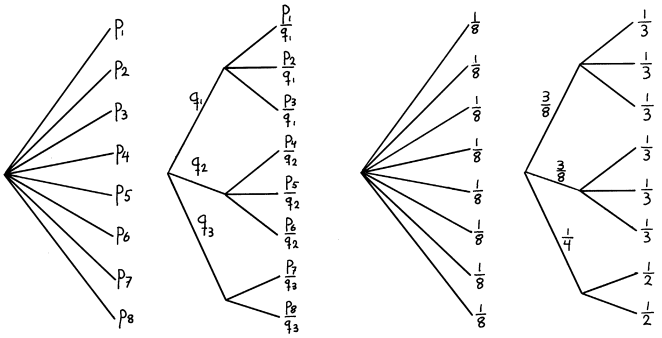


Figure 8: The recursion property illustrated: to the right it is used to determine $H(\frac{3}{8}, \frac{3}{8}, \frac{1}{4})$ in terms of the Shannon entropy for uniform distributions.

This is clearly interesting since it shows that the Shannon entropy is determined by the values it takes when all events are equally likely. Supplemented by some mild extra conditions the recursion property actually defines the function H uniquely, that is to say that no other reasonable function has this property.

A key property is concavity. Let $\vec{p}$ and $\vec{q}$ be two probability vectors, let $x \in [0, 1]$, and consider the mixture $x\vec{p} + (1 - x)\vec{q}$. Then

$$H(x\vec{p} + (1 - x)\vec{q}) > xH(\vec{p}) + (1 - x)H(\vec{q}) \ . \quad (176)$$

In words, the Shannon entropy is a *concave* function of its arguments, which means that a straight line between two points on its graph always lies below the graph.[41]

Concave functions, or *convex* functions for which the direction of the inequality is reversed, are important for many reasons. (To remember which is which, memorize that a convex function has a convex *epigraph*, and recall that the epicentre lies above the earthquake.) Concave functions are easy to optimize, because a concave function has at most a single maximum inside its domain.

Conditional entropy, joint entropy, and mutual information

To continue, it is convenient to associate the Shannon entropy with some particular random variable A, so that

$$H = H(A) = -\sum_i P(A = a_i) \log P(A = a_i) \ . \tag{177}$$

If we have two random variables we have the two probability distributions $P(A)$ and $P(B)$ to play with, as well as the joint and conditional probability distributions. (At this point, please recall eq. (3), known as *Bayes*' formula). Then we define the *conditional entropy*

$$H(A|B) = -\sum_{i,j} P(B = b_j) P(A = a_i|B = b_j) \log P(A = a_i|B = b_j) \tag{178}$$

and the *joint entropy*

$$H(A, B) = -\sum_{i,j} P(A = a_i, B = b_j) \log P(A = a_i, B = b_j) \ . \tag{179}$$

The joint entropy measures the uncertainty of a joint event, or equivalently the information received when both events are found to happen. The conditional entropy measures the uncertainty of the event A given that we know the outcome of the event B, weighted over all the possible outcomes of B.

[41] Exercise: Calculate the matrix of second derivatives of $H(p_1, p_2, \ldots, p_n)$. Show that it is negative definite, and that this is enough to prove concavity. Where in these notes have you seen this matrix before?

In the calculations to follow we will set

$$P(A = a_i|B = b_j) = p_{i|j} \ , \qquad P(A = a_i, B = b_j) = p_{i,j} \ , \tag{180}$$

$$P(A = a_i) = p_i = \sum_j p_{i,j} \ , \qquad P(B = b_i) = q_i = \sum_j p_{j,i} \ . \tag{181}$$

In this notation *Bayes*' formula (3) takes the form

$$p_{i,j} = p_{i|j} q_j = p_{j|i} p_i \ . \tag{182}$$

If we sum over i or j we see that we are on familiar ground here; the equation

$$q_j = \sum_i p_{i,j} = \sum_i p_{j|i} p_i \tag{183}$$

can be recognized as eq. (10). The conditional probabilities are the matrix elements of a stochastic matrix.

There are relations between the joint and conditional entropies. Using Bayes' formula it is easy to see that

$$H(A, B) = H(B) + H(A|B) = H(A) + H(B|A) \ . \tag{184}$$

The easy proof consists in writing out the definition of the conditional entropy,

$$\begin{aligned} H(A|B) &= -\sum_{i,j} p_{i,j} \ln \frac{p_{i,j}}{q_j} = -\sum_{i,j} p_{i,j} (\ln p_{i,j} - \ln q_j) = \\ &= -\sum_{i,j} p_{i,j} \ln p_{i,j} + \sum_j q_j \ln q_j = H(A, B) - H(B) \ . \end{aligned} \tag{185}$$

(Out of habit, we decided to replace the log with the natural logarithms in all the definitions.) If the two random variables are uncorrelated it immediately follows that $H(A|B) = H(A)$, so that the joint entropy is just the sum of the two entropies for the individual random variables.

We define one more useful quantity, the *mutual information*

$$H(A : B) = H(A) + H(B) - H(A, B) \ . \tag{186}$$

Mutual information will play a key role when we discuss the quality of communication channels. It is a measure of the correlations between the two random variables, and it equals zero if the events are uncorrelated.[42] An important property that it has is that it is a concave function. If one of its arguments is a convex mixture $\vec{p} = x\vec{r} + (1-x)\vec{s}$ then

$$H(\vec{p},\vec{q}) \geq xH(\vec{r},\vec{q}) + (1-x)H(\vec{s},\vec{q}) \ . \tag{187}$$

We omit the proof, but keep it in mind. It will be useful when we have to maximize the mutual information in one of its arguments.

There are important inequalities obeyed by the various quantities that we have introduced. The most obvious one is

$$H \geq 0 \tag{188}$$

with equality only for a pure state. Two more are suggested by the interpretation. The information received when a joint event happens must be greater than that received from only one of the events, so we must have

$$H(A,B) \geq H(A) \ . \tag{189}$$

Indeed this is true. Similarly, it must be the case that the conditional entropy obeys

$$H(A) \geq H(A|B) \tag{190}$$

with equality only for independent random variables A and B. To prove this, let the random variables have the probability distributions $\vec{p}$ and $\vec{q}$, respectively. Using the definition, and then *Bayes*'s formula (3) to rewrite the conditional probabilities, we observe that

$$\begin{aligned} H(A|B) - H(A) &= -\sum_{i,j} q_j \frac{p_{i,j}}{q_j} \ln \frac{p_{i,j}}{q_j} + \sum_{i,j} p_{i,j} \ln p_i = \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} p_{i,j} \ln \frac{p_i q_j}{p_{i,j}} \leq \sum_{i=1}^{n}\sum_{j=1}^{m} p_{i,j} \left(\frac{p_i q_j}{p_{i,j}} - 1 \right) = 1 - 1 = 0 \ . \end{aligned} \tag{191}$$

[42] Exercise: Prove that it is zero if the events are uncorrelated. The maximum value is trickier. Prove that $H(A:B) \leq H(A)$ and $H(A:B) \leq H(B)$. If $H(A) < H(B)$ the second bound cannot be reached. Try to see why.

We relied on the inequality

$$\ln x \leq x - 1 \ , \tag{192}$$

which holds for all $x > 0$.[43]

Using the connection between joint and conditional entropy the property of *subadditivity* follows immediately,

$$H(A) + H(B) \geq H(A, B) \ , \tag{193}$$

again with equality if and only if the random variables are independent. From eq. (186) we see that another way of saying this is that mutual information is always positive, or equal to zero for independent events.

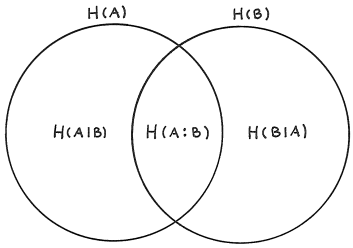


Figure 9: This picture appears in many textbooks, as an aid to memorize eqs. (184) and (186). It has the virtue of giving a central position to mutual information. The joint entropy is represented by the total area. If A and B are independent the two circles are disjoint and the mutual information vanishes.

Without giving the story away just yet, let me say that some of the entropy inequalities must be revisited when we come to quantum information theory. Then it will be seen that neither the conditional entropy nor the conditional probability distribution have any immediate analogues in the quantum case, while the mutual information will be very important.

Relative entropy

[43]Exercise: Prove the inequality (192). Why is the entropy inequality (190) necessary for the interpretation of $H(A|B)$ to make sense?

Boltzmann's H-theorem says that entropy cannot decrease as time passes. If the passage of time is governed by stochastic maps this is not true, in general, for the Shannon entropy. The bit-flip map (11) does increase entropy, but the coarse-graining map (14) can decrease it. The general statement is that a stochastic map will increase the Shannon entropy, $H(S\vec{p}) \geq H(\vec{p})$ for all $\vec{p}$ if and only if it has the maximally mixed probability distribution as a fixed point.

This is one reason to introduce the *relative entropy*

$$H(\vec{p}||\vec{q}) = \sum_{i=1}^{n} p_i \ln \frac{p_i}{q_i} \ . \tag{194}$$

This does have the desirable property of monotonicity under stochastic maps, namely that

$$H(S\vec{p}||S\vec{q}) \leq H(\vec{p}||\vec{q}) \tag{195}$$

for every stochastic map S. We omit the proof, but we (or you) will prove that relative entropy enjoys other interesting properties as well.

First of all it is non-negative. More than that, it obeys

$$H(\vec{p}||\vec{q}) \geq \frac{1}{2} \sum_{i=1}^{n} (p_i - q_i)^2 \ . \tag{196}$$

To prove this, note that any smooth function f obeys

$$f(x) = f(y) + (x-y)f'(y) + \frac{1}{2}(x-y)^2 f''(\xi) \ , \quad \xi \in (x,y) \ . \tag{197}$$

Apply this to the function $x \ln x$, and you get the result by summing.[44] Using this result you can derive a slightly sharper version of the inequality $H(\vec{p}) \leq \ln n$, as well as—by considering the relative entropy between a joint probability distribution and the probability distribution for two independent events—a slightly sharper version of the subadditivity inequality (193).[45]

We get an interpretation of relative entropy if we go back to the probability of obtaining an outcome m times in N trials with two outcomes, eq.

[44] Exercise: Do it!

[45] Exercise: Do this as well!

(17). Taking logarithms and applying Stirling's formula we find (after some calculation) that

$$\ln \binom{N}{m} \approx -m \ln \frac{m}{N} - (N-m) \ln \frac{N-m}{N} \ , \tag{198}$$

$$\ln \left(p^m (1-p)^{N-m} \right) = m \ln p + (N-m) \ln (1-p) \ . \tag{199}$$

Putting things together, and generalizing from the binomial to the multinomial distribution valid for n outcomes, we find that the probability to obtain the frequency vector $\vec{\nu}$ in N samplings from a probability distribution $\vec{p}$ obeys[46]

$$P(\vec{\nu}|\vec{p}) \approx e^{-NH(\vec{\nu}||\vec{p})} \ . \tag{200}$$

This suggests that relative entropy is a good measure of the distinguishability of two probability distributions when we do a reasonably large number N of samplings. If $H(\vec{\nu}|\vec{p})$ is large the probability that we will obtain a frequency vector $\vec{\nu}$ (and erroneously conclude that $\vec{p} = \vec{\nu}$) is small.

However, unlike distances relative entropy is highly asymmetric in its arguments. How different is a fair coin from a biased coin that always gives heads? Pick one of them and start flipping it to see which is which. The number of flips you have to make before you feel sure which one you picked depends very much on the choice.[47] So the asymmetry of this distinguishability measure may be desirable.

Error correction

So far we have focussed on data compression. We now change perspective, and observe that removing redundancy may be a very bad idea. If a message is phrased in a natural language it is hugely redundant—and this reduncancy is useful in communication, because it means that errors in the transmission are easily corrected. The misprints in these notes may be annoying, but they are not fatal. In the real world transmission of information is always distorted by noise. If you want to send a message from a space probe far out

[46] Exercise: Fill in the details!

[47] Exercise: Use eq. (200) to calculate P(fair|biased) and P(biased|fair) in the example.

in the Solar system, or if you want to build a quantum computer, this is a key issue. The way out is to introduce redundancies in the message, allowing us to spot and correct errors.

To be quantitative about this we need a model for the noise. A very simple, but useful, model is the binary symmetric channel defined by eq. (11). So we are sending bits, and each bit may flip with probability p. Suppose we want to send the message 1101. The message will come through correctly with probability $(1-p)^4$, which may be unacceptably low. The obvious way to deal with this is to repeat the message three times, so that we send 110111011101. Should an error occur in one place, we can correct it by taking a majority vote. In fact some double errors can also be corrected for. But the length of the message has gone up. This is bad in itself. Moreover, with increased length comes an increased risk of double errors, and if the error probability is high the repetition code may no longer be safe.

