Quantum Information

Jacopo Tissino

July 2019

Contents

1 The basics

Qubit It can be physically realized with any two-state system. It is a complex superposition of $|0\rangle$ and $|1\rangle$. Thanks to normalization and $U(1)$ gauge invariance (a ket is defined up to a phase) we can always make $|0\rangle$'s coefficient real and $\in [0, 1]$: the ket can always be written as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\varphi}|1\rangle \tag{1.1}$$

with $\varphi \in [0, 2\pi]$ and $\theta \in [0, \pi]$: these can be interpreted as angles on a sphere. The fact that θ is divided by two comes from the coordinates we choose in $S^3 \subset \mathbb{C}^2$.

We can use an n-qubit system:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle \tag{1.2}$$

where $|i\rangle$ is a base state of the tensor product space of the n Hilbert spaces: $|i\rangle = |\alpha_0\rangle_0 \otimes |\alpha_1\rangle_1 \otimes \dots |\alpha_{n-1}\rangle_{n-1}$; the α_j are the components of the representation of i in binary: $\alpha_0\alpha_1 \dots \alpha_{n-1}$ (with $\alpha_j = 0, 1$). This is called the *computational basis*.

We assume the state to be normalized: $\sum_i |a_i|^2 = 1$

Entanglement A state $|\psi\rangle$ is called *entangled* if there are no subsystem kets $|\psi_i\rangle_i$, $i = A, B$ such that $|\psi\rangle = |\psi_A\rangle_A \otimes |\psi_B\rangle_B$.

2 Quantum gates

They are unitary trasformations: $U : \mathcal{H} \to \mathcal{H}$, $U^\dagger U = UU^\dagger = \mathbb{1}$.

They can be decomposed into smaller gates, which are in general $2n \times 2n$ complex unitary matrices, but we will usually just use $n = 1, 2$.

If two gates are represented by 2×2 matrices, indexed in the computational basis as A_i^j and B_k^l with $i, j, k, l = 0, 1$, then their tensor product will be

$$[A_i^j B_k^l] = [A \otimes B]_{i\,k}^{j\,l} = [A \otimes B]_M^N \tag{2.1}$$

where we grouped the indices $ik = M$ and $jl = N$, in order to write two-component fourth order tensors as four-dimensional order two matrices. What are M and N then? i, j and so on are binary digits, so it is natural to interpret M and N as numbers between 0 and 3 written in binary. Of course, this can be generalized to any order, keeping the same pattern, and be applied to vectors as well.

Hadamard It is a *one-qubit gate* which switches from the computational basis to the eigenstates of σ_z, which we call $|+\rangle = H|0\rangle \propto |0\rangle + |1\rangle$ and $|-\rangle = H|1\rangle \propto |0\rangle - |1\rangle$.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.2}$$

We can also express it, for the basis states, as $H|x\rangle = \sqrt{1/2}\sum_{y=0}^{1}(-)^{xy}|y\rangle$.

Phase It is a *one-qubit gate* which gives a phase to a state: applying it to a generic qubit, written as (1.1), we get $R_z(\delta)|\psi\rangle = \cos(\theta/2)|0\rangle + \exp\big(i(\varphi + \delta)\big)\sin(\theta/2)|1\rangle$.

$$R_z(\delta) = \exp(i\delta\sigma_z) = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\delta) \end{bmatrix} \tag{2.3}$$

Control not It is a *two-qubit gate* which cannot be written as a tensor product of one-qubit gates.

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix} \tag{2.4}$$

It generates entanglement: let us apply it to the separable state $\alpha\left|00\right\rangle + \beta\left|10\right\rangle$: it returns $\alpha\left|00\right\rangle + \beta\left|11\right\rangle$, which is entangled.

Control phase It is a *two-qubit gate*:

$$\mathrm{CPHASE}(\delta) = \begin{bmatrix} \mathbb{1} & 0 \\ 0 & R_z(\delta) \end{bmatrix} \tag{2.5}$$

where we used the phase gate (2.3).

It can be written as $\mathrm{CPHASE}(\delta) = [\mathbb{1} \otimes R_z(\delta/2)][\mathrm{CNOT}][\mathbb{1} \otimes R_z(-\delta/2)][\mathrm{CNOT}][R_z(\delta/2) \otimes \mathbb{1}]$: the steps (multiplying from right to left, starting from just $[R_z(\delta/2) \otimes \mathbb{1}]$) are as follows:

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & e^{i\delta/2} & \\ & & & e^{i\delta/2} \end{bmatrix} \to \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & e^{i\delta/2} \\ & & e^{i\delta/2} & \end{bmatrix} \to \begin{bmatrix} 1 & & & \\ & e^{-i\delta/2} & & \\ & & & e^{i\delta/2} \\ & & 1 & \end{bmatrix} \to$$
$$\to \begin{bmatrix} 1 & & & \\ & e^{-i\delta/2} & & \\ & & 1 & \\ & & & e^{i\delta/2} \end{bmatrix} \to \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{i\delta} \end{bmatrix} \tag{2.6}$$

We can get any state $\left|\psi\right\rangle$ written as (1.1) with Hadamard and phase-shift:

$$\begin{aligned} \left|\psi\right\rangle &= R_z(\pi/2+\varphi) H R_z(\theta) H \left|0\right\rangle && \text{(2.7a)} \\ &= \frac{1}{2}\begin{bmatrix} 1+e^{i\theta} \\ i\left(e^{i\varphi} - e^{i(\theta+\varphi)}\right) \end{bmatrix} && \text{(2.7b)} \\ &= \frac{1}{2}\begin{bmatrix} e^{i\theta/2}+e^{-i\theta/2} \\ i^{-1}\left(e^{i\theta/2} - e^{-i\theta/2}\right)e^{i\varphi} \end{bmatrix} && \text{(2.7c)} \\ &= \begin{bmatrix} \cos(\theta/2) \\ \sin(\theta/2)e^{i\varphi} \end{bmatrix} && \text{(2.7d)} \end{aligned}$$

where in the step (2.7c) we used the fact that a quantum state is only defined up to a phase, and multiplied by $\exp(-i\theta/2)$.

Binary function unitarity In general a function $f : \{0,1\}^n \to \{0,1\}$ will not be injective, therefore it will not be unitary. In order to represent it as unitary we must "carry over" the input:

$$U_f \left|x\right\rangle \left|0\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle \tag{2.8}$$

in order to have a more general trasformation we define it for arbitrary input on the second system:

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle \tag{2.9}$$

where $\oplus$ is bitwise XOR.

Parallelism We can do lots of computation with a single gate: say we have a state like (1.2), then

$$U_f \sum_{x=0}^{2^n-1} a_x \left|x\right\rangle \left|y\right\rangle = \sum_{x=0}^{2^n-1} a_x \left|x\right\rangle \left|y \oplus f(x)\right\rangle \tag{2.10}$$

For this to be really different from classical computing, however, a significant portion of the 2^n coefficients a_x must be nonzero. We now will show how to produce the state in which they are all equal to $2^{-n/2}$, assuming we can produce $\left|0\right\rangle^{\otimes n}$. We apply a Hadamard gate to every qubit, which carries a normalization and a factor of $(-)^{x_i y_i}$, so we get:

$$H^{\otimes n} \left|x\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-)^{x\cdot y} \left|y\right\rangle \tag{2.11}$$

And the desired state can be found by setting $x = 0$. Do note that while this looks "entangled" we found it by applyng single-qubit gates: it is still separable (we can see this from the fact that its density matrix has the same value in every entry, so its rank is 1).

No cloning A *general* cloning unitary operator would look like: $U \left|x\right\rangle \left|0\right\rangle = \left|x\right\rangle \left|x\right\rangle$. Let us assume we have one, and let us apply it to two different states: $A = U \left|\psi\right\rangle \left|0\right\rangle = \left|\psi\right\rangle \left|\psi\right\rangle$ and $B = U \left|\varphi\right\rangle \left|0\right\rangle = \left|\varphi\right\rangle \left|\varphi\right\rangle$. Now, let us compute the scalar product of A and B:

$$A \cdot B = \left\langle\psi\right| \left\langle 0\right| U^\dagger U \left|\varphi\right\rangle \left|0\right\rangle \tag{2.12a}$$

$$= \left\langle\psi|\varphi\right\rangle \left\langle 0|0\right\rangle U^\dagger U \tag{2.12b}$$

$$= \left\langle\psi|\varphi\right\rangle \tag{2.12c}$$

but also

$$A \cdot B = \left\langle\psi\right| \left\langle\psi\right| \left|\varphi\right\rangle \left|\varphi\right\rangle \tag{2.13a}$$

$$= \left\langle\psi|\varphi\right\rangle^2 \tag{2.13b}$$

and in general $\left\langle\psi|\varphi\right\rangle \neq 0, \pm 1$, so we found a contradiction. Note that we *can* create a partial cloning machine which works only on the basis states of some basis: we extend by linearity the desired cloning. If we want to clone the computational basis, the gate is the CNOT (see 'Control not' on page 5).

Alternative proof: apply $U(\left|x\right\rangle + \left|y\right\rangle) \otimes \left|0\right\rangle = (\left|x\right\rangle + \left|y\right\rangle)^{\otimes 2}$ (a separable state), but U must be linear, so $U(\left|x\right\rangle + \left|y\right\rangle) \otimes \left|0\right\rangle = \left|x\right\rangle \left|x\right\rangle + \left|y\right\rangle \left|y\right\rangle$, generally an entangled state.

3 Algorithmic complexity

We can distinguish algorithms by how many resources (computation time, RAM, ...) they require:

1. P: classical polynomial time;
2. NP: classical nondeterministic polynomial time: there exists a nondeterministic Turing machine[1] which finds the solution in polynomial time — the solution can thus be verified in polynomial time;
3. $NP-$hard: problems to which every P problem can be reduced in polynomial time;
4. NPC: NP problems which are also $NP-$hard;
5. BPP: bounded error probabilistic polynomial: it can give us the correct answer in polynomial time with probability $\mathbb{P} > 1/2$.

[1] Same as a regular Turing machine, except that in a certain configuration it can have different actions, and in a certain sense it "tries them all".

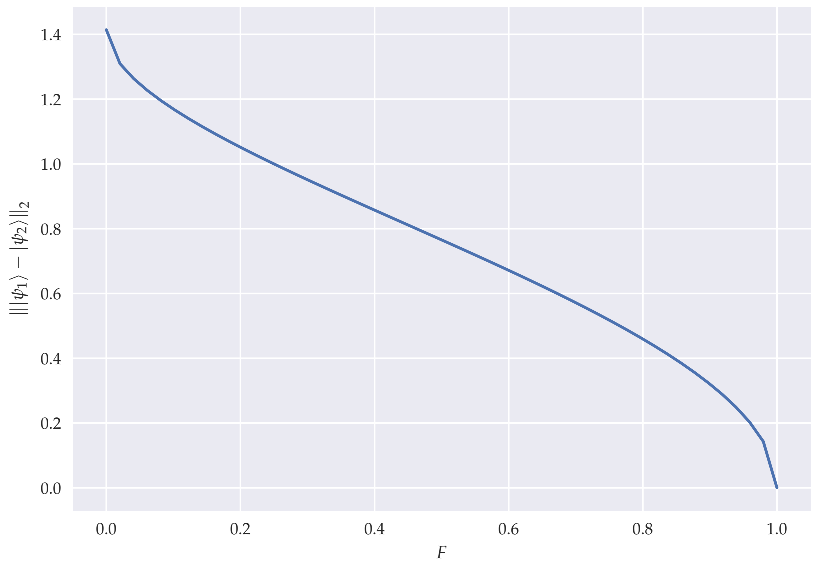

Figure 1: Norm of difference vs fidelity: a plot of equation (4.2)

6. BQP: bounded error quantum polynomial: it is a quantum algorithm which can give us the correct answer in polynomial time with probability $\mathbb{P} > 1/2$.