It was once believed that the only way to combat noise is to reduce it. For the binary symmetric channel, this means that one tries to reduce p. But *Shannon* took the amount of noise as given, and asked for the minimum amount of redundancy that will ensure that the message can be corrected on arrival. He proved a sharp theorem about this. As for the noiseless coding theorem the proof is non-constructive. It shows that an optimal error-correcting code must exist, but it does not provide it.

We will pass over the question of how to actually encode messages so that you come close to the limits set by the noiseless coding theorem. For this you have to consult a book on information theory. But before we come to the theorem about noisy channels we will give a simple example of an error-correcting code that improves on the simple repetition code above. One reason for doing so is that it will suggest ideas for error-correcting codes to be used in quantum computers.

We again assume that we wish to send one out of 2^4 possible messages, but we view the messages as linear combinations of four basis vectors in a four dimensional subspace of a seven dimensional vector space, where the only numbers available for the linear combinations are 0 and 1. Thus the vector space is not $\mathbf{R}^7$, it is $\mathbf{Z}_2^7$ where $\mathbf{Z}_2$ denotes the integers modulo two (so that $1+1=0$). To see why we choose seven please proceed—the point will be that seven is less than twelve, which is what we used for the repetition code.

To be precise, we let the four vectors be the four rows of the *generator*

matrix

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] . \tag{201}$$

The message we wanted to send, 1101, is then sent in the form of the sequence obtained by adding the first, second and fourth rows together, namely as 1101001. In all the 16 messages that we can send the first four entries are the message, and the last three are to be used for correcting errors. If we want to send a sequence a, b, c, d of four binary integers, what we actually send is the sequence $a, b, c, d, b + c + d, a + c + d, a + b + d$, where addition is modulo 2. Now the subspace of $\mathbf{Z}_2^7$ in which the code words live has been very carefully chosen. After staring at the basis vectors for some time one sees that in order to transform one of the 16 possible sequences into another one has to flip the value of at least three entries. This is interesting because it means that any single error can be corrected for by selecting the one out of the 16 that differs from the received message by a single bit flip. Hence all single errors will be corrected for, and none of the double errors.[48]

But the best part of the story is the way we correct the errors. Write the generator matrix as $G = [\mathbf{1}_4|A]$, where the 4×3 matrix A is defined by eq. (201). Define the 3×7 matrix $H = [-A^{\mathrm{T}}|\mathbf{1}_3]$. By construction

$$HG^{\mathrm{T}} = 0 . \tag{202}$$

This means that $H\mathbf{u} = 0$, where $\mathbf{u}$ is any linear combination of the four rows of G, that is to say if its components form one of the 16 correct messages. If an error occurs during the transmission the message received is given by the components of a vector $\mathbf{u} + \mathbf{e}$, and

$$H(\mathbf{u} + \mathbf{e}) = H\mathbf{e} . \tag{203}$$

The 3-component vector $H\mathbf{e}$ is known as the *error syndrome*. It is easy to check that if $\mathbf{e}$ has a single non-zero component then it can be reconstructed

[48] Exercise: For what values of p is the probability that the message comes out correctly larger than $(1 - p)^4$ if we use this code?

uniquely from a knowledge of the error syndrome.[49] Once this is known we can correct the message by subtracting $\mathbf{e}$ from the received message (or adding it, which is the same thing since we work with integers modulo two all the time).

We have just described the simplest example of a *Hamming code*. For messages of length 4 it is evidently less wasteful than the repetition code. Indeed we made do with less redundancy than we might have expected. But for us the really remarkable thing about it is that we can do the error correction without, in fact, reading the message. All we need is the error syndrome. Once we start sending quantum messages we have to measure the message in order to read it. This means that reading the message changes the message. Quantum error correction has to correct messages without reading them.

Channel capacity

We now get back on the path towards Shannon's theorem about noisy channels. A channel is any medium carrying a message. Physically it may be air, an optical fibre, or a printing press. The input of the message can be regarded as a random variable A, whose outcomes are the letters being sent. The output is another random variable B, whose outcomes are the letters received. The two random variables are connected by a conditional probability distribution $P(B|A)$, which tells us the probability that b_i is received given that a_j was sent. As we have seen these conditional probabilities are the matrix elements of a stochastic matrix, in this context often called *transition probabilities*. We will therefore equate a *channel* with a stochastic matrix. This means that we assume the channel to be *memoryless*. This may not be an accurate model of the physical channel, because real noise often has a tendency to come in bursts, but it is a good first approximation. The physical details of the channel are left to the engineers.

In a *noiseless* channel the output is in one-to-one correspondence with the input, which means that the stochastic matrix is a permutation matrix. A *noisy* channel offers more of a challenge. Given a stochastic matrix describing

[49] Exercise: How many single component errors are there, and how many error syndromes? Check the whole story of this Hamming code in detail.

a noisy channel, we want to know the maximal rate at which information can be sent over that channel.

The quality of the channel can be measured by the mutual information $H(A:B)$ between input and output. If the output is independent of the input the mutual information vanishes. If they are perfectly correlated the mutual information equals the information $H(A)$ in the input. We define the *capacity* of a noisy channel as

$$C = \max\, H(A:B)\ , \tag{204}$$

where the maximization is with respect to the probability distribution chosen for the input. The stochastic matrix defining the channel is kept fixed, so that C is indeed a property of the stochastic matrix. Calculating the channel capacity is a constrained optimization problem that can be addressed using the Lagrange multiplier method. We write the mutual information in the form

$$H(A:B) = H(B) - H(B|A)\ . \tag{205}$$

Then we set

$$\frac{\partial}{\partial p_i}\left[H(A:B) - \lambda(\sum_j p_j - 1)\right] = \frac{\partial}{\partial p_i}\left[\sum_{k,j} p_{k|j}p_j \ln\frac{p_{k|j}}{q_k} - \lambda(\sum_j p_j - 1)\right] = 0\,. \tag{206}$$

The conditional probabilities characterize the channel and are kept constant, but when taking the derivative we must remember that $\vec{q} = \vec{q}(\vec{p})$. Provided that no component of $\vec{p}$ vanishes we obtain

$$\sum_k p_{k|i} \ln\frac{p_{k|i}}{q_k} = \lambda + 1\ . \tag{207}$$

The "1" on the right hand side comes out when you take the derivative of q_k with respect to p_i. Fortunately we know that mutual information is concave, so these equations determine the unique maximum. Unfortunately they are difficult to solve.[50]

There is one easy case: the binary symmetric channel (11), for which $p_{0|0} = 1-p$, $p_{0|1} = p$ and so on, where p is fixed. For this channel there are

[50] Exercise: Show that the equations imply that $\lambda = C - 1$.

only two equations (206), and if you write them out you see that they imply $q_0 = q_1 = 1/2$. After that you quickly arrive at[51]

$$C = \ln 2 + p \ln p + (1-p) \ln (1-p) \ . \tag{208}$$

It remains to interpret this formula. For this purpose we assume that we are sending binary digits, and switch back to logarithms with base 2 (replacing $\ln 2$ by 1). We then have $H(\vec{p}) \leq 1$.

The precise interpretation of the channel capacity is provided by *Shannon*'s theorem. It is again concerned with a message containing letters chosen according to a probability distribution $\vec{p}$ and coded into bits. It says that *a string of bits of length $NH(\vec{p})$ can be coded into a string of bits of length N and transmitted through a channel with capacity C with arbitrarily small error, provided that*

$$H < C \ . \tag{209}$$

If $H > C$ this is not possible. Actually the theorem says more, and as was the case with the noiseless coding theorem some fine print should be attached. It is important to realize that the theorem applies to very long and 'typical' sequences only. But when it applies, and provided we know the capacity of the channel, it tells us exactly how much redundancy that has to be added to the message in a perfect error-correcting code. With this remarkable statement we take leave of classical information theory.

The von Neumann entropy of a quantum state

We turn to the quantum case. In our discussion of measurements we came to the conclusion that a quantum state ρ will return a wide variety of different probability distributions, depending on what measurement we choose to do. Each measurement of ρ is associated to some Shannon entropy. Is there a single one that deserves to be called 'the' entropy of ρ? The first observation is that if ρ is a pure state then there is a measurement that gives zero Shannon entropy, while other measurements give positive entropy. If ρ is a mixed

[51] Exercise: Do the whole calculation! If $p = 0.01$ and you use logarithms with base 2, what is the channel capacity?

state the issue is less obvious. If you stare at a point in the Bloch ball, and imagine the probability distribution returned during an arbitrary von Neumann measurement (defined by a pair of antipodal points on the surface), you see that the Shannon entropy is smallest if the measurement is performed in the eigenbasis of the state.

We just made a move that is typical for quantum Shannon theory. We start with a notion from the classical theory, and then we optimize it. In this case, we optimize over all possible measurements. One observation is that methods of optimization will be important throughout the subject.

By optimizing the Shannon entropy we arrive at the *von Neumann entropy*

$$S(\rho) = -\mathrm{Tr}\rho \ln \rho \ . \tag{210}$$

Calculating the logarithm, or any other reasonable function, of a positive operator poses no problem of principle. The function is defined in the eigenbasis of the operator, by replacing its eigenvalues with the function of these eigenvalues. Taking the trace that occurs in the definition of the von Neumann entropy is even easier, because we can calculate the trace in any basis we want. In particular, we can calculate the trace in a basis in which ρ is diagonal. Its eigenvalues form the probability vector $\vec{\lambda}$, and the von Neumann entropy is the Shannon entropy of that probability vector,

$$S(\rho) = -\sum_{i=0}^{d-1} \lambda_i \ln \lambda_i = H(\vec{\lambda}) \ . \tag{211}$$

The suggestion to call Shannon's information 'entropy' was actually made by *von Neumann*, who had already studied its quantum version.

The von Neumann entropy has the obvious property that

$$S(\rho) \geq 0 \ , \tag{212}$$

with equality if and only if the state ρ is pure. But the next obvious property is simply not true. We recall from our discussion of entanglement that we can have a pure state ρ_{12} in a composite Hilbert space, and reduced states ρ_1 and ρ_2 describing parts of the whole, such that

$$S_{12} = 0 \ , \qquad S_1 = S_2 \geq 0 \ . \tag{213}$$

We have lost the natural analogue of the obvious inequality (189). This, however, is not a weakness. It is simply the way things are.

The observation (213) does throw conditional entropy out of the game however. Suppose we try to define it by

$$S(\rho_1|\rho_2) \equiv S(\rho_{12}) - S(\rho_2) \ ,$$

in analogy with eq. (184). But it follows from what we just showed that $S(\rho_1|\rho_2)$, so defined, can become negative. Hence this definition is useless, or at least not obviously useful.

Entropy and measurement

The von Neumann entropy is indeed a very distinguished Shannon entropy, singled out by the state itself. We can choose an arbitrary POVM and obtain a probability vector having many more components that the vector $\vec{\lambda}$. Let $\vec{p}$ be any probability distribution returned by ρ in some measurement. Then one can show that

$$H(\vec{p}) \geq H(\vec{\lambda}) \ . \tag{214}$$

Our Bloch ball arguments should make this plausible. You will have the full proof for the special case of von Neumann measurements once you have done Problem 4 below.

An interesting way to look at this is to consider the two-step description of a von Neumann-measurement given in equations (147)–(148),

$$\rho \ \rightarrow \ \rho' = \sum_{i=1}^{d} P_i \rho P_i \ \rightarrow \ \rho_i = \frac{P_i \rho P_i}{\mathrm{Tr}(P_i \rho P_i)} \ , \tag{215}$$

where the final collapse happens with probability $p_i = \mathrm{Tr}(\rho P_i)$. If we describe the first step in the eigenbasis of the projectors P_i we see that we are simply deleting the off-diagonal elements of the density matrix. Problem 4 then implies

$$S(\rho') \geq S(\rho) \ . \tag{216}$$

In this sense a measurement is a dissipative, entropy-increasing process. A subtler result (due to *Lindblad*) that we will not prove here is that

$$S(\rho) \geq \sum_i p_i S(\rho_i) \ . \tag{217}$$

If entropy is regarded as "missing information" this gives a measure of the average information gain in the measurement process.

Strong subadditivity, quantum relative entropy, and mutual information

We have already noticed that some seemingly natural entropy inequalities fail in the quantum case. There is, however, a master inequality from which many other inequalities follow. It is called *strong subadditivity*. It states that

$$S(\rho_{123}) + S(\rho_2) \leq S(\rho_{12}) + S(\rho_{23}) \ . \tag{218}$$

This is a deep result due to *Lieb* and *Ruskai*. Since it was first proved in the 1970s there have been many attempts to find a simple proof, but these attempts have not been very successful.