Surely $P \subseteq BPP \subseteq BQP$. We are not sure whether $BQP \subseteq BPP$.

4 Fidelity

We introduce a notion of distance between states:

$$F = \left|\langle \psi_1 | \psi_2 \rangle\right|^2 \tag{4.1}$$

F is monotonous in $\left\| |\psi_1\rangle - |\psi_2\rangle \right\|_2$. F is also the $\cos^2(\theta/2)$, where θ is the angle between the two vectors in Bloch space.

Let us prove these statements: first of all notice that $\left\| |\psi_1\rangle - |\psi_2\rangle \right\|_2 = \sqrt{2 - 2\,\mathrm{Re}\,\langle \psi_1 | \psi_2 \rangle}$. Now, the scalar product $\langle \psi_1 | \psi_2 \rangle$ is in general a complex number but we can rotate the starting functions by an arbitrary phase, making it real and positive. So we get $\mathrm{Re}\,\langle \psi_1 | \psi_2 \rangle = \left|\langle \psi_1 | \psi_2 \rangle\right| = \sqrt{F}$. Then, we can see that

$$\left\| |\psi_1\rangle - |\psi_2\rangle \right\|_2 = \sqrt{2(1 - \sqrt{F})} \tag{4.2}$$

Now, we want to prove $F = \cos^2(\theta/2)$: let U be a unitary transformation which maps $|\psi_1\rangle$ to $|0\rangle$. We can rewrite $F = \left|\langle \psi_1 | U^\dagger U |\psi_2\rangle\right|^2$. We can expand the applications of U to the vectors to get $\left|\langle 0| \left(\alpha |0\rangle + \beta |1\rangle\right)\right|^2$.

Now, since states are always defined up to a phase, we can pick α to be real and positive. Then we have put the state $U|\psi_1\rangle$ in the canonical form (1.1), and the result follows.

5 Quantum teleportation

It is possible to clone a generic quantum state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ assuming we start with two entangled qubits, one in the starting location and one at the destination: so, if these two qubits are called A and B and the state we want to transmit is in subsystem C, we start with

$$\boxed{\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)_{AB} \otimes \left(\alpha\,|0\rangle + \beta\,|1\rangle\right)_C} \tag{5.1}$$

The protocol is this:

1. Apply the gate $\mathrm{C}_C\mathrm{NOT}_A$;
2. apply the gate H_C;
3. measure A and C in the computational basis: call the result x;
4. apply a gate V_x, selected according to table 1, to B.

x	V_x
00	$\mathbb{1}$
01	σ_z
10	σ_x
11	$\sigma_z\sigma_x$

Table 1: Possibilities for gate V_x.

We can realize all of this with the gates CNOT, Hadamard and σ_z (we can recover σ_x as $\sigma_x = H\sigma_z H$.

6 Quantum interferometry

Beam splitter We call the sides of the BS A and B, and denote the absence or presence of light on either side by $|0,1\rangle_{A,B}$. Then the action of the beam splitter is unitary and can be represented in the partial basis $|0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B$ as

$$U_{BS} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{6.1}$$

Note that $U_{BS}^2 = i\sigma_x$ in the BS-side basis: if we build a Mach-Zender interferometer, that is, we chain two beam-splitters, the light from the two paths interferes and we get some only on one side of the BS (the side opposite of the starting one).

Bomb detection If we block one of the paths between the detectors, around half of the time the light will hit this obstacle (our 'bomb'). Around half the time it will go to the second BS, and then a quarter of the time it will be detected on either side of the BS. On the other hand, if there is no obstacle, we will see photons *only* on a certain side of the final BS.

So around 1/4 of the time we will have detected the bomb without the photon actually *having been there*.

7 Zeno effect

We will work with $\hbar = 1$. We look of the *survival probability* with which we will retain our starting state: if our evolution operator is $U = \exp(-iHt)$, this probability is $\mathbb{P} = A^* A$, where $A = \langle\psi_0|\psi(t)\rangle$ and $|\psi(t)\rangle = U\,|\psi_0\rangle$.

How does this probability look like for small t? We can expand, for a small δt:

$$U \sim \mathbb{1} - iH\delta t - H^2\delta t^2 \tag{7.1}$$

then we will have

$$A = \langle\psi_0|\left(\mathbb{1} - iH\delta t - H^2\delta t^2\right)|\psi_0\rangle = 1 - i\,\langle H\rangle_0\,\delta t - \frac{1}{2}\left\langle H^2\right\rangle_0 \delta t^2 \tag{7.2}$$

so we can calculate $\mathbb{P}$:

$$\mathbb{P} = \left| 1 - i \left\langle H \right\rangle_0 \delta t - \frac{1}{2} \left\langle H^2 \right\rangle_0 \delta t^2 \right|^2 = 1 - \delta t^2 \left(\left\langle H^2 \right\rangle_0 - \left\langle H \right\rangle_0^2 \right) \tag{7.3}$$

Equation (7.3) is accurate to the order δt^3, since we only ignored a fourth order term. The term multiplying δt^2 can be interpreted as the inverse of a characteristic time:

$$\tau = \frac{1}{\sqrt{\left\langle H^2 \right\rangle_0 - \left\langle H \right\rangle_0^2}} = \frac{1}{\Delta H_0} \tag{7.4}$$

Repeated measurements If we measure some observable with $\left|\psi_0\right\rangle$ as an eigenspace, a fraction t^2/τ^2 of the time we will get something different from $\left|\psi_0\right\rangle$.

So, if in a long time t we measured N times, the probability of the system having remained in the original state is at least $\mathbb{P}(t) \geq \mathbb{P}^N(t/N)$: we consider the case in which the system remained in the state for *all* the measurements. The latter pertains to a small time so we can apply equation (7.3):

$$\mathbb{P} \geq \mathbb{P}^N \left(\frac{t}{N} \right) = \left(1 - \frac{t^2}{N^2 \tau^2} \right)^N \tag{7.5}$$

if we fix the inverse of the measurement rate $N/t = R$ this becomes $\mathbb{P} \geq x^t = \exp\big(t \log x\big)$, with $x = (1 - 1/R^2\tau^2)^R$, so $\log x = R \log(1 - 1/R^2\tau^2) < 0$. So, we call $-\log x = \gamma_{\text{eff}} > 0$: then

$$\boxed{\mathbb{P} \geq e^{-\gamma_{\text{eff}} t}} \tag{7.6}$$

Note that as $R \to \infty$, $\gamma_{\text{eff}} \sim R^{-1} \tau^{-2}$.

An example of nonunitary evolution We consider a Hamiltonian like $H = \Omega \sigma_x$, which might be that of a spin-1/2 particle, polarized along z, in a magnetic field along x. Say our system starts at $\left|\psi_0\right\rangle = \left|0\right\rangle$. Then the evolution looks like

$$\exp(-iHt) \left|0\right\rangle = \cos(\Omega t) \left|0\right\rangle - i \sin(\Omega t) \left|1\right\rangle \tag{7.7}$$

We can calculate the quantities from section 7: $A = \cos(\Omega t)$ and $\mathbb{P} = \cos^2(\Omega t)$, for small t: $\mathbb{P} \sim 1 - \Omega^2 t^2$. We recognise the expression for the Zeno time: in this case $\tau = \Omega^{-1}$

Let us introduce the nonunitary part: we change H to

$$H_{\text{int}} = \begin{bmatrix} -iV \\ \Omega \\ 0 \\ +iV \end{bmatrix} \cdot \begin{bmatrix} \mathbb{1} \\ \sigma_x \\ \sigma_y \\ \sigma_z \end{bmatrix} = -iV\mathbb{1} + \vec{h} \cdot \vec{\sigma} = \begin{bmatrix} 0 & \Omega \\ \Omega & -2iV \end{bmatrix} \tag{7.8}$$

to represent interaction with a second lower-energy system, to which our first one can decay *if it is in the state* $\left|1\right\rangle$. Can we get a Zeno-like effect with this kind of interaction, and without *measuring* anything? The evolution of this new Hamiltonian will look like

$$\exp(-itH) = e^{-tV} \exp\left(-it\vec{h} \cdot \vec{\sigma}\right) = e^{-tV} \left(\cosh(ht)\mathbb{1} - i \frac{\vec{\sigma} \cdot \vec{h}}{h} \sinh(ht) \right) \tag{7.9}$$

where $h = -i\left\|\vec{h}\right\| = \sqrt{V^2 - \Omega^2} \in \mathbb{R}$, since we assume the coupling is strong ($V \gg \Omega$).

This comes from the fact that for a unit vector $\vec{n}$: $(\vec{n} \cdot \vec{\sigma})^n = \mathbb{1}$) if N is odd, $\vec{n} \cdot \vec{\sigma}$ otherwise: thus we can show that

$$\exp\big(i\theta(\hat{n} \cdot \sigma)\big) = \cos(\theta)\mathbb{1} + i(\hat{n} \cdot \sigma) \sin(\theta) \tag{7.10}$$

So, we can compute $A = \left\langle U \right\rangle_0$, using the fact that σ_z is the only one of the Pauli matrices with a nonzero expectation value on $\left|0\right\rangle$:

$$A = \frac{1}{2}\left(1+\frac{V}{h}\right)e^{-(V-h)t} + \frac{1}{2}\left(1-\frac{V}{h}\right)e^{-(V+h)t} \tag{7.11}$$

V is close to h but slightly larger, so both the exponentials' arguments are negative.

For large times we can discard the quickly-decaying second exponential, and be left with

$$\mathbb{P} = \left|\frac{1}{2}\left(1+\frac{V}{h}\right)e^{-(V-h)t}\right|^2 \sim \left(1+\frac{\Omega^2}{2V^2}\right)\exp\left(-t\frac{\Omega^2}{V}\right) \tag{7.12}$$

So, weird normalizations for small times aside, $\gamma_{\text{eff}} = \Omega^2/V$, but $\Omega = \tau^{-1}$, so $V = R$, the 'rate of observation': the stronger the coupling, the more the other system influences ours.

8 Non-unitary evolution

It happens when the particle can escape the system; for example in optical systems there can be a complex index of refraction. The Hamiltonian will look like

$$H = H_0 - iV\mathbb{1} \tag{8.1}$$

where $V \in \mathbb{R}^+$. The unitary evolution has an i multiplying the Hamiltonian, so we get a decreasing real exponential.

We will have $A \sim 1 - V\delta t + O(\delta t^2)$, so $\mathbb{P} \sim 1 - 2V\delta t + O(\delta t^2)$: the first derivative is nonzero!

An example of a nonhermitian Hamiltonian We consider a system and its environment together:

$$H = \underbrace{\Omega\sigma_x}_{\text{system}} + \underbrace{\int d\omega\, |\omega\rangle\langle\omega|}_{\text{environment}} + \underbrace{\sqrt{\frac{\Gamma}{2\pi}}\int d\omega\, (|+\rangle\langle\omega| + |\omega\rangle\langle+|)}_{\text{interaction}} \tag{8.2}$$

Where σ_x is meant to be in the $|-\rangle, |+\rangle$ basis. Now, let us take a generic state $|\psi\rangle = x(t)|-\rangle + y(t)|+\rangle + \int d\omega\, z(\omega,t)|\omega\rangle$.

We will write the Schrödinger equation for the evolution of x, y and z and show that, if we just consider the first two, the effective Hamiltonian looks like the one in (7.8).