The inequality can be rewritten in an interesting form if we purify the state ρ_{123} by introducing a fourth factor Hilbert space such that $\rho_{123} = \mathrm{Tr}_4 \rho_{1234}$. By assumption the four-partite state is pure, so we can rely on

$$S_{1234} = 0 \qquad S_{123} = S_4 \quad \text{and} \quad S_{12} = S_{34} \ . \tag{219}$$

Using this (and changing the label $4 \to 1$ at the end, to make the formula look more pleasing) we find that the strong subadditivity inequality becomes

$$S(\rho_1) + S(\rho_2) \leq S(\rho_{13}) + S(\rho_{23}) \ . \tag{220}$$

For the classical Shannon entropy the inequalities $S_1 \leq S_{13}$ and $S_2 \leq S_{23}$ hold separately. In the quantum case they do not, but their sum does.

Many important results follow from strong subadditivity. For an easy example, let the Hilbert space $\mathcal{H}_2$ be one-dimensional so that $S_2 = 0$. The inequality (218) then collapses too

$$S_{13} \leq S_1 + S_3 \ . \tag{221}$$

This is the subadditivity inequality.

Finally we define the quantum relative entropy in analogy to the classical case,

$$S(\rho||\sigma) = \mathrm{Tr}\left(\rho(\ln\rho - \ln\sigma)\right) \ . \tag{222}$$

If $[\rho, \sigma] \neq 0$ the two density matrices do not share any common eigenbasis. It follows that the relative entropy is an object that is hard to manipulate, even though it is every bit as important to quantum information theory as is its classical cousin to classical information theory. One reason for this is a theorem due to *Lindblad*, who used strong subadditivity to show that *quantum relative entropy is monotone under arbitrary* CP *maps*. The statements are that

$$S(\rho_{12}||\sigma_{12}) \geq S(\rho_1||\sigma_1) \tag{223}$$

$$S(\rho||\sigma) \geq S\left(\Phi(\rho)||\Phi(\sigma)\right) \ , \tag{224}$$

where Φ is any CP map.[52]

An easier result, requiring just a little bit more background than provided in our 'Lengthy Introduction', is that

$$S(\rho||\sigma) \geq 0 \ . \tag{225}$$

This is what we need to show that, unlike conditional entropies, the mutual information of two density matrices is still in the game. We define it by

$$S(\rho_1 : \rho_2) \equiv S(\rho_1) + S(\rho_2) - S(\rho_{12}) \ . \tag{226}$$

We then prove that[53]

$$S(\rho_1 : \rho_2) = S(\rho_{12}||\rho_1 \otimes \rho_2) \geq 0 \ . \tag{227}$$

So quantum mutual information has a good and potentially useful definition.

The upper bound for quantum mutual information turns out to be

$$S(\rho_1 : \rho_2) \leq 2S(\rho_1) \ , \quad S(\rho_1 : \rho_2) \leq 2S(\rho_2) \ . \tag{228}$$

[52] Why does the second statement follow from the first?

[53] Do this, by first proving that $\ln(\rho_1 \otimes \rho_2) = \ln(\rho_1 \otimes \mathbf{1}) + \ln(\mathbf{1} \otimes \rho_2)$.

The upper bound is easily seen to be saturated if ρ_{12} is a maximally entangled pure state. This is striking because it is a factor of 2 larger than expected classically. According to this measure then the correlations between the parts are really strong.

Quantum channels

A quantum channel allows us to send qubits rather than classical bits to the receiver. An optical fibre through which we send polarized photons can serve as a physical example. In quantum information theory a quantum channel is modeled by a CP map. A main aim of the theory is to define quantum channel capacities analogous to that of Shannon. But there will now be several different capacities, such as the capacity C to transmit classical information using a quantum channel, the capacity Q for transmitting quantum states, and a capacity Q_2 for the channel to transmit quantum states if it is assisted by a classical channel through which supplementary classical information can be sent (as happened in the quantum teleportation protocol). Calculating these capacities is difficult. Moreover some quite unexpected phenomena can occur. Thus two quantum channels may transmit more than twice the information transmitted by a single channel, if their inputs are entangled.

The oldest result in the theory, first stated by *Levitin* and then proved by *Holevo*, gives a useful upper bound on the capacity C. Let us begin by defining the latter. The sender constructs the message by choosing from a fixed set of letters $1, 2, \ldots, n$ with probabilities $p_1, \ldots, p_n$. That is to say, she has a random variable X with outcomes x_i. For each choice of x_i she prepares a density matrix ρ_i and sends it through the channel. The receiver cannot 'see' what density matrices he receives, but he can perform a measurement of his choice, getting outcomes that can be described as a random variable Y. The question is how strong the correlations between X and Y can be. This will depend on the choice of measurement, so we define the *accessible information* $H(X : Y)$ as the maximum of their mutual information, taken over all possible choices of measurement schemes. Evidently, what we are describing is not something that is easily calculated. What *Holevo* was able to prove was that

$$H(X:Y) \leq S(\rho) - \sum_i p_i S(\rho_i) \ , \qquad \rho = \sum_i p_i \rho_i \ . \tag{229}$$

There is nothing very easy about the proof, but we can unravel the right hand side a little. Suppose that Alice sends pure states only. This is a favourable case since $S(\rho_i) = 0$ in this case. If the pure states she is sending are orthogonal to each other we are back in the classical case in the sense that $S(\rho) = H(\vec{p})$, where $H(\vec{p})$ is the Shannon entropy of the source. We can then reach the classical maximum of the mutual information between the sent and the received message. If the pure states fail to be orthogonal they cannot be perfectly distinguished from each other by any measurement, and indeed $S(\rho) < S(\vec{p})$ in this case.

It sounds as if quantum theory is making matters worse. In this setup at most one classical bit can be transmitted by sending a qubit. But this result, from 1973, is not the end of the story. Suppose that Alice and Bob are in the possession of a maximally entangled state of two qubits. Alice has one qubit and Bob the other. Now recall the quantum teleportation protocol, in which entanglement made it possible to transmit an entire qubit by sending two classical bits. You can turn this around, and arrive at a *quantum dense coding protocol*, in which you transmit two classical bits by sending a single qubit only.[54] There is no contradiction of *Holevo*'s theorem here, because in this protocol some shared entanglement is being used up. This idea was, in a way, the starting point for the effort to show that quantum communication is quite superior to classical communication in certain well defined contexts. By now all the main theorems of classical information theory have been been generalized to take quantum theory into account, and a number of interesting applications have surfaced.

But since we have not said anything about quantum computing yet, we turn the page and go to a different topic.

Problem 4: A *bistochastic* matrix is a stochastic matrix such that the sums over columns and the sums over rows equal 1. Show that, alternatively, it can be defined as a stochastic matrix having the maximally mixed probability distribution as a fixed point. Then prove eq. (214) for arbitrary von Neumann measurements. You

[54] Exercise: Figure out how this protocol works, and spell it out.

should begin by showing that the vectors $\vec{p}$ and $\vec{\lambda}$ are connected by a bistochastic matrix. Then you have to rely on the convexity of the function $x \ln x$.

QUANTUM COMPUTATION

With very little time left we start a discussion of what may, or may not, turn out to be the most important part of the course. Certainly progress in this area is fast. In 2019 a group at Google announced that they had built a programmable processor using 53 superconducting qubits that outperformed any existing classical computer in a carefully selected problem. This has been compared to the airplane flown at Kitty Hawk by the Wright brothers. Not yet useful, but it does show some promise. Whatever happens, quantum computing illuminates what quantum theory is about.

Computation and complexity

In the 1930ies *Turing* analysed the meaning of *computability*. He came up with the notion of a *universal Turing machine* which is supposed to be able to compute anything that can be computed by means of algorithmic procedures. From a modern perspective you can think of a universal Turing machine as any existing computer, having a finite number of internal states and a finite program but modified so that its memory grows linearly with the length of the computation. Indeed the computer can be stripped down a lot, making it very slow but still universal, in the sense that given enough time it can mimic the actions of any other computer. It is generally agreed that no machine, whether classical or quantum, can do better than the Turing machine in this regard.

The universal Turing machine is used to *define* what we are supposed to mean by 'computable'. A function is said to be computable if there exists a program for the machine which takes the argument of the function as an input, and outputs the value of the function after a finite time. Since the input and the output can be coded in binary digits, the function is a function from the integers to the integers. Any question you may care to ask can be phrased in these terms. In ASCII encoding every upper or lower case Latin letter, Arabic numeral, question mark, and so on, is given by a 7 digit binary integer. Two symbols are then given by a 14 digit binary integer, and so on. Hence your question can be assigned a number, and the answer will be a function of that number.

The story changes if we are interested in obtaining the result in reasonable time. Suppose that the task is to multiply $n \times n$ matrices together. Proceeding as usual you see that this requires n^3 multiplications. This gives us some feeling for how the complexity of the calculation grows with n. We could say that it grows like n^3. Actually it is possible to improve the algorithm by trading some multiplications for additions, which are cheaper.[55] One can set up matrix multiplication so that that the number of multiplications grows like $n^{2.37}$, and perhaps further improvements are possible. Either way the growth is polynomial in the size of the input. We count time in terms of the number of computational steps needed, and say that matrix multiplication can be done in *polynomial time*, or equivalently that it belongs to the *complexity class* **P**.

As another example, consider factoring an integer N into primes, using an algorithm that applies to any N. If we use *Erathostenes*' sieve we simply check, for every integer less than or equal to its square root, whether it divides the given integer. Measuring the size of the integer in terms of the number n of binary digits needed to write it down, the size of the calculation grows like $2^{n/2}$, that is to say exponentially in the size of the input. This leads us to define the complexity class **EXP**, consisting of problems that can be solved in a time that grows exponentially with the size of the input. Clearly **P** is a subclass of **EXP**. The distinction between the complexity classes is fundamental, even if we do not have a proof that prime factorisation does not belong to that subclass. An algorithm that belongs to **P** is regarded as 'tractable'.

You can object that, as a practical matter, it is not obvious what to choose if the choice is between an algorithm with a running time $10^6 + 10^6 \cdot n$ and another with running time $e^{10^{-6} \cdot n}$ But this situation rarely occurs in practice. A deeper answer is that one can build an interesting theory based on the distinction between **P** and **EXP**. For instance, once an algorithm has been shown to be tractable in the sense that it belongs to **P**, it can be called as a subroutine in a larger program without taking the latter out of **P**.

Returning to the factoring of integers, we can use this problem to introduce a few more complexity classes. Consider first the less ambitious

[55] Exercise: For the matrices A and B in eq. (79), suppose you are given the seven products $(a_{00} + a_{11})(b_{00} + b_{11})$, $(a_{10} + a_{11})b_{00}$, $a_{00}(b_{01} - b_{11})$, $a_{11}(b_{10} - b_{00})$, $(a_{00} + a_{01})b_{11}$, $(a_{10} - a_{00})(b_{00} + b_{01})$, $(a_{01} - a_{11})(b_{10} + b_{11})$. Show that no further multiplications are needed to construct AB.

question whether a given integer is a prime or not. This is a yes/no question. A yes/no question is said to belong to the complexity class **BPP**, spelt out as bounded-error probabilistic polynomial, if there is an algorithm that runs in polynomial time and gives the correct answer with probability equal to 3/4.[56] It turns out that primality testing belongs to the complexity class **BPP**. Algorithms for primality testing that are in actual use are of this type, but in 2002 it was discovered that there does exist a deterministic algorithm that runs in polynomial time. So primality testing belongs to **P**. The lesson is that it may be difficult to decide what complexity class a given problem belongs to.

If you want to know what the factors of a non-prime integer are, the best existing classical algorithm is known as the Number Field Sieve. Its running time grows as $2^{n^{1/3}}$, which means that it requires exponential time. On the other hand, if you make a lucky guess about the factoring, you can check in polynomial time whether it is correct. This leads us to define the complexity class **NP**, for *non-deterministic polynomial*, consisting of problems whose answers can be checked in polynomial time.

Of course this does not prove that factoring a prime cannot be done in polynomial time on a classical computer. In fact, one of the main open problems in theoretical computer science is whether there exist problems that belong to **NP** without also belonging to **P**. What is known is that there are many problems that are **NP** *complete*, in the sense that if one could prove that one of them is in **P**, then the two complexity classes coincide. This said, there is close to a consensus that **P** $\neq$ **NP**. (And also close to a consensus that this distinction will be unaffected by quantum computation).

The **BQP** *complexity class*

Turing's definition of 'computable' hinges on functions from the integers to the integers, and you may ask if an analog computer (operating, like most of classical physics, with real numbers) can bring changes. The standard answer is that a physical analog computer would need a precision increasing exponentially with the size of the input in order to give an advantage. A

[56] Exercise: Change the 3/4 to any number larger than 1/2. How does this affect the complexity class of the problem?

physical analog computer will always be subject to noise, and this prevents the analog computer to have much impact on complexity theory. A quantum computer shares some features with analog computers, since it takes a continuum to label its states, but on the other hand the theory of measurement means that the measured output consists of a discrete set of possibilities. It is not called 'quantum' for nothing.