The system so solve can be separated into

$$i\dot{x} = \Omega y \tag{8.3a}$$

$$i\dot{y} = \Omega x + \sqrt{\frac{\Gamma}{2\pi}}\int z\, d\omega \tag{8.3b}$$

$$i\dot{z} = \omega z + \sqrt{\frac{\Gamma}{2\pi}}y \tag{8.3c}$$

In can be readily verified that, with starting conditions $x = 1$, $y = z = 0$, we have

$$z(\omega,t) = -i\sqrt{\frac{\Gamma}{2\pi}}\int_0^t d\tau\, y(\tau)e^{-i\omega(t-\tau)} \tag{8.4}$$

so we substitute into the equation for y

$$i\dot{y} = \Omega x - i\frac{\Gamma}{2\pi}\int d\omega \int_0^t d\tau\, y(\tau)e^{-i\omega(t-\tau)} \tag{8.5}$$

but $\int d\omega\, e^{-i\omega(t-\tau)} = 2\pi\delta(t-\tau)$: so

$$i\dot{y} = \Omega x - i\Gamma y(t)/2 \tag{8.6}$$

The factor $1/2$ comes from the fact we integrated a δ on the *boundary* of the domain. We can combine the results into

$$i\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 & \Omega \\ \Omega & -i\Gamma/2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \tag{8.7}$$

9 Implementation of quantum gates

9.1 NOT gate

We want to implement a NOT gate (σ_x): we use a spin-1/2 particle, and two magnetic fields described by a Hamiltonian

$$H = -\mu\Big(B_0\sigma_z + B_1\Big(\cos(\omega t)\sigma_x + \sin(\omega t)\sigma_y\Big)\Big) \tag{9.1}$$

So the zeroth field is fixed on z, while the other rotates around the z axis staying on the xy plane.

Let us write the time-dependent Schrödinger equation for a state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, applying the Euler identity to the sines and cosines:

$$i\hbar\frac{\partial}{\partial t}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = -\mu\begin{bmatrix} B_0 & B_1 e^{-i\omega t} \\ B_1 e^{i\omega t} & -B_0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{9.2}$$

we can rewrite this introducing the characteristic angular velocities of the two magnetic fields:

$$\omega_0 = -\frac{2\mu B_0}{\hbar} \qquad \text{and} \qquad \omega_1 = -\frac{2\mu B_1}{\hbar} \tag{9.3}$$

where we arbitrarily introduced a factor of 2 to make calculations simpler later.

$$i\frac{\partial}{\partial t}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{\omega_0}{2}\alpha + \frac{\omega_1}{2}e^{-i\omega t}\beta \\ \frac{\omega_1}{2}e^{i\omega t}\alpha - \frac{\omega_0}{2}\beta \end{bmatrix} \tag{9.4}$$

Now, we want to simplify the ω exponentials: so, we use the rotation matrix $R_z(\omega t)$ (expressed with a global phase to simplify calculations) to change variables into

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} e^{i\omega t/2} & 0 \\ 0 & e^{-i\omega t/2} \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{9.5}$$

This is a spin rotation matrix: we go from the eigenstates of σ_z to those of a spin operator aligned with the vector $(B_1\cos(\omega t), B_1\sin(\omega t), B_0)$. We also need to express the derivatives of α and β, since this is a time-dependent change of variables it will be non-trivial.

$$\frac{\partial}{\partial t}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} e^{-i\omega t/2} & 0 \\ 0 & e^{i\omega t/2} \end{bmatrix}\frac{\partial}{\partial t}\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} (-i\omega/2)e^{-i\omega t/2} & 0 \\ 0 & (+i\omega/2)e^{i\omega t/2} \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} \tag{9.6}$$

If we substitute this in, bringing all the terms without time derivatives on the right hand side, we get:

$$i\begin{bmatrix} e^{-i\omega t/2}\dot{a} \\ e^{i\omega t/2}\dot{b} \end{bmatrix} = -i\begin{bmatrix} (-i\omega/2)e^{-i\omega t/2}a \\ (+i\omega/2)e^{+i\omega t/2}b \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \omega_0 e^{-i\omega t/2}a + \omega_1 e^{-i\omega t/2}b \\ \omega_1 e^{i\omega t/2}b - \omega_0 e^{i\omega t/2}b \end{bmatrix} \tag{9.7}$$

Notice that both equations are multiplied by an exponential, which we can simplify.

$$i\begin{bmatrix} \dot{a} \\ \dot{b} \end{bmatrix} = \begin{bmatrix} (-\omega/2)a \\ (+\omega/2)b \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \omega_0 a + \omega_1 b \\ \omega_1 b - \omega_0 b \end{bmatrix} = \frac{1}{2}\begin{bmatrix} \omega_0 - \omega & \omega_1 \\ \omega_1 & -(\omega_0 - \omega) \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} \tag{9.8}$$

We can express this as a Schrödinger equation with a Hamiltonian

$$\widetilde{H} = \frac{\hbar}{2}\begin{bmatrix} \omega_0 - \omega & \omega_1 \\ \omega_1 & -(\omega_0 - \omega) \end{bmatrix} = R_z(\omega t) H R_z(-\omega t) \tag{9.9}$$

So to study the time evolution of the starting system we just need to diagonalize $\widetilde{H}$. Its eigenvalues are $E_{1,2} = \pm\hbar/2\sqrt{(\omega_0-\omega)^2+\omega_1^2} \overset{\text{def}}{=} \hbar\omega_i/2$ (the notation conflict in the definitions of ω_1 may be confusing but I only use this notation once). The eigenvectors are the generators of $\ker(\widetilde{H}-E_i\mathbb{1})$: the ratios of their components are

$$\frac{b}{a} = \frac{\omega_i-(\omega_0-\omega)}{\omega_1} = \frac{\pm\sqrt{(\omega_0-\omega)^2+\omega_1^2}-(\omega_0-\omega)}{\omega_1} \tag{9.10}$$

We call $\omega_1/(\omega_0-\omega) = \tan(\theta)$. Then:

$$\frac{b}{a} = \pm\sqrt{1+\frac{1}{\tan^2(\theta)}}-\frac{1}{\tan(\theta)} \tag{9.11a}$$

$$\frac{b}{a}\tan(\theta) = \pm\sqrt{1+\tan^2(\theta)}-1 = \pm\frac{1}{\cos(\theta)}-1 \tag{9.11b}$$

$$\frac{b}{a}\sin(\theta) = \pm 1-\cos(\theta) \tag{9.11c}$$

$$\frac{b}{a} = \tan(\theta/2) \qquad \text{or} \qquad \frac{b}{a} = -\frac{1}{\tan(\theta/2)} \tag{9.11d}$$

To get step (9.11d) we used the identities $\sin^2(\theta/2) = \big(1-\cos(\theta)\big)/2$, $\cos^2(\theta/2) = \big(1+\cos(\theta)\big)/2$ and $\sin(\theta) = 2\sin(\theta/2)\cos(\theta/2)$.

Now, what we want to look at is the probability of a transition $\langle 1|\, U(t)\, |0\rangle$ (and vice versa, but there is symmetry and we just need to calculate this one).

Making the relation in (9.11d) explicit, our eigenfunctions are

$$|E_1\rangle = \begin{bmatrix}\cos(\theta/2)\\ \sin(\theta/2)\end{bmatrix} \qquad \text{and} \qquad |E_2\rangle = \begin{bmatrix}-\sin(\theta/2)\\ \cos(\theta/2)\end{bmatrix} \tag{9.12}$$

We express $|0\rangle$ and $|1\rangle$ in this basis: $|0\rangle = \cos(\theta/2)\,|E_1\rangle - \sin(\theta/2)\,|E_2\rangle$, $|1\rangle = \sin(\theta/2)\,|E_1\rangle + \cos(\theta/2)\,|E_2\rangle$. Then we can readily apply the evolution operator $U(t) = \sum_i \exp\big(E_i t/(i\hbar)\big)\,|E_i\rangle\langle E_i|$:

$$U(t)\,|0\rangle = \cos(\theta/2)\exp\left(\frac{E_1 t}{i\hbar}\right)|E_1\rangle - \sin(\theta/2)\exp\left(\frac{E_2 t}{i\hbar}\right)|E_2\rangle \tag{9.13}$$

and the desired transition probability is $\langle 1|\, U(t)\, |0\rangle$:

$$\big(\sin(\theta/2)\,\langle E_1| + \cos(\theta/2)\,\langle E_2|\big)\left(\cos(\theta/2)\exp\left(\frac{E_1 t}{i\hbar}\right)|E_1\rangle - \sin(\theta/2)\exp\left(\frac{E_2 t}{i\hbar}\right)|E_2\rangle\right) \tag{9.14a}$$

$$= \sin(\theta/2)\cos(\theta/2)\left(\exp\left(\frac{E_1 t}{i\hbar}\right)-\exp\left(\frac{E_2 t}{i\hbar}\right)\right) \tag{9.14b}$$

Then, we can compute the transition probability as $\mathbb{P} = \big|\langle 1|\, U(t)\, |0\rangle\big|^2$. Recall $\sin(\arctan\theta) = x/\sqrt{1+x^2}$: for the first part we have

$$\big|\sin(\theta/2)\cos(\theta/2)\big|^2 = \frac{1}{4}\left|\sin\left(\arctan\left(\frac{\omega_1}{\omega_0-\omega}\right)\right)\right|^2 = \frac{1}{4}\frac{\omega_1^2}{(\omega_0-\omega)^2+\omega_1^2} \tag{9.15}$$

for the exponentials, let us call $E_i = \pm x\hbar/2$ with $x = \sqrt{(\omega_0-\omega)^2+\omega_1^2}$.

$$\left|\exp\left(\frac{xt}{2i}\right)-\exp\left(\frac{-xt}{2i}\right)\right|^2 = 4\left|\sin\left(\frac{xt}{2}\right)\right|^2 \tag{9.16}$$

So, in the end we get

$$\mathbb{P} = \frac{4}{4} \frac{\omega_1^2}{(\omega_0 - \omega)^2 + \omega_1^2} \sin^2 \left(\frac{t}{2} \sqrt{(\omega_0 - \omega)^2 + \omega_1^2} \right) \tag{9.17}$$

Now, recall that the magnetic fields are under our control: we can change $\omega_{0,1}$ as we wish. So, if we set $\omega_0 = \omega$ we get

$$\mathbb{P} = \sin^2 \left(\frac{t}{2} \sqrt{(\omega_0 - \omega)^2 + \omega_1^2} \right) \tag{9.18}$$

therefore our NOT gate is: turn on the magnetic fields and wait for a time such that

$$\frac{t}{2} \sqrt{(\omega_0 - \omega)^2 + \omega_1^2} = \frac{\pi}{2} \tag{9.19}$$

9.2 CNOT gate

We start with a two-system Hamiltonian like

$$H = -B_0 \big(\mu_1 \sigma_1^z \otimes \mathbb{1}_2 + \mu_2 \mathbb{1}_1 \otimes \sigma_2^z \big) + J \sigma_1^z \otimes \sigma_2^z \tag{9.20}$$

this is already diagonal, and looks like:

$$H = \begin{bmatrix} -B_0(\mu_1 + \mu_2) + J & & & \\ & -B_0(\mu_1 - \mu_2) - J & & \\ & & -B_0(-\mu_1 + \mu_2) - J & \\ & & & -B_0(-\mu_1 - \mu_2) + J \end{bmatrix} \tag{9.21}$$

Now: we can add a sinusoidal perturbation Hamiltonian (say, sending LASER photons with energy $E = \hbar\omega$). We want to excite the transitions $|10\rangle \leftrightarrow |11\rangle$ but not $|00\rangle \leftrightarrow |01\rangle$: the energy needed for the former is $E_1 = 2(B_0\mu_2 + J)$, for the latter it is $E_0 = 2(B_0\mu_2 - J)$.

So, if we set the laser to $E = E_1$ and keep it on for the right amount of time we can invert the second qubit *only* if the first is in state $|1\rangle$.