Deutsch raised the question of what would happen if the Turing machine is allowed to operate under the laws of quantum mechanics. One of his conclusions was that a quantum Turing machine can be always be simulated by a classical Turing machine, so the theory of quantum computation does not affect the definition of computable functions. But he also concluded that for certain problems the quantum Turing machine will be faster than its classical cousin, so we have to look at the complexity classes with fresh eyes.

Of course, the point we are driving at is that in 1994 *Shor* found an algorithm for factoring integers whose running time on a quantum computer grows like n^3, and which returns an answer that is correct with a probability greater than 3/4. This leads to the definition of a new complexity class **BQP**, bounded-error quantum polynomial. This has now to be placed somewhere in the hierarchy of classical complexity classes. The belief is that **BQP** is larger than **P** and larger than **BPP**, but not large enough to include all of **NP**. On the other hand it may include some problems outside **NP**. Evidently, since the question whether $\mathbf{P} \neq \mathbf{NP}$ is open, this is conjectural only, but the question what a quantum computer can do is presently attracting considerable interest.

We make three overall remarks before trying to define a quantum computer. The first is that in the years that have passed since *Shor*'s discovery, the number of genuinely new and interesting quantum algorithms that have been discovered is quite small. The second is that the obvious objection to quantum computers, that they will be prone to errors that cannot be corrected, has been quite succesfully countered. The objection simply does not hold, or at least it is not obvious that it holds. The third and final remark is that as far as practical applications are concerned the most promising ones seem to be *quantum simulators*, that is to say quantum computers designed to simulate physically interesting quantum systems. This possibility was first raised by *Feynman*, and it seems quite plausible that it will have consequences for, say, quantum chemistry in the not too distant future. We will,

however, spend the time that is left to us on the construction of a universal quantum computer. Whether useful or not, this is a machine that sheds light on quantum mechanics.

We have a fourth remark too. There are many choices to be made in the architecture of the universal quantum computer. We will use the *circuit model*, but other options exist. We will take the machine to operate on qubits, but this is not necessary. Eventually we will choose one out of many possible sets of universal gates. And so on. So the fourth remark is that whenever we make a choice, we make it without much comment.

The circuit model

A classical computer operates on bits, represented by integers $a, b, \ldots$, counted modulo two. That is, the integers take the values 0 or 1 and $1+1=0$. Physically, this may be no voltage, or some voltage. The aim is to calculate functions of strings of zeros and ones, taking values that are again strings of zeros and ones. The action can be broken down into elementary logical components called *gates*. Examples of gates include AND, OR, and NOT, connected by wires that are allowed to bifurcate. The AND gate accepts two inputs a and b, and returns the output ab. The OR gate also accepts two inputs, and returns the output $a+b+ab$. The NOT gate accepts a single input a and returns $a+1$. In all cases the arithmetic is modulo two.[57] From these simple ingredients one can build a universal computer. Of course there is some physics behind, but Figure 10 is our only comment on this. As *Turing* was saying, "being digital should be of more interest than being electronic". (Soon after he said that, the transistor was invented. The physical realization of computers is actually of considerable interest.)

A problem with the AND, OR, and NAND gates is that they are irreversible. You cannot recover their inputs from their outputs. There are thermodynamic reasons to worry about this, because irreversible evolutions generate heat. *Leclerc* and *Bennett* showed that one can construct classical computers that operate entirely with reversible gates. This was an important

[57]Exercise: Write the AND, OR, and NOT gates as logical truth tables. Write the NAND gate (AND followed by NOT) using both notations. Then show that you can construct OR from AND and NOT, and finally AND and NOT using only NAND gates.

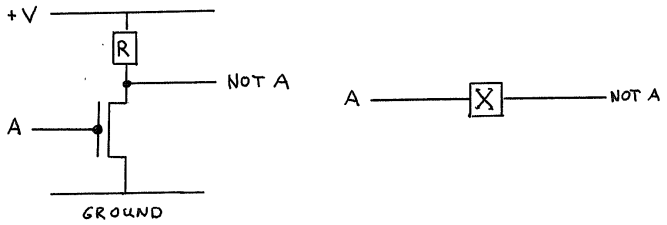


Figure 10: Two increasingly schematic pictures of the NOT gate. It includes a transistor, a (quantum!) device that conducts currents only in the presence of a voltage supplied by the input. A resistor is included as well.

step towards quantum computers.

A quantum computer operates by applying a reversible unitary transformation to a multi-qubit state described in a *computational basis* formed by product vectors. A measurement in the computational basis is performed at the end, in order to read the output. The unitary transformation must be built up from a finite number of more elementary unitary transformations, again called *gates*, in a way that can be efficiently described. We need a small set of gates, but large enough so that any unitary transformation can be well approximated. Then we have a *universal quantum computer*. On paper, that is.

The problem of finding a universal set of gates is solved in three steps. First we find a small set of unitary 2×2 matrices such that any unitary 2×2 matrix can be approximated, to any given precision, as a finite product of matrices from the set. In the second step we show that any unitary transformation acting on the full Hilbert space can be written as a string of unitary matrices that act non-trivially only on one or two qubits at a time. In the third step we show that it suffices to add a single two-qubit gate to the set of one-qubit gates.

For the first step we use the set $\{H, T\}$, where H is the Hadamard gate (67) and T is the $\pi/8$-*gate*

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \sigma \end{pmatrix} = e^{\frac{i\pi}{8}} \begin{pmatrix} e^{\frac{-i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{pmatrix} , \qquad \sigma \equiv e^{\frac{\pi i}{4}} . \tag{230}$$

The second equality is there only to explain the name of the gate. We can now construct other unitaries such as $Z = T^4$, $X = HT^4H$, and so on. The

key step in the proof of universality is to compose T and H in such a way that the resulting unitary effects a rotation of the Bloch sphere through an angle that is an irrational multiple of 2π. Once this is achieved the argument proceeds along the lines that *Euler* used to introduce his Euler angles, and you can go on to approximate any rotation to within some arbitrarily small ϵ. Two unitaries U and V are said to approximate each other to within ϵ if

$$||U|\psi\rangle - V|\psi\rangle||^2 < \epsilon \tag{231}$$

for every unit vector $|\psi\rangle$. We cut a complicated story short by saying that it is known how to take the first step, and that the number of discrete qubit gates you need to approximate arbitrary qubit unitaries grows like a small power of the logarithm of $1/\epsilon$.

The second and third steps are actually easier than the first, but we simply give the answer. All we need to add to our generating set is the *controlled-X* or CNOT gate acting on two qubits according to

$$|00\rangle \to |00\rangle \ , \quad |01\rangle \to |01\rangle \ , \quad |10\rangle \to |11\rangle \ , \quad |11\rangle \to |10\rangle \ . \tag{232}$$

The action of a gate on any state is defined by its action on the computational basis. In words we describe the CNOT gate by saying that you apply the X gate to the second qubit if and only if the first qubit is in the state $|1\rangle$. If we have several qubits we can apply the CNOT gate to any pair, leaving the others as they are.[58] In the course of the calculation it can happen that the qubits become entangled, in which case they do not have pure states of their own, but we can still apply our gates to them. The logic is exactly the same as when we represent an operator as a matrix.

The conclusion is that the set $\{H, T, \mathrm{CNOT}\}$ is a *universal* set of gates, in the sense that it can be used to approximate every unitary acting on n qubits. We skipped the proof, but you will probably trust the second and third step of the argument after looking at a few examples.

When we start to combine the gates we can use at least three different ways to describe things. We can use matrices (not recommended). One

[58] Exercise: Write out (232) as a matrix. Compare it with the matrices representing $X \otimes \mathbf{1}$ and $\mathbf{1} \otimes X$. Then write out all 8×8 matrices that describe the CNOT gate applied to any two out of three qubits.

alternative is to use arithmetic modulo two to describe the action on the basis states. The one qubit gates are generated by

$$H|a\rangle = (-)^a|a\rangle + |a+1\rangle \ , \qquad T|a\rangle = \sigma^a|a\rangle \ , \quad \sigma = e^{\frac{i\pi}{4}} \ . \tag{233}$$

Normalization factors are understood. We can now calculate the action of $X = HZH = HT^4H$ in three steps.[59] We obtain

$$|a\rangle \to (-)^a|a\rangle + |a+1\rangle \to |a\rangle + (-)^{a+1}|a+1\rangle \to |a+1\rangle \ . \tag{234}$$

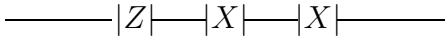
The CNOT is often denoted by C_X, for controlled-X. This prepares the notation for handling controlled-U gates, which apply the one-qubit unitary U to a qubit if the control qubit is in state $|1\rangle$, but leaves things alone if the control qubit is in state $|0\rangle$. Compare Problem 3 for the Dirac notation. The action of C_X on the basis states is

$$C_X|a,b\rangle = |a,b+a\rangle \ . \tag{235}$$

The notation becomes more cumbersome once we have to specify which, out of many, qubit serves as the control qubit and which qubit serves as the target.

Circuit diagrams

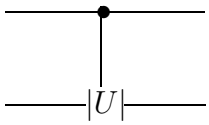
We now switch to *circuit diagrams*, in which each qubit is represented by a horizontal line interrupted by boxes to keep track of which unitary operator that is acting. The input is on the left and the output on the right. Thus the sequence XXZ is written as



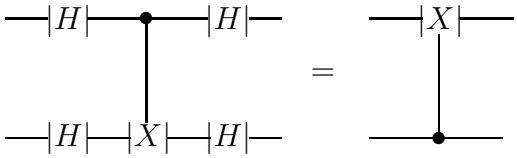
The controlled-U gate is[60]

[59] Exercise: Do all steps explicitly, and compare with the matrix notation.

[60] Exercise: Construct a C_Z gate from our universal set. Is it trivial to construct C_U for general U? Give a reason. (If your answer is no, rest assured that someone has done it.)

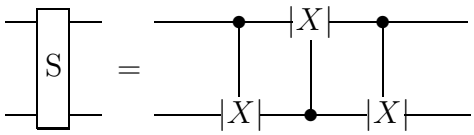


If you go through a few examples you will find that the circuit diagrams are close to self-explanatory.[61] The first example shows that we can switch the role of control and target in the definition of C_X:



At first sight, this looks wrong. Since $H^2 = \mathbf{1}$ it seems that we do nothing on the first qubit to the left of the equality sign, while we certainly do something on it to the right. The point, however, is that the matrices $H \otimes H$ and C_X do not commute.

In the second example we construct the SWAP gate, whose action can alternatively be written as $|a, b\rangle \to |b, a\rangle$:



Once we have constructed the SWAP gate it can be used as subroutine in larger circuit diagrams, which saves you from writing out three CNOT gates.

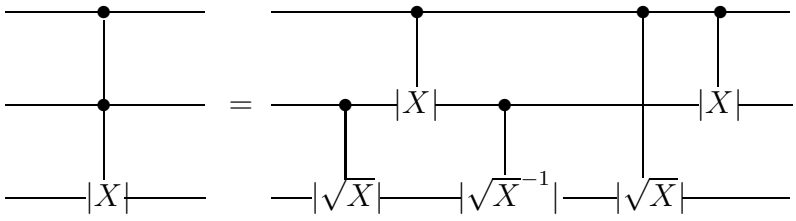
Note that, like the CNOT gate, the SWAP gate can be used in a classical computer too. Classically one can use two SWAP gates to interchange the role of control and target in a CNOT gate. The quantum computer manages this interchange using only Hadamard gates, which act on single qubits only.

Our third example is the *Toffoli gate*, which has two control qubits and one target. The action is $|a, b, c\rangle \to |a, b, c + ab\rangle$. The construction to follow makes use of the fact that, in quantum theory, NOT has a square root:

$$\sqrt{X} = HT^2H \quad \Rightarrow \quad (\sqrt{X})^2 = HT^4H = X \ . \tag{236}$$

[61] Exercise: Verify the following three circuit diagram equalities by tracing through what happens to the computational basis states.

The circuit diagram that defines the Toffoli gate is[62]



Like the gates X and C_X the Toffoli gate can be defined also in classical computer circuits acting on bits. You can see that if the third input bit is set to 1 the third output bit will be the NAND of the first two inputs. Given that the NAND gate is all you need for a universal computer this means that the Toffoli gate is all you need to make a reversible classical computer universal. But classically it has to be defined as a primitive, because the square root of NOT does not exist classically.

The quantum case is different because one and two-qubit gates are enough to ensure universality. This is very good news if you want to build a quantum computer. One qubit gates are easier to fabricate than are two qubit gates. Fabricating three qubit gates would be very hard.

Continuing in this way, we can build a circuit that approximates any unitary acting on an arbitrary finite number of qubits. (I did not say it is easy.) But we have still to discuss the *sine qua non* of the quantum computer: preparation and measurement.

Preparation and readout

We make the convention that the qubit register is initialized in the state $|0, 0, \ldots, 0\rangle$. The computation therefore begins by creating some more interesting state to act on. We may take it that the aim is to compute an integer valued function f, taking an integer x as its argument. Let us assume that $x < 2^n$ and $f(x) < 2^m$. We then divide the register into an n qubit *input register* and an m qubit *output register*. We may need additional work qubits to act on, and if so we must take care that the calculation does not leave them entangled with the input and output qubits.

[62]Exercise: In view of our discussion of open systems, what is the reason for the final CNOT gate?

We write the integer x in binary form, so that we get a sequence of no more than n zeros and ones. By means of a unitary transformation the register is transformed into the state $|x\rangle_n|0\rangle_m$, where $|x\rangle$ is an n-qubit state encoding the input. The m-qubit state $|0\rangle_m$ is there to ensure that the transformation is reversible, as we will see in a moment. By hook or crook, we find a unitary transformation U_f such that

$$U_f|x\rangle_n|y\rangle_m = |x\rangle_n|y + f(x)\rangle_m \ . \tag{237}$$

In particular[63]

$$U_f|x\rangle_n|0\rangle_m = |x\rangle_n|f(x)\rangle_m \ . \tag{238}$$

This transformation is reversible, and in fact its own inverse, because

$$U_f|x\rangle_n|f(x)\rangle_m = |x\rangle_n|f(x) + f(x)\rangle_m = |x\rangle_n|0\rangle_m \ . \tag{239}$$

A similar division of the register into an input and an output register is needed for a reversible classical computer to work.

Pause to make sure what is being meant. Suppose we wish to compute $f(5) = 3$. In binary this is $f(101) = 11$. It is enough to use a three qubit input register and a two qubit output register. We need to build a unitary transformation such that

$$U_f|101\rangle|00\rangle = |101\rangle|11\rangle \ . \tag{240}$$

It should be clear why $|f(x) + f(x)\rangle_m = |0\rangle_m$ even though $f(x) + f(x) \neq 0$. It happens because the arithmetic of the ket labels is modulo 2, meaning that we do no carrying on the ket labels. In fact $f(x) + f(x)$ *is* equal to zero modulo 2.

So far the discussion would apply also to a reversible classical computer. But let us apply a Hadamard gate to every input qubit,

$$H|0\rangle = |0\rangle + |1\rangle \ , \quad H^{\otimes^2}|00\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle \ , \tag{241}$$

[63]Exercise: Set $f(x) = x$. Are we violating the no-cloning theorem? If not, why not?

and so on for $H^{\otimes 3}$ acting on a three-qubit Hilbert space, etc. (As usual we ignore overall normalisation factors.) When we do go on, we obtain the remarkable formula[64]

$$H^{\otimes^n}|0\rangle_n = \sum_{x<2^n} |x\rangle \ . \tag{242}$$

A single application of the unitary U_f now has the effect that

$$U_f(H^{\otimes^n} \otimes \mathbf{1}^{\otimes^m})|0\rangle_n|0\rangle_m = \sum_{x<2^n} |x\rangle_n|f(x)\rangle_m \ . \tag{243}$$

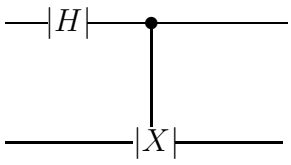
It seems as if we have computed every value of the function in a massively parallel computation. But the information has not yet reached its destination. In the end we have to perform a measurement. In quantum computation this is not just an afterthought. It is an essential part of the computation.

If we start by measuring the input register in the computational basis the state collapses with equal probability to anyone of the states

$$|x\rangle_n|f(x)\rangle_m \ . \tag{244}$$

We now know x, and a measurement on the output register yields the value of the function $f(x)$. This quantum computation therefore gives as much information as the classical one. The one difference is that the choice of x was made at random after the completion of the calculation (which is a bit odd, but hardly an advantage).

But maybe we did not ask the right question? Perhaps we could design some measurement that extracts global information about the function f, rather than some special value? Before asking this in earnest we practice a little on how to prepare interesting input states. It is easy enough to design a circuit that affects the transition $|0,0\rangle \to |0,0\rangle + |1,1\rangle$, namely



[64]Exercise: Make sure that you understand this and the following formula, for instance by writing them out for three qubits.

This is interesting because we have created an entangled state from a separable state. This supports the claim—whose proof I skipped—that we can approximate arbitrary unitary transformations using only the gates H, T, and C_X, so that we can produce any state whatsoever from the initial state $|0\rangle_n$.[65]

Many quantum information protocols end with a measurement in some basis other than the computational one. In the quantum teleportation protocol Alice is asked to perform a measurement using a nice error basis, that is to say (if she teleports qubits) in the Bell basis

$$|\Phi^{\pm}\rangle = |0,0\rangle \pm |1,1\rangle \ , \qquad |\Psi^{\pm}\rangle = |0,1\rangle \pm |1,0\rangle \ . \tag{245}$$

A moment's thought shows that our insistence that the result of the quantum computation should be read out by means of a measurement in the computational basis imposes no restriction. We can still perform a measurement in the Bell basis if we first perform a unitary transformation that turns the Bell basis into the computational basis, and then measure.[66]

The Deutsch–Jozsa algorithm

The *Deutsch–Josza* algorithm is a proof-of-principle, showing that there exists a problem where a quantum computer provides a speed-up compared to what a classical computer can do. The problem it solves is not particularly interesting in itself, in fact it is quite contrived, but the underlying idea recurs in more interesting algorithms. Suppose we have a function from $\{0,1\}$ taking values 0 or 1, and a circuit that computes it, that is to say that

$$U_f|0\rangle|y\rangle = |0\rangle|y + f(0)\rangle \ , \qquad U_f|1\rangle|y\rangle = |1\rangle|y + f(1)\rangle \ , \tag{246}$$

where $y \in \{0,1\}$ is arbitrary. It may be expensive to run this calculation however. The question is: How many times do we have to run the calculation before we know whether $f(0) = f(1)$? This is an example of an *oracle* problem. Applying the unitary U_f is like asking an oracle for an answer. The question is how many times we have to ask the oracle before we know

[65] Exercise: Design a circuit that effects the transition $|0,0,0\rangle \to |\mathrm{GHZ}\rangle$, where the GHZ state is $|\mathrm{GHZ}\rangle = |0,0,0\rangle + |1,1,1\rangle$.

[66] Exercise: Design the circuit we need for this.

the answer we want to have. In a classical computer we would have to ask twice, but the Deutch-Josza algorithm allows a quantum computer to answer the question with only a single application of U_f.

The trick is to make a suitable preparation before the oracle is called. Thus

$$|0\rangle|0\rangle \to (H \otimes H)(X \otimes X)|0\rangle|0\rangle = (|00\rangle - |01\rangle - |10\rangle + |11\rangle \ . \tag{247}$$

Now we call the oracle. Denoting $f(x) + 1 = \bar{f}(x)$ we obtain

$$|0\rangle|f(0)\rangle - |0\rangle|\bar{f}(0)\rangle - |1\rangle|f(1)\rangle + |1\rangle|\bar{f}(1)\rangle \ . \tag{248}$$

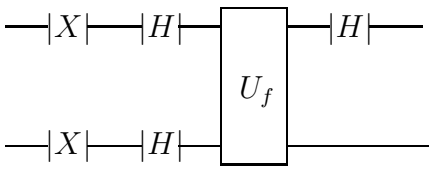
It is a small exercise to check this, and then to check that if $f(0) = f(1)$ the result is

$$(|0\rangle - |1\rangle)(|f(0)\rangle - |\bar{f}(0)\rangle) \ , \tag{249}$$

while if $f(0) = \bar{f}(1)$ it is

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |\bar{f}(0)\rangle) \ . \tag{250}$$

Finally we apply a Hadamard gate to the input register, and make a measurement of the input register. If the qubit collapses to $|1\rangle$ the function is constant, if it collapses to $|0\rangle$ the function is not constant.[67] And the oracle was called only once, as you can see from the circuit diagram.



Notice however that if we measure the output register we get no information about the actual values taken by the function. At most we can say that it is $f(0)$ with probability one half or $\bar{f}(0)$ with probability one half. So it is a trade off. We changed the question to be about a global property of the

[67] Exercise: Check it all, starting from the small exercise mentioned in the text.

function. And in a sense this is the point: In a quantum computer we can ask a wider range of questions about the function.

You may object that, when claiming that the quantum computer outperforms the classical one, we are to some extent comparing apples to oranges. The answer obtained from the quantum oracle is more structured than is that from the classical oracle, so it is not surprising that more can be done with it. More is needed to convince us that there are tasks where the quantum computer wins.

The need to reverse

There is a complication to be faced as well. If the function that is being evaluated (by the oracle, or by some circuit that we have designed for the purpose) is a complicated one, then the quantum computer will need a number of 'work qubits' to act on as well. If, in the course of the calculation, the work qubits become entangled with those in the output register then we have a problem, because then the state of the qubits in the output register is no longer pure. Measuring the output register will provide information about how the output is correlated to the work qubits, and not about the result of the calculation.

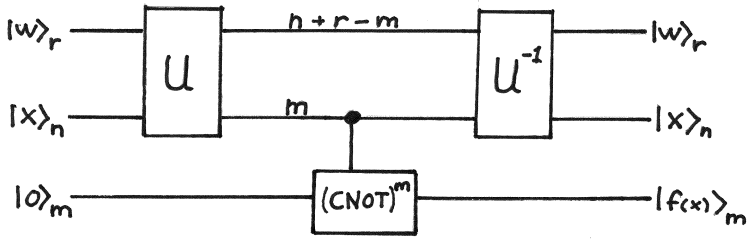


Figure 11: How to disentangle the output from the machine.

This is where it becomes important that unitary transformations are reversible. Let the dimension of the work subspace be 2^r, the dimension of the input subspace be 2^n, and the dimension of the subspace where we intend to encode the result be 2^m. The unitary operator U_f will act on the $r + n$ qubits forming the work and input subspaces. The next step is to copy the

output onto the m qubits that form the output register. Using CNOT gates this can be done without disturbing the output of the calculation. Then we perform the inverse transformation U_f^{-1} on the first $r+n$ qubits. At the end the work qubits and the input register have returned to their initial separable states, while the output is safely registered where we want to have it. Figure 11 should make this clear.

This solves the problem, but it shows that quantum computation is twice as expensive as you may have expected.

Shor's algorithm

The Deutsch-Josza algorithm answers no interesting question, but it serves as an inspiration for algorithms that do. The outstanding example remains *Shor*'s algorithm for finding the two prime factors of a large number N. We will look at it in some detail, because it is probably a very good example of what universal quantum computers can do—if supported by classical computers that do calculations on the side.

Let n be the number of binary digits of N. In the best of the known classical factoring algorithms the number of calculational steps grows like $2^{n^{1/3}}$, while it grows like n^3 or (with improvements) like n^2 in the central part of Shor's algorithm. We are allowed to add classical calculations that grow like n^2, and the exponential speed-up is still there. We also note that the problem is in **NP**, that is to say if it is suggested that N is equal to pq then we can check it in polynomial time. This means that all we need is an algorithm that gives the correct answer with a non-zero probability. If we did not obtain the correct answer we simply run the algorithm again.

The quantum speed-up actually happens in a subroutine, where one uses a discrete Fourier transformation to find the period of a certain function. Before we come to that it is worthwhile to understand something about the problem, why it is of practical interest, and how the result of the subroutine is used to solve the problem. It may be that all useful applications of a universal quantum computer will hinge on our ability to see the kind of questions that quantum computers are good at, sitting inside some genuinely interesting mathematical problem.

Prime factorisation and RSA cryptography

First we will see why prime factorisation is of practical interest, and how it can be reduced to the problem of finding the period of a certain function. We will come back to quantum computing once we have the answers.

Prime factorisation plays a role in *public key cryptography*. The idea here is to rely on a mathematical problem that is easy to solve one way, and hard to solve the other way. Using factorisation of integers for this purpose leads to *RSA cryptography* (for *Rivest*, *Shamir*, and *Adleman*, who were the first outside the British Secret Service to come up with the idea). Imagine a cryptographic protocol that requires a composite number N for encryption, but the prime factorisation $N = pq$ for decryption. Starting from two large primes p and q the receiver announces N publicly, so that anyone can use it for encryption. To read the encrypted message you must either know p and q in advance, which is true only for the intended receiver of the message, or calculate them, which will take an inordinate amount of time if you rely on an algorithm whose running time grows exponentially with the number of digits in N.