10 Density matrices

Say we have a generic observable $\hat{A} = \sum_i a_i |a_i\rangle\langle a_i|$, and our has a probability p_i of being in the state $|\psi_i\rangle$: of course we must have $\sum_i p_i = 1$. Then, we want to compute the expectation value $\langle A \rangle$ in this "mixed" state: it will look like

$$\begin{aligned} \langle A \rangle &= \sum_{i,k} p_i a_k \langle \psi_i | a_k \rangle \langle a_k | \psi_i \rangle && \text{(10.1a)} \\ &= \sum_{i,j,k} p_i a_k \langle a_k | \left(\left| a_j \right\rangle\!\left\langle a_j \right| \right) |\psi_i\rangle \langle \psi_i | a_k \rangle && \text{(10.1b)} \\ &= \sum_k \langle a_k | \left(\sum_j \underbrace{a_k}_{\substack{k \equiv j \text{ since it is} \\ \text{multiplied by } \delta_{jk}}} \left| a_j \right\rangle\!\left\langle a_j \right| \right) \left(\sum_i p_i |\psi_i\rangle\langle\psi_i| \right) |a_k\rangle && \text{(10.1c)} \\ &= \operatorname{Tr}\big(A\rho\big) = \operatorname{Tr}\big(\rho A\big) && \text{(10.1d)} \end{aligned}$$

So, we have defined

$$\rho \overset{\text{def}}{=} \sum_k p_k |\psi_k\rangle\langle\psi_k| \tag{10.2}$$

Properties

1. $\operatorname{Tr}\rho = 1$
2. $\rho = \rho^\dagger$
3. $\rho \geq 0$
4. $\operatorname{Tr}\rho^2 \leq 1$

These can be deduced from writing the matrix elements $\rho_{ij} = \langle i| \rho |j\rangle$ in an ON basis, or by noticing that ρ is a positively-weighted sum of projectors, each of which is self-adjoint.

The first one needs the components approach, I think: $\rho_{ii} = \sum_{ik} \left|\langle \psi_k | i \rangle\right|^2 = 1$ since they are the components in a basis of a normalized ket.

The last property can be seen by noticing that ρ is self-adjoint, so it has an orthonormal basis: then squaring it is easy, and all the coefficients are such that $p_i^2 \leq p_i$.

Time evolution of a density matrix How does ρ evolve? If we have U, we can write the evolution by linearity as

$$\rho(t) = \sum_k p_k U |\psi_k\rangle\langle\psi_k| U^\dagger = U\rho_0 U^\dagger \tag{10.3}$$

If instead we wish to look at the differential formulation, starting from $i\hbar |\dot\psi_k\rangle = H|\psi_k\rangle$ and its adjunct $-i\hbar\langle\dot\psi_k| = \langle\psi_k| H$ we get

$$\frac{\mathrm{d}}{\mathrm{d}t}\rho(t) = \sum_k p_k \frac{\mathrm{d}}{\mathrm{d}t}\Big(|\psi_k\rangle\langle\psi_k|\Big) = \frac{1}{i\hbar}\sum_k p_k \Big(H|\psi_k\rangle\langle\psi_k| - |\psi_k\rangle\langle\psi_k| H\Big) = \frac{[H,\rho]}{i\hbar} \tag{10.4}$$

Pure states A density matrix is a *pure state* if it has only one component, in the sense that: $\rho = |\psi\rangle\langle\psi|$. The following are equivalent:

1. ρ is a density matrix;
2. ρ has rank 1;
3. $\operatorname{Tr}\rho^2 = 1$.

The quantity $\operatorname{Tr}\rho^2$ is called the *purity*, and is surely greater than $1/d$, d being the dimension of the Hilbert space (consider $\rho = d^{-1}\mathbb{1}$).

Examples of density matrices For a single pure qubit:

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \cos^2(\theta/2) & \cos(\theta/2)\sin(\theta/2)e^{-i\varphi} \\ \cos(\theta/2)\sin(\theta/2)e^{i\varphi} & \sin^2(\theta/2) \end{bmatrix} \tag{10.5}$$

For a generic one-qubit mixed state:

$$\rho = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma}) = \frac{1}{2}\begin{bmatrix} 1 \\ x \\ y \\ z \end{bmatrix} \cdot \begin{bmatrix} \mathbb{1} \\ \sigma_x \\ \sigma_y \\ \sigma_z \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix} \tag{10.6}$$

it can be shown by direct computation that in this case $\operatorname{Tr}\rho^2 = {}^1\!/_2(1+|r|^2)$,where $\vec{r} = (x,y,z)$: so the state is pure for $|\vec{r}| = 1$, and the purity is quadratic in $|\vec{r}|$.

We could also look at $\det\rho = {}^1\!/_4(1-|r|^2)$ and see that it is zero when $|\vec{r}| = 1$, but that method seems less powerful...

Composite systems Say we have two Hilbert spaces 1 and 2, with their respective orthonormal bases $|i\rangle$ and $|\alpha\rangle$ respectively (let us work with finite-dimensional ones for simplicity).

Say we want to calculate the expectation value of an observable A_1 on 1: we must write it as $A_T = A \otimes \mathbb{1}_2$. Of course, our density matrix will also have four indices. Then

$$\langle A\rangle = \operatorname{Tr}\left(\rho A_T\right) = \sum_{k\gamma} \langle k\gamma| \left(\sum_{ij\alpha\beta} \rho^{j\beta}_{i\alpha} |i\alpha\rangle\langle j\beta|\right) \left(\sum_{mn\sigma\xi} A^n_m \delta^\xi_\sigma |m\sigma\rangle\langle n\xi|\right) |k\gamma\rangle \tag{10.7}$$

So we can make the sums implicit, the components of A explicit, and simplify some δs:

$$\operatorname{Tr}\left(\rho A_T\right) = \delta^i_k \delta^\alpha_\gamma \rho^{j\beta}_{i\alpha} \delta^m_j \delta^\sigma_\beta A^n_m \delta^\xi_\sigma \delta^k_n \delta^\gamma_\xi = \rho^{j\alpha}_{i\alpha} A^i_j \tag{10.8}$$

The simplifications are easier to understand by writing the index equivalencies: $m \equiv j$, $i \equiv k \equiv n$ and $\alpha \equiv \gamma \equiv \xi \equiv \sigma \equiv \beta$.

The trace with a simple one-subsystem density matrix, with the same one-subsystem observable A, would look like

$$\operatorname{Tr}\left(\rho A\right) = \rho^j_i A^k_j \delta^i_k = \rho^j_i A^i_j \tag{10.9}$$

So it becomes clear that we can use the traced matrix $\rho^{j\alpha}_{i\alpha} \overset{\text{def}}{=} (\rho_1)^j_i$ as a *reduced density matrix* for the first subsystem. We can write this in index-free notation as

$$\rho_1 = \underset{2}{\operatorname{Tr}} \rho \tag{10.10}$$

Note that even when ρ is a pure state, if we trace out a subsystem it can become mixed: this can be seen with $\rho = 1/2(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$, whose $\rho_1 = 1/2(|0\rangle\langle 0| + |1\rangle\langle 1|)$.

11 Correlations

We want to characterize quantum observables x and y. Let us start by defining the standard deviation:

$$\sigma_x = \sqrt{\left\langle (x - \langle x\rangle)^2 \right\rangle} \tag{11.1}$$

So, we can define the covariance between two variables:

$$C_{xy} = \frac{\left\langle (x - \langle x\rangle)(y - \langle y\rangle) \right\rangle}{\sigma_x \sigma_y} = \frac{\langle xy\rangle - \langle x\rangle \langle y\rangle}{\sigma_x \sigma_y} \tag{11.2}$$

(Unless $[x, y] = 0$ this is not the same as C_{yx}!)

12 Schmidt decomposition

Let us take a generic state in a two-subsystem system: $|\psi\rangle = \sum_{i,\alpha} c_{i\alpha} |i\rangle_A |\alpha\rangle_B$. In general, this will be a superposition of $\dim A \dim B$ states. Schimdt says we can write it as

$$|\psi\rangle = \sum_{i=1}^{k} \sqrt{p_i}\, |i\rangle_A \left|\alpha(i)\right\rangle_B \tag{12.1}$$

where k is called the *Schmidt rank*, and the $\left|\alpha(i)\right\rangle$ are orthormal. Also, $p_i \geq 0$ and $\sum_i p_i = 1$.

How do we get this? We start from our generic state and rewrite it:

$$|\psi\rangle = \sum_{i,\alpha} c_{i\alpha} |i\rangle_A |\alpha\rangle_B \tag{12.2a}$$

$$= \sum_i |i\rangle \left(\sum_\alpha c_{i\alpha} |\alpha\rangle \right) \tag{12.2b}$$

$$= \sum_i |i\rangle \left|\widetilde{\alpha}(i)\right\rangle \tag{12.2c}$$

This seems fine, but the $\left|\widetilde{\alpha}(i)\right\rangle$ do not have the properties we want: they are not orthonormal. Let us use equation (10.10), with an explicit one-subsystem matrix, and set it equal to the density matrix of (12.2c).

$$\sum_i p_i |i\rangle\langle i| = \operatorname*{Tr}_2 \left(\sum_{i,j} |i\rangle \left|\widetilde{\alpha}(i)\right\rangle \langle j| \left\langle\widetilde{\alpha}(j)\right| \right) \tag{12.3a}$$

$$= \sum_\gamma \langle\gamma| \left(\sum_{i,j} |i\rangle \left|\widetilde{\alpha}(i)\right\rangle \langle j| \left\langle\widetilde{\alpha}(j)\right| \right) |\gamma\rangle \tag{12.3b}$$

$$= \sum_{i,j} |i\rangle \langle j| \left(\left\langle\widetilde{\alpha}(i)\right| \left(\sum_\gamma |\gamma\rangle\langle\gamma| \right) \left|\widetilde{\alpha}(j)\right\rangle \right)^* \tag{12.3c}$$

$$= \sum_{i,j} |i\rangle \langle j| \left\langle\widetilde{\alpha}(j)\middle|\widetilde{\alpha}(i)\right\rangle \tag{12.3d}$$

So, in order for the equality to work it must be that $\left\langle\widetilde{\alpha}(j)\middle|\widetilde{\alpha}(i)\right\rangle = p_i\delta_{ij}$. So, we can rewrite equation (12.2c) with $\left|\widetilde{\alpha}(i)\right\rangle \to \left|\widetilde{\alpha}(i)\right\rangle / \sqrt{p_i}$, which are orthonormal. So, we get

$$|\psi\rangle = \sum_i \sqrt{p_i}\, |i\rangle \left|\widetilde{\alpha}(i)\right\rangle \tag{12.4}$$

and the properties of the p_i are inherited from the one-subsystem matrix.

Note that the Schmidt rank is very susceptible to small perturbations.

Correletions for separable states A separable state can be written as $|\psi\rangle = |i\rangle_A |\alpha\rangle_B$. If we have an observable on either system, then the correlation will be zero, since the averaging in $\langle x_A y_B \rangle$ will factor.

Purification If we have a generic state $\rho = \sum_i p_i |i\rangle\langle i|$, we can add a second subsystem in order to make it into a pure state: let us call the full density matrix $\sigma = |\psi\rangle\langle\psi|$, which must equal ρ if we trace out the second system. The components of σ will look like $\sigma_{i\alpha}^{j\beta} = c_{i\alpha}c_{j\beta}^*$, c being the components of $|\psi\rangle$ in the two-system basis.

$$\rho = \sum_\gamma \langle\gamma| \left(\sum_{ij\alpha\beta} \sigma_{i\alpha}^{j\beta} |i\alpha\rangle \langle j\beta| \right) |\gamma\rangle \tag{12.5a}$$

$$= \sum_{ij\alpha\beta} \sigma_{i\alpha}^{j\beta} |i\rangle \langle j| \langle\beta|\alpha\rangle \tag{12.5b}$$

$$\sum_{ij} \rho_{ij} |i\rangle\langle j| = \sum_{ij\alpha\beta} c_{i\alpha}c_{j\beta}^* \delta_\alpha^\beta |i\rangle\langle j| \tag{12.5c}$$

So the equation to be solved is $\rho_{ij} = c_{i\alpha}c_{j\alpha}^*$: these are $(\dim A)^2$ equations, and we have $(\dim B)^2$ parameters to tweak: so this can always be done with $\dim B = \dim A$.