To see how this comes about we need some knowledge of arithmetic. First we note that *Euclid* provided a very fast algorithm for finding the greatest common divisor (a, b) of two integers. If $a < b$ you divide b with a to obtain the remainder r, and then observe that $(a, b) = (r, a)$. This reduces the size of the problem, and by repeating the process you reach the answer in polynomial time, in fact in about the time it would take to just multiply the two numbers together. Given any two integers a and b this algorithm also yields two integers m and n such that

$$am + bn = (a, b) \ . \tag{251}$$

If $(a, b) = 1$ the pair of integers have no common factor, and then they are said to be *relatively prime*.

Before we continue our journey through elementary number theory, let me say that although all the proofs we need are simple they can be quite exhausting to follow. We are tackling a serious mathematical problem, and it is only to be expected that this will involve some serious mathematics.You may prefer to take it on trust, as being part of the classical pre- and post-processing of the quantum algorithm.

With this warning we come to *modular arithmetic*. Two integers are declared to be *equal modulo* N if they differ by a multiple of N,

$$a = b \bmod N \quad \Leftrightarrow \quad a = b + nN \ . \tag{252}$$

Addition and multiplication modulo N is defined in the obvious way. Now consider two relatively prime integers a and N. From eq. (251), with N in the role of b and with $(a, N) = 1$, it follows that there always exist an integer m such that

$$am = 1 \bmod N \ . \tag{253}$$

Hence, provided $(a, N) = 1$, a has an inverse in arithmetic modulo N. This means that the set of non-zero integers relatively prime to N form a *group* under multiplication modulo N. We will be interested in the *order* of this group, that is to say in the number of its elements. This is given by *Euler*'s *totient function* $\phi(N)$, defined as the number of integers smaller than and relatively prime to N. If p and q are distinct primes the totient function is

$$\phi(p) = p - 1 \ , \qquad \phi(pq) = (p-1)(q-1) \ . \tag{254}$$

We need only these two cases. Clearly, if we know pq and $\phi(pq)$ we can determine p and q.

Confusingly we will also be interested in the *order* of an integer a, that is to say in the smallest integer r such that

$$a^r = 1 \bmod N \ . \tag{255}$$

Given an integer a relatively prime to N the set of integers of the form a^x mod N forms a subgroup of the multiplicative group we are interested in. The order of this subgroup is r. *Lagrange*'s theorem says that the order of a subgroup always divides the order of the whole group, so r divides $\phi(N)$. In every case it must be true that

$$a^{\phi(N)} = 1 \bmod N \ . \tag{256}$$

This is called *Euler's theorem*. It must hold, otherwise the number of elements in the group would be larger than its order.[68]

[68] Exercise: For $N = 4, 5, 6, 7, 9, 10, 15$, find the multiplicative inverse modulo N of every

In our examples N will be huge. It is nevertheless a quick affair to let a computer calculate a^x modulo N. The number of multiplications needed is kept modest if we do the calculation by repeated squaring,

$$a \to a^2 \to a^{2^2} \to a^{2^3} \to \dots \ . \tag{257}$$

Then a^x is created by multiplying a subset of these powers together. In this way a^x can be calculated in polynomial time on a classical computer.[69]

Incidentally, this gives us a hint why primality testing is easier than factorisation. If there is an integer $a < N$ such that $a^{N-1} \neq 1$ modulo N then N cannot be a prime number because a and N would have a common factor. Unfortunately there are composite numbers that pass this test ($361 = 3{\cdot}11{\cdot}17$ is the smallest example), which is why the full story is much longer.

We now have all the number theory we need for RSA cryptography. The protocol starts when the receiver picks two large primes p and q, and another integer c relatively prime to $(p-1)(q-1)$. She also calculates the inverse of c in arithmetic modulo $(p-1)(q-1)$. This is an integer d such that

$$cd = 1 \bmod (p-1)(q-1) \ . \tag{258}$$

The product $N = pq$ and the integer c are made public, but p, q, and d are kept secret. Anyone wanting to send a message to the receiver converts the message to an integer a less than N (using ASCII encoding, say), and checks that a is relatively prime to N. Then she calculates the encrypted message

$$b = a^c \bmod N \ . \tag{259}$$

The message is easily decrypted by anyone knowing the secret integer d, because

$$b^d = a^{cd} = a^{1+n(p-1)(q-1)} = a \bmod N \ . \tag{260}$$

All the calculations are done in polynomial time.

What can the eavesdropper do? To compute d she needs to factor the integer N. Mathematicians have worked on this problem since the days of

integer that has one, and count them. Verify that $\phi(pq) = (p-1)(q-1)$ when p and q are distinct primes. Find examples of integers having an order lower than $\phi(N)$. Finally, $\phi(403) = 360$. Use this information to factor 403.

[69] Exercise: Calculate 2^{21} modulo 35, using only six multiplications.

Eratosthenes, and so far the best algorithm they have come up with runs in exponential time. If N is large enough this suggests that the message will be safe from eavesdroppers for many years to come. To learn what large enough means in practice, we note that in 2016 the NSA recommended keys with at least 3072 bits. Keep in mind that the NSA has a history of recommending cryptos that they themselves can just break.

Actually the eavesdropper can get by with somewhat less. She only needs to find the order of b, that is to say an integer r such that

$$b^r = 1 \bmod N \ . \tag{261}$$

The order divides $\phi(N) = (p-1)(q-1)$, but may not be equal to it. Now the publicly known integer c is relatively prime to the unknown integer $\phi(N)$. Since r is one of the factors of the latter it follows that $(c, r) = 1$. It then follows that there exists an integer d' such that

$$cd' = 1 \bmod r \ . \tag{262}$$

The next point to notice is that when two integers a and b are related the way they are in the RSA protocol then they have the same period. This is because we are assured that integers c and d exist such that $b = a^c$ and $a = b^d$. This means that the integers a and b belong to the same cyclic subgroup of the multiplicative group of integers relatively prime to N, and their respective orders are both equal to the order of that subgroup. Hence $a^r = 1 \bmod r$. Equipped with all these assurances, and assuming that she can find the period r in the time at her disposal, the eavesdropper performs the calculation

$$b^{d'} = a^{cd'} = a^{1+nr} = a \bmod N \ . \tag{263}$$

She can now read the message at her leisure.

What is the size of the calculation Eve must do to find the period r? It is convenient to rephrase the problem slightly by defining the function $f_a(x) = a^x$. Then the element a is of order r if and only if the function $f_a(x)$ is a periodic function of period r in arithmetic modulo N,

$$f_a(x) = a^x \quad \Rightarrow \quad f_a(x+r) = a^{x+r} = a^x = f_a(x) \ . \tag{264}$$

Now the question is how hard it is to find the period of this function. Classically, the way to find the period is to evaluate $f_a(x)$ for many values of x, until one finds a pair x_1 and x_2 such that $f_a(x_1) = f_a(x_2)$. The period will then be a divisor of $x_1 - x_2$, and by finding a few such coincidences it is likely that the period is the largest common divisor of them all. But since the difference $f_a(x_1) - f_a(x_2)$ can take N different values we need to examine about N different pairs to find a coincidence. The number of different pairs is roughly the square of the number of evaluations of f_a that we perform, so it follows that we are likely to need $\sqrt{N}$ evaluations of the function before we find a single coincidence. If $N \approx 2^n$ this means that the procedure is exponential in n. And this is *provably* the best a classical algorithm can do with the period finding problem. But a quantum computer offers an exponential speed-up. A constant number of evaluations, followed by some computational steps that take polynomial time only, suffice.

Before we turn to this, we should perhaps finish the factorisation question. If we know $\phi(pq)$ we can factor $N = pq$, but there is no guarantee that the period r equals $\phi(pq)$. It could be a divisor of $\phi(pq)$. However, suppose that we are lucky, and that the period r we find is even. Then we can write

$$0 = a^r - 1 \bmod N = (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) \bmod N \ . \tag{265}$$

If either $a^{\frac{r}{2}} + 1$ or $a^{\frac{r}{2}} - 1$ is a multiple of N then we are out of luck, and learn nothing. But if not, the greatest common divisor of N with one of the factors on the right hand side will be a factor of N (and the greatest common divisor can be calculated efficiently using Euclid's algorithm). Fortunately, number theorists can prove that if you pick the integer a at random then with probability 3/8 the period will be even and neither of the above factors are multiples of N (although this theorem takes us a bit beyond Euclid). So, once we have found the period we can factor N with probability 3/8. If the algorithm that allowed us to find the period runs in polynomial time we can simply repeat the procedure until we get lucky. This proves that if the period finding problem belongs to the complexity class **BQP** then so does the factoring problem.

Period finding

We have reached the conclusion that it is of great theoretical and practical interest to find the period of the function $f(x) = a^x$ modulo N where N is a product of two primes and a is a given integer. Thus we ask for an integer r such that $f(x+r) = f(x)$ modulo N. The hope is that quantum theory will allow us to ask for the period of the function without actually having to ask for the values it takes.

In the first step we realize the transformation

$$|0\rangle_{\bar{n}}|0\rangle_n \;\rightarrow\; |x\rangle_{\bar{n}}|0\rangle_n \;\rightarrow\; \sum_{x=0}^{2^{\bar{n}}-1} |x\rangle_{\bar{n}}|f(x)\rangle_n \;, \tag{266}$$

where $f(x) = a^x$ and n is the smallest integer such that $2^n > N$. The input register consists of $\bar{n}$ qubits, and for a reason that will only transpire at the end we choose $\bar{n} = 2n$. The transformation goes along the lines of equation (243), but this time it is not an oracle problem. We work with a concrete function. If the number of binary digits in N is 3072, or thereabouts, we need many qubits for the purpose. However, on paper, making use of the fact that the function is quite special and can be handled with repeated squaring as in equation (257), we can do this in an efficient manner. I skip the details of this interesting step.

To reduce clutter we now perform a measurement on the output register, and obtain a value $f(x_0)$ for the function. This means that the $\bar{n}$ qubit input register collapses to a superposition of all the values of x that return this value of f, namely

$$|x\rangle_{\bar{n}} \;\rightarrow\; |\psi\rangle = \sum_{j=0}^{m-1} |x_0 + jr\rangle_n \;. \tag{267}$$

Here x_0 is the smallest integer for which the function returns the value we found, and m is the smallest integer such that $x_0 + mr \geq 2^{\bar{n}}$. We write it all out for clarity, this time including the normalization:

$$|\psi\rangle = \frac{1}{\sqrt{m}}(|x_0\rangle + |x_0 + r\rangle + \ldots + |x_0 + (m-1)r\rangle) \;. \tag{268}$$

The unknown period r is in there, but it is not so easy to get it out. A measurement on the input register would collapse the state to one of the m states

$$|x_0 + jr\rangle \ . \tag{269}$$

This is not helpful, because the value of x_0 is not known, and it would change if we run the procedure again. So we change the question.

We need a unitary transformation that moves the unwanted integer x_0 into an overall phase factor that does not affect the probability vector. The *discrete Fourier transformation* in dimension d is defined by its action on the basis states, as[70]

$$F|x\rangle_{\bar{n}} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{xk} |k\rangle_{\bar{n}} \ , \qquad \omega_d = e^{\frac{2\pi i}{d}} \ . \tag{270}$$

Note carefully that in the exponent of ω the integers x and k are treated as ordinary integers. The product is nevertheless taken modulo d because ω is a dth root of unity. In our application we set $d = 2^{\bar{n}}$. The discrete Fourier transformation is very important in many applications, also in classical signal processing. In fact it is important enough to deserve an acronym of its own: DFT.

When we apply F to the input register we obtain

$$F|\psi\rangle = \frac{1}{\sqrt{2^{\bar{n}} m}} \sum_{k=0}^{2^{\bar{n}}-1} \sum_{j=0}^{m-1} \omega^{(x_0+jr)k} |k\rangle_{\bar{n}} = \frac{1}{\sqrt{2^{\bar{n}} m}} \sum_{k=0}^{2^{\bar{n}}-1} \omega^{x_0 k} \sum_{j=0}^{m-1} \omega^{jkr} |k\rangle_{\bar{n}} \ . \tag{271}$$

Now we perform the measurement on the input register. The probability of obtaining the kth outcome is

$$p_k = |\langle k|F|\psi\rangle|^2 = \frac{1}{2^{\bar{n}} m} \left| \sum_{j=0}^{m-1} \omega^{jkr} \right|^2 \ . \tag{272}$$

This depends on the period r while x_0 has disappeared, just as we wanted.

There are two questions left to address. How do we physically implement the Fourier transformation, and how do we extract r from the probabilities? We will see the quantum speed-up when we address the first question.

[70] Exercise: Prove that this is a unitary operator. Square it to see what happens. Also verify equation (272).