13 Kraus representation

How does a subsystem ρ_1 of $\rho = \rho_1 \otimes |G\rangle\langle G|_2$ evolve? We are using a pure state for subsystem 2 but the construction will be general, since as we saw in 'Purification' on page 16 we can purify states. We know that $\rho(t) = U\rho U^\dagger$, so:

$$\rho_1(t) = \operatorname*{Tr}_2\Big(U\big(\rho_1 \otimes |G\rangle\langle G|_2\big)U^\dagger\Big) = \sum_k \langle k| U |G\rangle \rho_1 \langle G| U^\dagger |k\rangle \tag{13.1}$$

so we define $E_k = \langle k| U |G\rangle$. Note that this is still a matrix, since we only contracted the subsystem 2 indices. These matrices obey $\sum_k E_k^\dagger E_k = \mathbb{1}$. With this, we get

$$\rho_1(t) = \sum_k E_k \rho_1 E_k^\dagger \tag{13.2}$$

This defines a *superoperator* $\mathcal{S} : \rho \to \sum_k E_k \rho E_k^\dagger$.

Because of how it was defined, $\mathcal{S}$ has the following properties:

1. it preserves self-adjointness;
2. it preserves the trace;
3. it preserves non-negativity.

The set of the $\mathcal{S}$ also has a group structure, and $\mathcal{S}^{-1}$ exists iff $\mathcal{S}$ is unitary.

Kraus representations Any superoperator with properties 1, 2 and 3 it can be written as

$$\mathcal{S}(\rho) = \sum_k E_k \rho E_k^\dagger \tag{13.3}$$

14 Generalized measurements

A generalized measurement is defined by a set of operators M_i, such that $\sum_i M_i^\dagger M_i = \mathbb{1}$. They represent the possible results of the measurement: the wavefunction is reduced to

$$\frac{M_i |\psi\rangle}{\|M_i \psi\|} \qquad \text{with probability} \qquad p_i = \Big\| M_i |\psi\rangle \Big\|^2 = \langle\psi| M_i^\dagger M_i |\psi\rangle \tag{14.1}$$

Note that the probabilities are normalized: $\sum_i p_i = 1$.

If all the M_i are projectors ($M_i = M_i^\dagger = M_i^2$) then we get the usual Von Neumann projective measurements.

Naimark Theorem Generalized measurements are equivalent to projective measurements in a larger space: more specifically, a generalized measurement is equivalent to:

1. Adding some ancillary qubits;
2. evolving the whole system unitarily;
3. taking a projective measurement.

Unitary characterization of Kraus evolution We have a Kraus evolution $\rho \to \sum_k E_k \rho E_k^\dagger$, with $\sum_k E_k^\dagger E_k = \mathbb{1}$.

Let us introduce a subsystem 2, with dimension the number of Kraus operators, and its orthonormal basis $|k\rangle$, and the operator

$$U |\psi\rangle_1 |0\rangle_2 \overset{\text{def}}{=} \sum_k E_k |\psi\rangle_1 |k\rangle_2 \tag{14.2}$$

Claim 14.1. *U as defined is unitary.*

Proof. We can show this by proving $\langle\psi 0| U^\dagger U |\psi 0\rangle = 1$. This is then just a calculation:

$$\langle\psi 0| U^\dagger U |\psi 0\rangle = \sum_{k,k'} \langle\psi|_1 \left\langle k'\right|_2 E_{k'} E_k |\psi\rangle_1 |k\rangle_2 = \langle\psi|_1 \left(\sum_k E_k^\dagger E_k\right) |\psi\rangle_2 = 1 \tag{14.3}$$

□

Claim 14.2. *Taking the Kraus evolution of $\rho_1 = |\psi\rangle\langle\psi|$ is equivalent to evolving $\rho = |\psi 0\rangle\langle\psi 0|$ according to U and then tracing out subsystem 2.*

Proof. The evolution of ρ is $\sum_{k,m} E_k |\psi\rangle_1 |k\rangle_2 \langle\psi|_1 \langle m|_2 E_m^\dagger$. Let us take the trace of this wrt subsystem 2: we get

$$\sum_j \langle j|_2 \left(\sum_{k,m} E_k |\psi\rangle_1 |k\rangle_2 \langle\psi|_1 \langle m|_2 E_m^\dagger \right) |j\rangle_2 = \sum_k E_k |\psi\rangle\langle\psi|_1 E_k^\dagger = \sum_k E_k \rho_1 E_k^\dagger \tag{14.4}$$

□

Claim 14.3. *Evolving $|\psi\rangle |0\rangle$ according to U and then taking a projective measurement of subsystem 2 is equivalent to a generalized measurement on subsystem 1.*

Proof. We take the measurement $P = \mathbb{1}_1 \otimes |i\rangle\langle i|_2$.

$$\begin{aligned}
\operatorname*{Tr}_{12}(\rho P_i) &= \sum_{jq} \langle j|_1 \langle q|_2 \left(\sum_{k,m} E_k |\psi\rangle_1 |k\rangle_2 \langle\psi|_1 \langle m|_2 E_m^\dagger \right) \left(\mathbb{1}_1 \otimes |i\rangle\langle i|_2\right) |j\rangle_1 |q\rangle_2 && \text{(14.5a)}\\
&= \sum_j \langle j|_1 \left(E_i |\psi\rangle\langle\psi|_1 E_i^\dagger \right) |j\rangle_1 && \text{(14.5b)}\\
&= \operatorname*{Tr}_1 \left(|\psi\rangle\langle\psi| E_i^\dagger E_i \right) && \text{(14.5c)}
\end{aligned}$$

□

Weak measurements We wish to measure a system without disturbing it too much: let us consider a System-Environment couple of qubits, in the initial state $|\psi\rangle = \left(\alpha |0\rangle + \beta |1\rangle\right)_S \otimes |0\rangle_E = \alpha |00\rangle + \beta |10\rangle$. We apply the gate

$$U = (R_z(-\theta)_S \otimes \mathbb{1}_E)\left(\cos(\theta)\mathbb{1}_{SE} - i\sin(\theta) \mathrm{C}_S\mathrm{NOT}_E\right) = \begin{bmatrix} e^{-i\theta} & & & \\ & e^{-i\theta} & & \\ & & e^{-i\theta}\cos\theta & -ie^{-i\theta}\sin\theta \\ & & -ie^{-i\theta}\sin\theta & e^{-i\theta}\cos\theta \end{bmatrix} \tag{14.6}$$

The global phase can be removed. The phases on the bottom square of the matrix come from the rotation, while the ones on the top come from Euler's identity applied to the CNOT.

(θ is small). The result of the application of this gate to $|\psi\rangle$ is

$$U|\psi\rangle = \alpha |00\rangle + \beta\left(\cos(\theta) |10\rangle - i\sin(\theta) |11\rangle\right) \tag{14.7}$$

Now, we measure the environment: we will most likely (with probability $\sim 1 - |\beta|^2\theta^2$) get 0: in this case the system is reduced to

$$\frac{\alpha |00\rangle + \beta\cos(\theta) |10\rangle}{\sqrt{|\alpha|^2 + |\beta\cos(\theta)|^2}} \tag{14.8}$$

which approaches $|\psi\rangle$ as $\theta \to 0$. If, instead, we get 1, the state becomes $|11\rangle$.

This does not seem very useful, as it can only provide us with some statistical bounds on the size of β if we measure a few times, but we must not do it too often...

14.1 POVMs

We get some set of positive operators F_i such that $\sum_i F_i = \mathbb{1}$, and use these as the possible results of our measurement, which we will get with probabilities $p_i = \langle\psi|F_i|\psi\rangle$, or more generally $p_i = \mathrm{Tr}(\rho F_i)$.

They are useful in describing destructive measurements, like a photodetector. It is interesting when $p_i = 0$ with some ψ, because if we see that detector go off we know the system was *not* in ψ.

15 Quantum channels

An example of decoherence by interaction If our first system starts in $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, so

$$\rho = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \tag{15.1}$$

Now, let us consider a second subsystem, so the state becomes $\alpha|00\rangle + \beta|10\rangle$, then we apply a CNOT gate controlling on our first subsystem: the state becomes $\alpha|00\rangle + \beta|11\rangle$. If we trace the second subsystem out, the density matrix becomes

$$\rho' = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix} \tag{15.2}$$

Linear transformations in Bloch space We take a Kraus transformation of a density matrix as given in equation (13.3), and represent it as in equation (10.6): $\rho = 1/2(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$ (and in the same fashion ρ' with r').

Claim 15.1. *This Kraus transformation corresponds to a linear map $r_i \to M_i^j r_j + c_i$ which is a contraction.*

Proof. We can expand the Kraus matrices as $E_k = \gamma_k\mathbb{1} + \sum_i a_{ik}\sigma_i$: our full expression becomes

$$\rho \to \rho' = \sum_k \left(\gamma_k\mathbb{1} + \sum_i a_{ik}\sigma_i\right)\frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})\left(\gamma_k^*\mathbb{1} + \sum_j a_{jk}^*\sigma_j^\dagger\right) \tag{15.3}$$

and our claim is that

$$\rho' = \frac{1}{2}\left(\mathbb{1} + \left(M_i^j r_j + c_i\right)\sigma_i\right) \tag{15.4}$$

for some matrix M_i^j and vector c_i. This can be readily seen by noticing that:

1. products of Pauli matrices are linear combinations of Pauli matrices: $\sigma_a\sigma_b = \delta_{ab}\mathbb{1} + i\varepsilon_{abc}\sigma_c$;
2. the Kraus transformation sends density matrices into density matrices, so the trace of ρ' will still be 1 and we will be able to separate the trace term $\mathbb{1}/2$ from the traceless Pauli matrix part (that is, there will not be any transformation-dependents coefficients multiplying the identity).

Now, to see that it is a contraction recall that $\operatorname{Tr}\rho^2 \leq 1$. We will apply the formula:

$$(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = (\vec{a}\cdot\vec{b})\mathbb{1} + i(\vec{a}\wedge\vec{b})\cdot\vec{\sigma} \tag{15.5}$$

So then:

$$\operatorname{Tr}(\rho')^2 = \operatorname{Tr}\left(\frac{1}{4}\left(\mathbb{1} + \vec{r'}\cdot\vec{\sigma}\right)^2\right) = \operatorname{Tr}\left(\frac{1}{2}\left(\frac{1 + |r'|^2}{2}\mathbb{1} + \vec{r'}\cdot\vec{\sigma}\right)\right) \tag{15.6}$$

therefore $|r'| \leq 1$: the image of the unit sphere is contained in the unit sphere. □

We can write explicit equations for M and c:

$$M_{jk} = \sum_l \left(2\operatorname{Re}\left(a_{lj}a_{lk}^*\right) + \delta_{jk}\left(|\gamma_l|^2 - \sum_p \left|a_{lp}\right|^2\right) + 2\sum_p \varepsilon_{jkp}\operatorname{Im}\left(\gamma_l^* a_{lp}\right)\right) \tag{15.7a}$$

$$c_j = 2i\sum_{klm}\varepsilon_{jlm}a_{kl}a_{km}^* \tag{15.7b}$$

It seems like it should be true that $|\det M| = 1$ (and $\vec{c} = 0$) iff there is only one E_k, that is, the channel is actually a unitary transformation.

***-flip channel**

$$\mathcal{S}(\rho) = |\alpha|^2 \sigma_i \rho \sigma_i^\dagger + \left(1 - |\alpha|^2\right)\rho \tag{15.8}$$

So $E_0 = \alpha\sigma_i$ and $E_1 = \sqrt{1 - |\alpha|^2}\mathbb{1}$.

1. $i = x$: bitflip
2. $i = z$: phaseflip
3. $i = y$: bitphaseflip

In the Bloch sphere, it keeps the dimension i still and shrinks along the other two by a factor $1 - 2|\alpha|^2$. For example, the bitflip gate approaches σ_x as $|\alpha|^2 \to 1$.