The Fourier transform: Fast and faster

We have arrived at the heart of the matter, where the quantum speed-up happens. Acting on the components of a vector, rather than on the basis vectors, the discrete Fourier transform in dimension d is

$$\hat{\mathbf{f}} = F_d \mathbf{f} \quad \Leftrightarrow \quad \hat{f}_j = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega_d^{jk} f_k \ . \tag{273}$$

It arises whenever a continuous signal has been sampled at discrete points. A first look suggests that it requires d^2 multiplications. However, classically, the Fast Fourier Transform (or FFT) achieves the same goal with only $d \log d$ multiplications, and the even faster quantum Fourier transform builds on that idea. It is assumed that $d = 2^n$. (This is the case we are interested in. If d is not of this form we can pad the vector to be transformed with zeros until the dimension reaches 2^n for some n.) The $d = 2$ Fourier matrix is already familiar to us,

$$F_2 = H \ . \tag{274}$$

Moving on to $d = 2^2$ we decide to label the components of the vector using binary digits. Then we see that

$$F_4 \mathbf{f} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^2 & 1 & \omega_4^2 \\ 1 & \omega_4^3 & \omega_4^2 & \omega_4 \end{pmatrix} \begin{pmatrix} f_{00} \\ f_{01} \\ f_{10} \\ f_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4^2 & \omega_4 & \omega_4^3 \\ 1 & 1 & \omega_4^2 & \omega_4^2 \\ 1 & \omega_4^2 & \omega_4^3 & \omega_4 \end{pmatrix} \begin{pmatrix} f_{00} \\ f_{10} \\ f_{01} \\ f_{11} \end{pmatrix} \ . \tag{275}$$

Remembering that $\omega_4^2 = i^2 = -1 = \omega_2$, we see that provided we reorder the components of the vector before applying the matrix, we can replace the matrix F_4 with

$$F_4 \ \rightarrow \ \begin{pmatrix} F_2 & D_2 F_2 \\ F_2 & -D_2 F_2 \end{pmatrix} \ , \quad \text{where} \quad D_2 = \begin{pmatrix} 1 & 0 \\ 0 & \omega_4 \end{pmatrix} \ . \tag{276}$$

We achieve this by placing the even columns of the matrix before the odd ones. In the vector, the even components f_{a0} are placed before the odd components f_{a1}.

The same trick works when we double the dimension again. Before applying F_8, we place the even vector components f_{ab0} above the odd components f_{ab1}, and we place the even columns of the matrix before the odd ones. This has the effect that

$$F_8 \;\to\; \begin{pmatrix} F_4 & D_4F_4 \\ F_4 & -D_4F_4 \end{pmatrix}, \qquad \text{where} \qquad D_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \omega_8 & 0 & 0 \\ 0 & 0 & \omega_8^2 & 0 \\ 0 & 0 & 0 & \omega_8^3 \end{pmatrix}. \quad (277)$$

(Yes, this becomes easier to see if you write it out explicitly, but typographically it takes a lot of space.) We now work recursively. We replace F_4 with the expression we already have. We can do this if we perform the appropriate reordering within the two sets of four components of the vector. So, reordering in two steps,

$$\begin{pmatrix} f_{000} \\ f_{001} \\ f_{010} \\ f_{011} \\ f_{100} \\ f_{101} \\ f_{110} \\ f_{111} \end{pmatrix} \to \begin{pmatrix} f_{000} \\ f_{010} \\ f_{100} \\ f_{110} \\ f_{001} \\ f_{011} \\ f_{101} \\ f_{111} \end{pmatrix} \to \begin{pmatrix} f_{000} \\ f_{100} \\ f_{010} \\ f_{110} \\ f_{001} \\ f_{101} \\ f_{011} \\ f_{111} \end{pmatrix}. \quad (278)$$

The net effect is that we have ordered the components in *bit reversed* order.

We can start the recursion from a Fourier matrix of arbitrary size. Moving all the even numbered columns to the left we replace

$$F_d \;\to\; \begin{pmatrix} F_{\frac{d}{2}} & D_{\frac{d}{2}}F_{\frac{d}{2}} \\ F_{\frac{d}{2}} & -D_{\frac{d}{2}}F_{\frac{d}{2}} \end{pmatrix}, \quad (279)$$

where the definition of the diagonal matrix D_d should be clear. The fact that this works is known as the *Danielson–Lanczos* lemma, formulated back in the days when discrete Fourier transformations were performed by humans, and multiplication took a lot of time. It leads to the following recipe for performing the Fast Fourier Transform: Start with a vector having 2^n components

and write its components in bit reversed order. Apply F_2 to all successive pairs of components. In the second step we apply the matrix

$$\begin{pmatrix} \mathbf{1} & D_2 \\ \mathbf{1} & -D_2 \end{pmatrix} \tag{280}$$

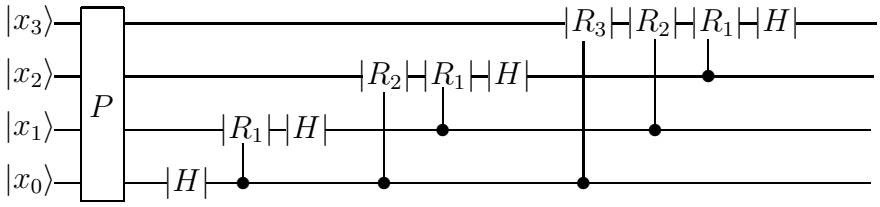
to all quartets of components. In the third step we apply

$$\begin{pmatrix} \mathbf{1} & D_{2^2} \\ \mathbf{1} & -D_{2^2} \end{pmatrix} \tag{281}$$

to each set of 2^3 components. And so on. In each step we perform about d multiplications, and we are done after $n = \log d$ steps. This is to say that we have brought the number of multiplications down, from d^2 to $d \log d$. The preliminary bit reversal is computationally cheap, so this is a remarkable achievement. But it remains exponential in n.

We want more. We want the calculation to be polynomial in n. At the same time we are willing to settle for less, because we do not need to calculate the individual components of the Fourier transformed vector. All we need is to calculate $F|\psi\rangle$ in eq. (271). From this we can extract at most one component by means of a measurement.

Let us construct a circuit that does this. The case of a four qubit Hilbert space is enough to give the idea. I first give the answer:



We have yet to define P and R_k, but it should already be clear what the circuit looks like for any n. In particular you can write down the circuits for $n = 2$ and $n = 3$ and play with them, until you see why they work as advertized.

The circuit begins with a computationally cheap permutation P effecting a qubit reversal of the input,

$$|x_3x_2x_1x_0\rangle \to |x_0x_1x_2x_3\rangle \ . \tag{282}$$

Then follows a number of Hadamard gates, and a number of controlled unitaries C_{R_k}, where the one qubit phase gates R_k are defined as

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \sigma_k \end{pmatrix} \ , \qquad \sigma_k = e^{\frac{i\pi}{2^k}} \ . \tag{283}$$

In the circuit the chosen integer k depends on the 'distance' to the control qubit. This is all.

Why does this work? If we act with this circuit on an n-qubit computational basis state we will get a superposition of 2^n basis states out, because each qubit is subject to a Hadamard before we let it go. It will be an equal weight superposition because the only amplitudes we introduce are phase factors. The 2^nth root of unity $\omega_n = \sigma_{n-1}$ will appear only if the last digit in the output is 1, and then only if the last (because of the P-gate) digit of the input is 1. The phase factor $\omega_n^2 = \sigma_{n-2}$ will appear if the next to last digit in the output and the last digit in the input is 1, and if the last digit in the output and the next to last digit in the input is 1. And so on. And this is just right for the DFT.[71]

It is time to count the number of gates that appear in the circuit for arbitrary n. For the initial reordering it is enough to use $n/2$ SWAP gates. Then there are n Hadamard gates, while the number of phase gates is

$$1 + 2 + \ldots + (n-1) = \frac{n(n-1)}{2} \ . \tag{284}$$

Hence the number of gates needed to effect the quantum Fourier transform grows like n^2, a remarkable improvement compared to the classical FFT which needs $2^n n$ operations. It is true that we do not get as much information out of the quantum Fourier transform as we get out of the FFT, but we do get out all the information we need for Shor's algorithm to work.

We are using a number of two-qubit gates here, and these are difficult to manufacture. So while their number is small from the point of view of complexity theory, it is large from the point of view of engineering. There is a variant of all this which performs a measurement on each qubit, and

[71] Exercise: If this explanation leaves you cold, give a better one. The best way to start may be to calculate explicitly what happens for all the eight basis states when $n = 3$.

then conditions the unitary that acts on the next qubit on the result of that measurement. But we decided at the outset to choose only one out of the many variants of architecture for quantum computers, so we do not go into this here.

There is a critical question to ask. When n is large we will need to implement phase gates that rotate their qubits through very small angles. This suggests that the quantum computer is subject to the same objection that one can raise against classical analog computers: the precision needed will grow with the complexity of the calculation in a way that nullifies any advantages it may have. This question was analysed by *Coppersmith*, who pointed an interesting moral. The conclusion is that small errors in the phases will cause the probabilities in equation (272) to deteriorate somewhat, but it will not affect the actual outcomes, which are discrete. Discrete quanta, if you like. Indeed, one can fix a sufficiently large integer k_0 and decide not to implement any R_k with $k > k_0$. So the surprising answer to the critical question is that not only is there no problem, we can in effect do the calculation with a number of gates that grows like n rather than like n^2. Ultimately it is the discreteness of the output from a quantum computer that saves the day.

Some classical post-processing

Now that we know how to take the quantum Fourier transforms it remains to extract the period r from the probabilities given in equation (272). The period is what we need to factor our integer.

The easy case is when the period r divides 2^n. For one thing, then we can set $\bar{n} = n$ in all the formulas above, so the size of the input register shrinks by one half. Recalling the definition of m from equation (268) we observe that we can set

$$m = \frac{2^n}{r} \ . \tag{285}$$

Now look at equation (272). We consider the expression

$$\sum_{j=0}^{m-1} (e^{\frac{2\pi i}{2^n}})^{jkr} = \sum_{j=0}^{m-1} (e^{\frac{2\pi ik}{m}})^j \ . \tag{286}$$

But we know that

$$\omega = e^{\frac{2\pi i}{m}} \;\Rightarrow\; \sum_{j=0}^{m-1} \omega^j = 0 \;\Rightarrow\; \sum_{j=0}^{m-1} \omega^{jk} = \begin{cases} m \text{ if } k \text{ is a multiple of m} \\ 0 \text{ otherwise .} \end{cases} \tag{287}$$

It follows that the probability p_k in equation (272) vanishes unless k is a multiple of m. We can afford to run the algorithm a few times, and determine the greatest common divisor m of the resulting outcomes k. Then equation (285) gives us the period r. Whatever the outcomes are, and even if N is large, the mathematics of the last step guarantees that with high probability we need only a few repetitions to determine r.

Let us do an example. Set $N = 15$ and choose $a = 7$, which is relatively prime to 15. In arithmetic modulo 15 we find

$$a = 7 \ , \ a^2 = 4 \ , \ a^3 = 13 \ , \ a^4 = 1 \ . \tag{288}$$

So the period $r = 4$. (If you want to do modular arithmetic in your head, think $a^3 \cdot a = 13 \cdot 7 = -2 \cdot 7 = -14 = 1$ modulo 15.) Even if we do not know the value of r, the machine does, in some sense. When we measure on the output register we might obtain the value $f_7(x) = 4$, in which case the input register is in the superposition

$$|\psi\rangle = |2\rangle + |6\rangle + |10\rangle + |14\rangle \ . \tag{289}$$

In fact $m = 4$, but this we do not know yet. The probability to obtain the kth out of the 16 outcomes is

$$p_k = \frac{1}{16}\frac{1}{4}\left|\sum_{j=0}^{3} \omega_{16}^{4jk}\right|^2 = \frac{1}{16}\frac{1}{4}\left|\sum_{j=0}^{3} \omega_4^{jk}\right|^2 = \begin{cases} \frac{1}{4} & \text{if} \quad k = 0, 4, 8, 12 \\ \\ 0 & \text{otherwise .} \end{cases} \tag{290}$$

So there are only four possible outcomes. Say that we obtain the outcome 8. We repeat the procedure, and obtain a different value, say 12. We compute the greatest common divisor $(8, 12) = 4$. Then we have determined the integer $16/r = 4$, so that we can calculate $r = 4$, and from there we can factorize 15.

When does the easy case occur? Recalling that the period also divides $(p-1)(q-1)$, we see that the prime factors of N must be of the form 2^x+1 for some integer x. This includes the *Fermat primes* $2^{2^x}+1$, of which the only known examples are $3, 5, 17, 257, 65537$. Reports that $15 = 3\cdot 5$ has been factored in the lab deal with the easy case.