This circuit can be represented as unitary evolution: we add a subsystem with a wavefunction $|\psi\rangle = \alpha\,|1\rangle + \sqrt{1 - |\alpha|^2}\,|0\rangle$, and perform a control-$\sigma_i$ (where the new subsystem is the controller).

In the expression of ψ the 0 and 1 are swapped, right?

Depolarizing channel It mixes states: the fixed point is $r = 0$.

$$\mathcal{S}(\rho) = \frac{P}{3}\left(\sum_i \sigma_i \rho \sigma_i^\dagger\right) + (1 - P)\rho \tag{15.9}$$

$$r \to r\left(1 - \frac{4P}{3}\right) \tag{15.10}$$

Amplitude damping channel Its Kraus matrices are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-P} \end{bmatrix} \qquad E_1 = \begin{bmatrix} 0 & \sqrt{P} \\ 0 & 0 \end{bmatrix} \tag{15.11}$$

It moves the population towards $|0\rangle\langle 0|$: it maps $|1\rangle\langle 1| \to P\,|0\rangle\langle 0| + (1 - P)\,|1\rangle\langle 1|$.

The fixed point is a pure state, so this channel can increase the purity of a state; however, it is fundamentally an incoherent process.

In the Bloch sphere, the amplitude damping channel looks like:

$$r \to \begin{bmatrix} \sqrt{1-P} & & \\ & \sqrt{1-P} & \\ & & 1-P \end{bmatrix} r + \begin{bmatrix} 0 \\ 0 \\ P \end{bmatrix} \tag{15.12}$$

So, for example, $r = -\hat{z} \to (2P - 1)\hat{z}$. This transformation has only $(0, 0, 1)^\top$ as its fixed point.

Phase damping channel It models what we might see if our particle was in a variable magnetic field: the phase of the particle is rotated by varying similar continuously distributed angles. We can write the phase gate as $R_z(\theta) = \operatorname{diag}\left(e^{-i\theta/2}, e^{i\theta/2}\right)$. We assume the phase angles are normally distributed with variance λ:

$$p(\theta) = \frac{\exp\left(\frac{-\theta^2}{2\lambda}\right)}{\sqrt{\pi\lambda}} \tag{15.13}$$

then the channel looks like

$$\rho \to \int_{-\infty}^{+\infty} R_z(\theta)\rho R_z(-\theta) p(\theta)\, \mathrm{d}\theta \tag{15.14}$$

Now let us take a generic density matrix:

$$\rho = \begin{bmatrix} P & \alpha \\ \alpha^* & 1-P \end{bmatrix} \to \int \mathrm{d}\theta\, p(\theta) \begin{bmatrix} P & \alpha e^{-i\theta} \\ \alpha^* e^{i\theta} & 1-P \end{bmatrix} \tag{15.15}$$

and by putting together $p(\theta)e^{\pm i\theta}$ we can complete the square to get a Gaussian integral (which equals one since the pdf is already normalized) times $e^{-\lambda}$. So

$$\rho' = \begin{bmatrix} P & \alpha e^{-\lambda} \\ \alpha^* e^{-\lambda} & 1-P \end{bmatrix} \tag{15.16}$$

This can be also be interpreted as repeated application of the channel with the Kraus matrices

$$E_0 = \sqrt{1-P}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad E_2 = \sqrt{P}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \qquad E_2 = \sqrt{P}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{15.17}$$

which send

$$\rho \to \begin{bmatrix} \rho_{00} & \rho_{01}(1-P) \\ \rho_{10}(1-P) & \rho_{11} \end{bmatrix} \tag{15.18}$$

and if $P = \lambda\delta t$ for small δt and the interactions are very fast then $\rho'_{01} \to (1-\lambda\delta t)^{t/\delta t} \sim e^{-\lambda t}$.

Entanglement damping channel Let us consider a nice entangled couple of qubits, with $|\psi\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. How can we break it? We will use the Kraus operators $E_{1,2} = \mathbb{1} \otimes \mathrm{diag}(1, \cos(\theta))$ or $\mathbb{1} \otimes \mathrm{diag}(1, \sin(\theta))$.

Then, the density matrix becomes:

$$\frac{1}{2}\begin{bmatrix} & & & \\ & 1 & 1 & \\ & 1 & 1 & \\ & & & \end{bmatrix} \to \frac{1}{2}\begin{bmatrix} & & & \\ & 1 & \cos(\theta) & \\ & \cos(\theta) & 1 & \\ & & & \end{bmatrix} \tag{15.19}$$

If we trace out one subsystem, we get $\rho_i = 1/2\mathbb{1}$, before and after the transformation.

16 Master equation

We want to describe the time evolution of a system with Kraus matrices:

$$\rho(t) = \mathcal{S}(t, t_0)[\rho] = \sum_{k=0}^{N-1} E_k \rho E_k^\dagger \tag{16.1}$$

with $N \leq (\dim\mathcal{H})^2$. It must have the following properties:

1. $\mathcal{S}(t,t) = \mathbb{1}$;
2. It should become the conventional unitary evolution if $N = 1$;
3. at any time, we must have $\sum_k E_k^\dagger E_k = \mathbb{1}$.

How will these matrices look? We would like to assume $E_0 = \mathbb{1} + H/i\hbar\, \mathrm{d}t$, but this will not work: let us add a term $K\,\mathrm{d}t$, with a self-adjoint K.

The other E_k will then be $L_k\sqrt{\mathrm{d}t}$ to first order.

Expanding condition 3 to first order gives:

$$\left(\left(\mathbb{1}+\left(\frac{H}{i\hbar}+\frac{K}{\hbar}\right)\mathrm{d}t\right)\left(\mathbb{1}+\left(-\frac{H}{i\hbar}+\frac{K}{\hbar}\right)\mathrm{d}t\right)+\sum_k L_k^\dagger L_k\right)\mathrm{d}t \overset{!}{=} \mathbb{1}\,\mathrm{d}t \tag{16.2}$$

So, we must have $K = -\hbar/2\sum_k L_k^\dagger L_k$ (indeed self-adjoint). How will our density matrix evolve after $\mathrm{d}t$ then? We will assume $\mathcal{S}(t+\mathrm{d}t, t)[\rho] = \rho + \dot{\rho}\,\mathrm{d}t + O(\mathrm{d}t^2)$.

$$\dot{\rho} = \frac{[H,\rho]}{i\hbar} + \frac{\{K,\rho\}}{\hbar} + \sum_k L_k\rho L_k^\dagger \tag{16.3}$$

We can plug in our formula for K and compact the sums into one, to get the

Gorini–Kossakowski–Sudarshan–Lindblad equation

$$\dot{\rho} = \frac{[H,\rho]}{i\hbar} + \sum_k\left(L_k\rho L_k^\dagger - \frac{1}{2}\left\{L_k^\dagger L_k, \rho\right\}\right) \tag{16.4}$$

This works if the system has no memory. If, instead, the evolution depends not only on the present state but on events further past, we must use the

Markovian version The form we show here is the diagonal one. We have the restriction that the L_k must be traceless.

$$\dot{\rho} = \frac{[H,\rho]}{i\hbar} + \sum_k \gamma_k\left(L_k\rho L_k^\dagger - \frac{1}{2}\left\{L_k^\dagger L_k, \rho\right\}\right) \tag{16.5}$$

17 One-key cryptography

The simplest paradigm: we have a key k, decryption and encryption algorithms D and E: if P is the clear-text message and C is the encrypted one then $E_k(P) = C$ and $D_k(C) = P$.

Even a very simple algorithm is secure if the key is longer than the message, private and only used once: for example, if we have n letters in our alphabet, we can do $E_kP_i = (P_i - k_i) \mod n$ and $E_kC_i = (C_i + k_i) \mod n$.

We can distribute the keys with *Quantum Key Distribution*: there are different algorythms to do it, a modern one we will not treat uses entanglement and is called E91 since Eckert invented it. We will look at Bennet & Brassard.

Quantum Key Distribution: BB84 Alice wants to send Bob a secure string of ones and zeroes.

She selects two bases, say $B_z = \{|0\rangle, |1\rangle\}$ and $B_x = \{H|0\rangle, H|1\rangle\}$ (where we use the Hadamard gate, see 'Hadamard' on page 4).

At random, she chooses a basis with which to send each qubit, and keeps a record of the bases she used.

Bob receives the qubits and also measures them in a basis chosen between B_z and B_x, and keeps a record of the bases he used.

After the communication is finished, they exchange in clear text the list of the bases they used, and discard the bits where they used a different basis.

Now they have a secure shared list of bits: if Eve were to try to measure the qubits in the middle, around half the time she'd collapse the state into the wrong basis. So, Alice and Bob just need to check a portion of the bits they *should* share, and if they don't match then something is wrong: either there is too much noise, or somebody's listening in. Either way, they discard the whole key and try again.

Correction methods

1. First of all, we check on a part of our message the error rate R: if R/N is large ($\sim 1/2$) then we discard everything.

2. Now that we know R, we can choose some length ℓ such that $R\ell/N$ is still small: then, we do a parity check on every ℓ long block.

3. If we somehow know that Eve knows k bits of our message, we can still generate a key she will not be able to know: if we split our message into $n-k-s$ snippets for some s, she will be able to gather only $O(2^{-s})$ bits of information: after splitting the message, our *new* message is something like the parity of each snippet.

Attack methods Eve cannot intercept the qubits and resend them, that's the point. There are some things she could do, though:

1. **translucent attack**: Eve operates unitarily on the passing qubits, entangling them with some qubits she keeps, and which she measures only *after* Alice and Bob have communicated which basis they used.
   Surely she cannot completely *clone* the passing qubit, but she might do some sneaky low-interference stuff.
2. **collective attacks** on several qubits at once.

18 Dense coding

Bob and Alice prepare two qubits together, in $|\psi\rangle = \text{CNOT}(H \otimes \mathbb{1})\,|00\rangle = {}^1\!/\!\sqrt{2}(|00\rangle + |11\rangle)$. Now Alice takes a qubit with her, and Bob keeps the other.

Now they are far apart. Alice wants to send two classical bits xy. She chooses based on her two bits an operator between $U_i = \left\{\mathbb{1}, \sigma_x, \sigma_z, \sigma_y\right\}$ and applies it to her qubit.

The state becomes one of these:

$$U_0\,|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{18.1a}$$

$$U_1\,|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \tag{18.1b}$$

$$U_2\,|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{18.1c}$$

$$U_3\,|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \tag{18.1d}$$

Now she sends her qubit to Bob, who still has his.

Bob applies $\big(\text{CNOT}(H \otimes \mathbb{1})\big)^{-1} = (H \otimes \mathbb{1})\text{CNOT}$ to the qubits.

$$\big(\text{CNOT}(H \otimes \mathbb{1})\big)^{-1} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix} \tag{18.2}$$

Now, as can be seen by summing the combinations of rows of the matrix in (18.2) corresponding to the states $U_i\,|\psi\rangle$, Bob's qubits will be in the state $|xy\rangle$.

In the end, the protocol can be written as:

$$(H \otimes \mathbb{1})\text{CNOT}(U_i \otimes \mathbb{1})\text{CNOT}(H \otimes \mathbb{1})\,|00\rangle = |i\rangle \tag{18.3}$$

If we tried to do this with a mixed state, the application of $\mathbb{1}$ and σ_z would give the same result (${}^1\!/\!{}_2(|00\rangle\langle 00| + |11\rangle\langle 11|)$) as would σ_x and σ_y (${}^1\!/\!{}_2(|01\rangle\langle 01| + |10\rangle\langle 10|)$). So, since there would be only two distinguishable states, only 1 bit would be transmitted.

19 Bell Inequalities

Alice and Bob have some (entangled) state on their hands, and are separated by a space-like interval. Alice makes a measurement x and gets outcome a, Bob makes a measurement y and gets outcome b.

They repeat this several times, always with the same starting state. This whole experiment is then characterized by the function $\mathbb{P}(ab|xy)$. In general we will have correlations, so $\mathbb{P}(ab|xy) \neq \mathbb{P}(a|x)\mathbb{P}(b|y)$. If our theory is local, however, these cannot be explained by the transmission of information from Alice to Bob. Can we describe them by some local unknown (*hidden*) variable which determines the measurement *a priori*?

Claim 19.1. *The results of a Bell experiment which are predicted by quantum mechanics* cannot *be described by a hidden variable λ distributed according to some function $q(\lambda)$, with an expression in the form:*

$$\mathbb{P}(ab|xy) = \int q(\lambda)\mathbb{P}(a|x;\lambda)\mathbb{P}(b|y;\lambda)\,\mathrm{d}\lambda \tag{19.1}$$

Proof. We prove the statement by contradiction. How do we calculate a correlation under our hypothesis? To simplify, we assume $a, b \in \{+1, -1\}$ and $x, y \in \{0, 1\}$. I will use the (improper) notation $\mathrm{d}q = \mathrm{d}\lambda\, q(\lambda)$

$$\langle ab \rangle_{xy} = \sum_{ab} ab\mathbb{P}(ab|xy) = \int \mathrm{d}q \left(\sum_a a\mathbb{P}(a|x;\lambda)\right)\left(\sum_b b\mathbb{P}(b|y;\lambda)\right) \tag{19.2}$$

Therefore, $\langle ab \rangle_{xy} = \int \mathrm{d}q\, \langle a \rangle_{x,\lambda} \langle b \rangle_{y,\lambda}$. Subscripts, here, mean conditioning.

Hidden variable inequality (CHSH) Now, we consider the following quantity:

$$S = \langle ab \rangle_{00} + \langle ab \rangle_{01} + \langle ab \rangle_{10} - \langle ab \rangle_{11} \tag{19.3}$$

The minus sign is arbitrarily placed, it just matters that there is just one negative and three positive terms. We can show that $S \leq 2$: surely

$$S \leq \int \mathrm{d}q \left[\left|\langle b \rangle_{0,\lambda} + \langle b \rangle_{1,\lambda}\right| \sup \langle a \rangle_{0,\lambda} + \left|\langle b \rangle_{0,\lambda} - \langle b \rangle_{1,\lambda}\right| \sup \langle a \rangle_{1,\lambda}\right] \tag{19.4}$$

and, since the outcomes are ±1, for any λ: $\langle a \rangle_{x,\lambda} \leq 1$ and $\langle b \rangle_{y,\lambda} \leq 1$, so

$$S \leq \int \mathrm{d}q \left[\left|\langle b \rangle_{0,\lambda} + \langle b \rangle_{1,\lambda}\right| + \left|\langle b \rangle_{0,\lambda} - \langle b \rangle_{1,\lambda}\right|\right] \tag{19.5}$$

WLOG we can assume $\langle b \rangle_{0,\lambda} \geq \langle b \rangle_{1,\lambda} \geq 0$. Therefore the integrand is bounded by $\langle b \rangle_{0,\lambda} + \langle b \rangle_{1,\lambda} + \langle b \rangle_{0,\lambda} - \langle b \rangle_{1,\lambda} = 2\langle b \rangle_{0,\lambda} \leq 2$.

The probability density of λ must be normalized: $\int \mathrm{d}q = 1$. So, the integrand is an upper bound for the integral, and we get $S \leq 2$.

(This can be generalized to $|S| \leq 2$).

Quantum CHSH violation We use as our observables the spin in different directions: if we have a vector $\vec{a}$, then $\hat{O}_a = \vec{a} \cdot \vec{\sigma}$. As our state we take the antisymmetric spin singlet, $|\psi\rangle = {}^1\!/\!\sqrt{2}(|01\rangle - |10\rangle)$. We want to show that the correlation expectation value $\langle O_a \otimes O_b \rangle_\psi$ is equal to $-a \cdot b$. We only need to compute the central four elements of the 4x4 matrix $O_a \otimes O_b$, which correspond to the 01 and 10 basis elements.

$$[O_a \otimes O_b]_{\text{reduced}} = \begin{bmatrix} -a_z b_z & (a_x + ia_y)(b_x - ib_y) \\ (a_x - ia_y)(b_x + ib_y) & -a_z b_z \end{bmatrix} \tag{19.6}$$

We compute the expectation value of the matrix in (19.6):

$$\langle O_a \otimes O_b \rangle_\psi = \frac{1}{2}\begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} -a_z b_z & (a_x + ia_y)(b_x - ib_y) \\ (a_x - ia_y)(b_x + ib_y) & -a_z b_z \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{19.7a}$$

$$= \frac{1}{2}\Big(-a_z b_z - (a_x + ia_y)(b_x - ib_y) - (a_x - ia_y)(b_x + ib_y) + (-a_z b_z)\Big) \tag{19.7b}$$

$$= -\vec{a} \cdot \vec{b} \tag{19.7c}$$

Now: we pick as our measurement with possible outcomes 0, 1 two *pairs* of directions, and we call the result 0 if the spin is measured along the first, 1 if it measured along the second.

1. For $\vec{a}$, we call the result 0 if the spin direction is $\vec{a}_0 = \hat{x}$ and 1 if the spin direction is $\vec{a}_1 = \hat{y}$;
2. for $\vec{b}$, we call the result 0 if the spin direction is $\vec{b}_0 = -(\hat{x}+\hat{y})/\sqrt{2}$ and 1 if the spin direction is $\vec{b}_1 = -(\hat{x}+\hat{y})/\sqrt{2}$

So, we can compute S using equation (19.7c):

$$S = \langle ab \rangle_{00} + \langle ab \rangle_{01} + \langle ab \rangle_{10} - \langle ab \rangle_{11} = \frac{4}{\sqrt{2}} = 2\sqrt{2} > 2 \tag{19.8}$$

□

20 Nonlocal correlations

We want to define *probability spaces*. We will use the notation of section Bell Inequalities. If a, b can have $\Delta \in \mathbb{N}$ values, and there are $m \in \mathbb{N}$ possible measurements (x, y) we can make. Then, our correlations are a point $\mathbb{P}(ab|xy)$ in some subset $\mathcal{P}$ of $\mathbb{R}^{m^2\Delta^2}$, bounded by:

1. $\forall x, y, a, b : \mathbb{P}(ab|xy) \geq 0$;
2. $\forall x, y$:
$$\sum_{a=1}^{\Delta} \sum_{b=1}^{\Delta} \mathbb{P}(ab|xy) = 1 \tag{20.1}$$

Now, we define some subsets of this space.

No-Signaling The set is called NS. We impose a condition which means: *no matter what we do with a measurement, it will not affect the other*: $\forall x, x', y, y', a$

$$\sum_{b=1}^{\Delta} \mathbb{P}(ab|xy) = \sum_{b=1}^{\Delta} \mathbb{P}(ab|xy') \qquad \sum_{a=1}^{\Delta} \mathbb{P}(ab|xy) = \sum_{a=1}^{\Delta} \mathbb{P}(ab|x'y) \tag{20.2}$$

this implies $\mathbb{P}(a|x) = \mathbb{P}(a|xy) = \sum_b \mathbb{P}(ab|xy)$.

In the $\Delta = 2$ case, $a, b = \pm 1$ the No-Signaling conditions become

$$\mathbb{P}(ab|xy) = \frac{1 + a\langle A_x \rangle + b\left\langle B_y \right\rangle + ab\left\langle A_x B_y \right\rangle}{4} \geq 0 \tag{20.3}$$

so if A and B have zero average, $1 \pm \left\langle A_x B_y \right\rangle \geq 0$.
What?

Local correlations The set is called L. It is the set of correlations that can be written as in equation (19.1).

Quantum correlations The set is called Q.
If we have some operators $M_{a|x}$ and $M_{b|y}$ in their respective Hilbert spaces, such that for each conditioning they still form a POVM (see 'POVMs' on page 18), then Q is the set of the probabilities which can be expressed as

$$\mathbb{P}(ab|xy) = \operatorname{Tr}(\rho_{AB} M_{a|x} \otimes M_{b|y}) \tag{20.4}$$

This is in the context of nonprojective measurements, but as we saw in 'Purification' on page 16 states can be purified so that everything we do is unitary. In that context,

$$\mathbb{P}(ab|xy) = \left\langle \psi \middle| A_x \otimes B_y \middle| \psi \right\rangle \tag{20.5}$$

with some self-adjoint families of operators A_x and B_y.
It can be useful to have $A_x B_y$, a product of commuting observables $[A_x, B_y] = 0$ on the same space, instead of $A_x \otimes B_y$; these descriptions are surely equivalent in the finite-dimensional case, maybe the latter is more general in the infinite-dimensional one.

Shapes and inclusions Every one of these sets is of the same dimension, and it can be shown that NS, L are polytopes while Q's boundary is curved. Also, $L \subset Q \subset NS \subset \mathcal{P}$.

They are all bounded, convex, closed. The planes which separate them are in general called Bell Inequalities.

The $\Delta = 2, m = 2$ case We can have different linearly independent Ss, (S being the one defined in (19.3)). In 2D (a projection?) we have: L is a square ($|S_x| \leq 2$, $\left|S_y\right| \leq 2$), Q is a circle ($|S|^2 \leq 8$), NS is a square ($\left|S'_{x,y}\right| \leq 4$, with $S'_{x,y} = HS_{x,y}$ (H is the Hadamard gate)).

21 Entropy

A message is a sequence of characters from an alphabet. If the alphabet is $\mathcal{A} = \{a_i\}_i$ and each of the characters in the alphabet appears with probability p_i, we can define $\mathcal{A}$'s *entropy* as

$$H = -\sum_i p_i \log(p_i) \tag{21.1}$$

with the convention $0 \log 0 = 0$

Noiseless coding: Shannon's theorem Given a k-long message, asyntotycally as $k \to \infty$ there exists an encoding with which we can express each character of the message with H bits on average, or the whole message with kH bits.

If we take any encoding, it can only do as good as Shannon encoding, and no better (at least not *in general*).

Von Neumann entropy We can define the entropy of a mixed state ρ as

$$S_V = -\operatorname{Tr}\left(\rho \log \rho\right) \tag{21.2}$$

1. For pure states we have $S_V(|\psi\rangle\langle\psi|) = 0$;
2. S_V is invariant wrt unitary transformations;
3. $0 \leq S_V \leq \dim\mathcal{H}$;[1]
4. $S_V \leq H$: the Von Neumann entropy is always less than or equal to the classical one.

Quantum Noiseless coding: Schumacher's theorem If our alphabet is now made of pure states, the probability distribution of a message will be some hyper-density matrix, $\rho^{\otimes N}$.

Schumacher says: in the limit of infinite message length, we can always compress it with S_V bits per letter.

22 Entanglement measurements

We want a measurement $E(\rho)$ which satisfies:

1. If ρ is separable, then $E(\rho) = 0$;
2. $E(\rho) = E(U\rho U^\dagger)$;
3. If we have a set of operators $A_i \otimes B_i$, to each of which we associate a probability $p_i = \operatorname{Tr}\left((A_i \otimes B_i)\rho(A_i \otimes B_i)^\dagger\right)$, and which can project the state into the normalized application of the Kraus operators $\sigma_i = (A_i \otimes B_i)\rho(A_i \otimes B_i)^\dagger / p_i$, then

$$E(\rho) \geq \sum_i p_i E(\sigma_i) \tag{22.1}$$

[1] Since $\prod_{i=1}^N p_i^{-p_i} \leq N$.