The general case requires rather more analysis, and it is this that forces us to use $\bar{n} = 2n$ qubits for the input register. Although $2^{\bar{n}}/r$ is no longer an integer there will be constructive interference in equation (272) for values of k such that

$$k = c\frac{2^{\bar{n}}}{r} + \epsilon \quad \Leftrightarrow \quad \frac{k}{2^{\bar{n}}} = \frac{c}{r} + \frac{\epsilon}{2^{\bar{n}}} \ , \tag{291}$$

where c is an integer and ϵ is small. The amplitude that occurs in equation (272) becomes

$$p_k = \frac{1}{2^{\bar{n}}m}\left|\sum_{j=0}^{m-1} e^{\frac{2\pi i}{2^{\bar{n}}}jkr}\right|^2 = \frac{1}{2^{\bar{n}}m}\left|\sum_{j=0}^{m-1}\omega^{\epsilon jr}\right|^2 \ . \tag{292}$$

The peak is surprisingly sharp.[72] When we have observed the kth outcome we know the rational number $k/2^{\bar{n}}$, and going back to equation (291) we also know that this rational number can be approximated with a rational number having a much smaller denominator (namely $r < 2^n < 2^{\bar{n}}$). As it happens there is a branch of number theory that uses *continued fractions* to find approximations of real numbers with rational numbers of small denominators. This is a useful procedure in many contexts where one wants to compare two incommensurable periods, say when one computes the date of Easter, and it is necessary in order to make Shor's algorithm work in the general case. But I do not go through it here. I just remark that, provided the input register contains $2^{\bar{n}}$ qubits, a multiple of the period r can be found, efficiently and uniquely, using continued fractions. In the end the conclusion is the same as in the easy case: if the Fourier transformation can be done in polynomial time then the probability that we will be done in polynomial time can be made as high as we please. And an interesting point emerges, which is that the analysis succeeds in identifying r precisely because the set of possible

[72] Exercise: For $N = 21$ and $f(x) = 2^x$ modulo 21, use a (classical) computer to plot the probabilities p_k that come out of Shor's algorithm.

measurement outcomes is discrete, or if you like because in some ways the quantum computer is more digital than analog.

Other algorithms

The period finding core of *Shor*'s algorithm can be used to speed up the solution of many other interesting problems that hinge on the structure of commutative groups. It can for instance be used to find principal ideals and unit groups in algebraic number theory. And it can be used to calculate *discrete logarithms* in polynomial time, hence to break the widely used cryptosystem due to *Diffie* and *Hellman* (and again to the British secret service). The discrete logarithm is another example of a *one way function*, that is to say a function that is easy to compute but hard to invert. We again do arithmetic modulo some (large) integer N. If a and x are given integers it is easy to calculate the integer a^x, but if a and a^x are given it is hard to calculate x. The Diffie–Hellman scheme is a clever application of this fact. The integer a is the message. Alice and Bob secretly choose two integers x and y that are invertible modulo N. Alice sends the integer a^x to Bob, Bob calculates $(a^x)^y = a^{xy}$ and sends it back to Alice, and Alice sends $(a^{xy})^{x^{-1}} = a^y$ back to Bob, who can then read the message by applying his secret key y^{-1} to it. It happens that the inverse of an integer modulo N can be calculated using the Euclidean algorithm, hence in polynomial time, so Alice and Bob can do their calculations quickly. But as far as we know, if N is large the eavesdropper can read the message only if she has a quantum computer available.[73]

Still there are some public key cryptosystems that remain safe, and it should be remembered that the rapid development of classical computers happened because it was possible to make money out of each improvement. It is difficult to see anyone making money out of unit groups in algebraic number theory. At the moment it seems that the most likely practical applications of quantum computing lie in the direction of letting one quantum system simulate another, as originally suggested by *Feynman*. But the whole subject is moving: there are small-scale quantum computers with public interfaces on the internet.

[73]Exercise: Why does the eavesdropper need to compute a discrete logarithm to read the message?

Quantum error correction

A classical computer can easily perform Avogadro's number of operations without committing a single bit error. Its electronic switches are large on the scale of the thermal fluctuations, oscillations are quickly damped out, and whatever happens the bits remain unentangled with the environment. Quantum gates are not that reliable, and a quantum computer able to factorize a cryptographically interesting prime would need something like 10^9 gates. Then quantum error correction becomes essential. For several reasons it used to be thought that quantum error correction is impossible, but *Shor* and *Steane* surprised the world by showing that it is not.

The naive idea for error correction is to make sure that every qubit comes in triplicate. This founders on the fact that we cannot copy an unknown quantum state. A first attempt around this problem might be to use two ancillas and store the state $z_0|0\rangle + z_1|1\rangle$ as a three-qubit state,

$$|0\rangle|0\rangle(z_0|0\rangle + z_1|1\rangle) \to z_0|000\rangle + z_1|111\rangle \ . \tag{293}$$

This violates no rules, and is indeed easily achieved by means of two CNOT gates. We assume that at most one qubit at a time is affected by noise, so an error to be corrected for could be the 'bit-flip'

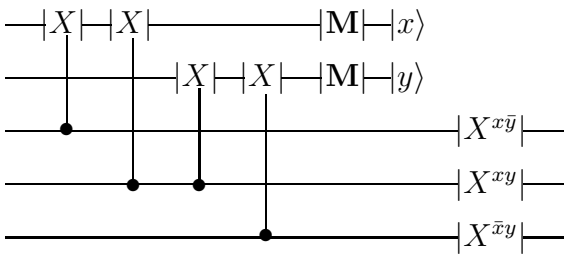
$$z_0|000\rangle + z_1|111\rangle \to z_0|010\rangle + z_1|101\rangle \ . \tag{294}$$

Now we run into the second problem. We cannot inspect a quantum state without changing it in an irreversible way. If we measure any of the qubits in the computational basis, the state collapses to either $|010\rangle$ or to $|101\rangle$. Then we know that an error occurred, but we cannot restore the original three-qubit state because all information about the amplitudes z_0 and z_1 has been lost. Indeed the problem is worse, because there may be a 'phase-flip' error

$$z_0|000\rangle + z_1|111\rangle \to z_0|000\rangle - z_1|111\rangle \ . \tag{295}$$

We would not even notice this if we measure in the computational basis. Still worse, in many ways the quantum computer behaves like an analog computer, so the errors are not discrete. There may be a small amplitude for an error, which then builds up during the computation.

Let us focus on bit flip errors to begin with. We are going to correct for single bit flips affecting one qubit only, without looking at the state to be transmitted. The key observation is that the uncorrupted state $z_0|000\rangle + z_1|111\rangle$ belongs to a two dimensional *code subspace*. A single error transforms the state so that it sits in one out of three mutually orthogonal two dimensional subspaces, all of them orthogonal to the code subspace. This desirable situation occurs because the state to be transmitted belongs to a 2^3 dimensional Hilbert space. To do the correction we introduce two additional ancilla qubits set to $|0\rangle$ initially, and on which measurements $\mathbf{M}$ will be performed. We will apply gates to the interesting qubits conditional on the outcome of those measurements. The circuit diagram is



In the final round we apply gates such as $X^{x\bar{y}}$, where as usual $\bar{y} = y + 1$ in binary arithmetic and y is the outcome of the measurement on one of the two ancillary qubits. You can easily check that the output is the desired—and still unknown—state $z_0|000\rangle + z_1|111\rangle$, also if the input is a state in which one of the qubits has been corrupted by a bitflip, such as $z_0|001\rangle + z_1|110\rangle$.

Of course this is only a partial success, because we still have to deal with phase flips, and the various kinds of continuous drifts that can occur. In fact the case we dealt with is a rather harmless one, in which the error is some unwanted unitary transformation of a qubit. The three qubit state stays pure. But in a system that is open to an environment the state can evolve in many ways that do not preserve this property.

It helps to look at this a little more abstractly. Suppose that the state we want to protect is encoded in an n-qubit state $|\Psi\rangle$, and that the relevant rest of the world starts out in some reference state $|0\rangle$. The state is corrupted by some unitary transformation acting on the whole Hilbert space. We can 'discretize' this by means of a unitary operator basis $\{U_I\}$ for unitary operators acting on the state we want to protect, so that the state transforms

according to

$$|\Psi\rangle|0\rangle_R \;\rightarrow\; \sum_I U_I|\Psi\rangle|\psi_I\rangle_R \;. \tag{296}$$

This is completely general because we assume nothing whatsoever about the reservoir states $|\psi_I\rangle$. They are neither orthogonal nor normalized. Thus the 'discretization' is kind of a fake at this point. Nevertheless the unitary operator basis will soon earn its alternative name "error basis".

To proceed we need to assume something about the noise, and something about the state $|\Psi\rangle$ that we are trying to protect. We need to ensure that

$$\mathrm{Tr}|\Psi\rangle\langle\Psi|U_I^\dagger U_J = \delta_{IJ} \;. \tag{297}$$

If this can be arranged the error basis gives rise to a set of mutually exclusive alternatives, and a measurement can be devised so that the state collapses according to

$$\sum_I U_I|\Psi\rangle|\psi_I\rangle_R \;\rightarrow\; U_I|\Psi\rangle|\psi_I\rangle_R \;. \tag{298}$$

Once we know the outcome we can apply the appropriate operator $U_I^\dagger$ to the state. The error is corrected, and never mind the reservoir state.

Concerning the noise, we assume that it acts on each qubit separately, and moreover that it does not affect more than w qubits. Thus we assume that we do not need the full unitary operator basis, but only elements of the form

$$U_I = E_I^{(1)} \otimes E_I^{(2)} \otimes \ldots \otimes E_I^{(n)} \;, \tag{299}$$

where, for each I, at most w of the unitary operators $E_I^{(i)}$ differ from the identity. Most, but not all, people who worked on this agree that this is a physically reasonable assumption.

Now we look at (297) with new eyes. The equality would hold if $|\Psi\rangle\langle\Psi|$ was replaced by the maximally mixed state. But now we have arranged that, in any term of the trace, at most $2w$ of the factors contain non-trivial error operators. We can begin by taking the partial trace of $|\Psi\rangle\langle\Psi|$ over the remaining $n-2w$ factors (those that have not been affected by the noise). It is enough if this partial trace is the maximally mixed state in the $2w$-partite Hilbert space that is affected by the noise.

We now specialize to the case $n = 5$ and $w = 1$, that is we aim to correct single qubit errors only. Consider the following interesting state, in which every computational basis state with an even number of 1s has been included,

$$|v_0\rangle = |00000\rangle + |11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle -$$

$$-|10010\rangle - |10100\rangle - |01001\rangle - |01010\rangle - |00101\rangle - \quad (300)$$

$$-|11110\rangle - |11101\rangle - |11011\rangle - |10100\rangle - |01111\rangle \ .$$

It clearly has a lot of structure. (It also has a misprint, which serves to make Problem 5 below more realistic.) This structure is actually coming from a discrete Heisenberg group, and this is also the way to give a more compact description.[74] There is a corresponding orthogonal state $|v_1\rangle$, obtained by switching the 0s and the 1s in $|v_0\rangle$. Together they span a two dimensional code subspace, consisting of the states

$$|\Psi\rangle = z_0|v_0\rangle + z_1|v_1\rangle \ . \quad (301)$$

You can now check that if we take the partial trace over any three out of the five factors, there holds

$$\mathrm{Tr}_{123}|v_0\rangle\langle v_0| = \mathrm{Tr}_{123}|v_1\rangle\langle v_1| = \mathbf{1}_{45} \ , \ \mathrm{Tr}_{123}|v_0\rangle\langle v_1| = \mathrm{Tr}_{123}|v_1\rangle\langle v_0| = 0 \ . \quad (302)$$

I am being cavalier about normalisation factors here, and I singled out the first three factors as an example only. The calculation is most conveniently done by first calculating the eight scalar products $\langle abc|v_0\rangle$, where a, b, c are integers modulo 2. The scalar products $\langle abc|v_1\rangle$ are obtained by switching 0 and 1, and then you can do the sum that defines the trace. Given this result it follows that, for any state in the code subspace and regardless of which three factors you trace out,

$$\mathrm{Tr}_{123}|\Psi\rangle\langle\Psi| = |z_0|^2\mathrm{Tr}_{123}|v_0\rangle\langle v_0| + |z_1|^2\mathrm{Tr}_{123}|v_1\rangle\langle v_1| = \mathbf{1}_{45} \ . \quad (303)$$

[74] Exercise: Using the notation X, Y, Z, for the Pauli matrices, and a compact notation for tensor products, show that the state is an eigenstate of the five commuting operators $XXZ\mathbf{1}Z$, $ZXXZ\mathbf{1}$, $\mathbf{1}ZXXZ$, $Z\mathbf{1}ZXX$, $ZZZZZ$.

Given that at most one error occurs, this is all that is needed for eq. (297) to hold. We can code a *logical* qubit as a state in this code subspace, and we are assured that any single qubit error can be detected and corrected.

This is a promising start for the subject of quantum error correction. It is also where these notes end, and I am afraid that they have exceeded the hundred pages that I tried to limit them to.

Problem 5: Verify in complete detail my claim that the state (301) obeys equation (297) if at most one error occurs. (Remember to correct the misprint.)