> This means: the entanglement is invariant under local Kraus evolution: the systems cannot become *more* entangled when evolving on their own.
>
> NOT CLEAR HOW

4. If $\rho = \rho_A$ is a pure state then $E(\rho) = S_V(\rho_A)$.

Entanglement of formation We can define

$$E_F(\rho) = \min \sum_i p_i S_V(\rho^i_A) \tag{22.2}$$

where the minimum is to be taken over all the possible decompositions $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\rho^i_A = \mathrm{Tr}_B(|\psi_i\rangle\langle\psi_i|)$: so, we pick a decomposition, we trace out the second system and take the entropy.

Concurrence This only applies to two-qubit systems.

$$C(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{22.3}$$

Where the λ_i are eigenvalues of $\left(\rho\sigma_y^{\otimes 2}\right)^2$, taken in decreasing order.

23 Quantum algorithms

23.1 Oracle interrogation: Deutsch–Jozsa algorithm

We have an oracle function $f(x) : \{0,1\}^n \to \{0,1\}$ which is either *constant* (always gives the same result) or *balanced* (gives 0 for half of its inputs, and 1 for the other half).

With a classical computer, we'd need $\max(\lfloor n/2 \rfloor, 2)$ calls to the oracle in the worst case to be sure that it is one and not the other. With a quantum computer, we can do it in just one call.

Take $n = 1$ for simplicity.

Our unitary representation of an oracle must be invertible, so we take the input along:

$$U_f |x\rangle |y\rangle \to |x\rangle |f(x) \oplus y\rangle \tag{23.1}$$

where $\oplus$ is the XOR binary gate. y is generic, it could be set to zero but we want a general gate. The algorithm is

1. Start with $|xy\rangle = |01\rangle$;
2. apply $H \otimes H$;
3. apply U_f;
4. apply $H \otimes \mathbb{1}$;
5. measure the first qubit.

First of all: $(H \otimes H)|01\rangle = (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)/2$. Now:

$$U_f |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-)^{f(x)} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{23.2}$$

So after the application of the oracle gate, the first qubit's state has become

$$\frac{1}{\sqrt{2}}\left((-)^{f(0)} |0\rangle + (-)^{f(1)} |1\rangle\right) \tag{23.3}$$

and if we apply a Hadamard to it, it becomes

$$\frac{1}{2}\left(\left((-)^{f(0)} + (-)^{f(1)}\right) |0\rangle \left((-)^{f(0)} - (-)^{f(1)}\right) |1\rangle\right) \tag{23.4}$$

therefore the state is *surely* $|\psi\rangle = [f(0) = f(1)]\,|0\rangle + [f(0) \neq f(1)]\,|1\rangle$.

***n*-qubit case** We do the same thing as before, only with n qubits: $|x\rangle = |0\rangle^{\otimes n}$ at the start, so after the Hadamards we get

$$H^{\otimes(n+1)} |x\rangle |y\rangle = \frac{1}{2^{(n+1)/2}} \sum_{x=0}^{2^n-1} |x\rangle_1 \left(|0\rangle - |1\rangle\right)_2 \tag{23.5}$$

so after applying the oracle and another Hadamard set we get

$$H^{\otimes n} \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-)^{f(x)} |x\rangle \right) \tag{23.6}$$

on the first qubit registry. Now, either $f(x)$ is constant or it is balanced: if it is constant then this is just $|0\rangle$. If it is not, then it is orthogonal (since at least one of the bits must be different): so we can just check whether the system is in $|0\rangle$.

23.2 Grover

The classical complexity for a search in an unstructured database is $O(N)$, with Grover's algorithm we get $O(N^{1/2})$.

The problem looks similar to the oracle: now our $f(x) = [x = \overline{x}]$ and we seek $\overline{x}$. We explain the procedure with $n = 2$:

1. Start with $\left|xy\right\rangle = \left|\vec{0}1\right\rangle$;
2. apply $H^{\otimes(n+1)}$;
3. apply U_f;
4. apply $D \otimes \mathbb{1}$;
5. measure the $|x\rangle$ state.

as before, after applying step 3 we get

$$|\psi\rangle_1 = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-)^{f(x)} |x\rangle = \frac{1}{2^{n/2}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) - 2 |\overline{x}\rangle \tag{23.7}$$

Now, D is 1/2 of the matrix with -1 on the diagonal, and 1 in every other entry. Its eigenvectors are exactly the possible $|x\rangle$ after the oracle, so after the application of D we get exactly $|\overline{x}\rangle$.

This D can be made with the usual gates as $H^{\otimes 2}\sigma_x^{\otimes 2}(\mathbb{1} \otimes H)\mathrm{CNOT}(\mathbb{1} \otimes H)\sigma_x^{\otimes 2}H^{\otimes 2}$. Below is the Python code to verify that it works.

We will also need the matrix D', which is such that $D = H^{\otimes 2}D'H^{\otimes 2}$. It turns out that $D' = \eta_{\mu\nu}$ for a Minkowski flat spacetime.

```python
import numpy as np
H = 1/np.sqrt(2)* np.array([[1,1], [1,-1]])
H2 = np.kron(H, H)
sigma_x = np.array([[0,1], [1,0]])
sigma_x2 = np.kron(sigma_x, sigma_x)
CNOT = np.array([[1,0,0,0],[0,1,0,0],[0,0,0,1],[0,0,1,0]])
idH = np.kron(np.identity(2), H)
print(’D = ’, H2 @ sigma_x2 @ idH @ CNOT @ idH @ sigma_x2 @ H2)
print(’Dprime = ’, sigma_x2 @ idH @ CNOT @ idH @ sigma_x2)
```

Arbitrary n This method only works for $n = 2$. In general, we have a state proportional $\sum_{x=0}^{2^n-1} |x\rangle |y\rangle$, an oracle such that $U_f |\overline{x}\rangle |y\rangle = -|\overline{x}\rangle |y\rangle$ while $U_f |x\rangle |y\rangle = |x\rangle |y\rangle$ for all the other $x \neq \overline{x}$.

Now, we can write $D' = \mathbb{1} - 2 |0\rangle\langle 0|_1$: so $D = \mathbb{1} - 2 |S\rangle\langle S|_1$, with $S = H^{\otimes 2} |0\rangle = \sum_{x=0}^{2^n-1} |x\rangle$.

Our main gate will be $G = DU_f$. What does it do? first, it flips the component of the state along $|\overline{x}\rangle$; then it flips the component along $|S\rangle$.

We know for sure that $|S\rangle$ and $|\overline{x}\rangle$ are not orthogonal: the angle between them will have $\cos(\varphi) = 2^{-n/2}$, the coefficient of $|\overline{x}\rangle$ in $|S\rangle$. We are interested in $\pi/2 - \varphi$, which we will call $\delta\theta$.

It can be shown by a simple geometric argument that the application of G sends a state which has an angle θ from the hyperplane $|\overline{x}\rangle^{\perp}$ into a state with an angle $\theta + 2\delta\theta$. So, we need K applications of G to get $\theta \to \pi/2$, with $K = (\pi/2)/(2\delta\theta)$: since $\sin\delta\theta = 2^{-n/2}$ and the rest are constants, $K = O(\sqrt{2^n}) = O(\sqrt{N})$, where N is the database size.

23.3 Quantum Fourier Transform

We have n qubits, and their states are $|x\rangle$ with x ranging from 0 to $N-1$, with $N = 2^n$.

Classical FFT The definition of the discrete Fourier transform of a vector x_i, with $i = 0, \dots, N-1$, $(N = 2^n)$ is

$$X_k = \sum_{j=0}^{N-1} x_j \exp\left(-\frac{2\pi ijk}{N}\right) \tag{23.8}$$

To do this in $O(N\log N)$ instead of $O(N^2)$, we split the sum into the even and odd parts:

$$X_k = \sum_{j=0}^{N/2-1} x_{2j} \exp\left(-\frac{2\pi i(2j)k}{N}\right) + \exp\left(-\frac{2\pi ik}{N}\right) \sum_{j=0}^{N/2-1} x_{2j+1} \exp\left(-\frac{2\pi i(2j)k}{N}\right) \tag{23.9}$$

Or in other words

$$\mathrm{FFT}(x)_k = \mathrm{FFT}(\mathrm{even}(x))_k + \exp\left(-\frac{2\pi ik}{N}\right)\mathrm{FFT}(\mathrm{odd}(x))_k \tag{23.10}$$

Then, we can apply the same split for the FFT of the even and odd parts, and so on.

This split will happen $\log N = n$ times, after which there will just be one term in the sum. We have to to this computation once for every possible value of the result vector, so in the end the complexity is $O(N\log N)$.

Quantum version We define

$$\mathrm{QFT}(|J\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi iJk}{N}\right) |k\rangle \tag{23.11}$$

where as usual $|k\rangle = |k_0k_1\dots k_{n-1}\rangle$. So, we can rewrite this as a sum over all the k_α:

$$\begin{aligned}
\mathrm{QFT}(|J\rangle) &= \frac{1}{\sqrt{N}} \prod_{\alpha=0}^{n-1} \sum_{k_\alpha=0}^{1} \exp\left(-\frac{2\pi iJ}{N}\right) \exp\left(\sum_{\alpha=0}^{n-1} k_\alpha 2^{n-\alpha-1}\right) |k\rangle && (23.12a)\\
&= \frac{1}{\sqrt{N}} \prod_{\alpha=0}^{n-1} \sum_{k_\alpha=0}^{1} \exp(-2\pi iJ) \exp\left(\sum_{\alpha=0}^{n-1} k_\alpha 2^{-\alpha-1}\right) |k\rangle && (23.12b)\\
&= \frac{1}{\sqrt{N}} \prod_{\alpha=0}^{n-1} \sum_{k_\alpha=0}^{1} \exp\left(-2\pi iJk_\alpha 2^{-\alpha-1}\right) |k\rangle && (23.12c)\\
&= \frac{1}{\sqrt{N}} \prod_{\alpha=0}^{n-1} \left(\sum_{k_\alpha=0}^{1} \exp\left(-2\pi iJk_\alpha 2^{-\alpha-1}\right) |k_\alpha\rangle\right) && (23.12d)\\
&= \frac{1}{\sqrt{N}} \prod_{\alpha=0}^{n-1} \left(|0\rangle_\alpha + \exp\left(-2\pi iJ2^{-\alpha-1}\right) |1\rangle_\alpha\right) && (23.12e)
\end{aligned}$$

but in the $\exp(-2\pi iJ2^\alpha)$ the terms in the binary expansion of J with a power higher than α will just make the term rotate by 2π, doing nothing.

So, to the Least Significant Bit $|J_{n-1}\rangle$ we just apply a Hadamard. To the second LSB $|J_{n-2}\rangle$ we apply a Hadamard, and then a control-$R_z(2\pi i/2^2)$. In general

$$|J_\alpha\rangle \to \bigotimes_{k=2}^{n-\alpha} (C_{|J_{n-k+1}\rangle} - R_z)(2\pi i/2^k) \otimes H\,|J_\alpha\rangle \tag{23.13}$$

23.4 Shor's algorithm

It is a method to factor a product of large numbers.

Motivation: two-key RSA cryptography Alice wants to communicate a message P to Bob. Bob generates a public key K_{Pu} and a private key K_{Pr}, he sends the public key K_{Pu} to Alice, who encodes the message with an algorithm E which depends on the public key:

$$C = E_{K_{\text{Pu}}}(P) = P^e \mod N \tag{23.14}$$

where N is chosen such that $N = pq$, with $p, q \in \mathbb{Z}_{\text{prime}}$, $\Phi = (p-1)(q-1)$, $1 < e < \Phi$, and $\text{GCD}(\Phi, e) = 1$.

The *public key* is $K_{\text{Pu}} = (N, e)$; the *private key* is $K_{\text{Pr}} = \Phi$ or equivalently (p, q).

She then sends C to Bob, who uses K_{Pr} to decode it with an algorithm D:

$$P = D_{K_{\text{Pr}}} C = C^d \mod N \tag{23.15}$$

where d is chosen such that $de = 1 \mod \Phi$.

This works because of Euler's theorem. If $\Phi(x)$ is the totient function, which returns the number of naturals $< x$ which are coprime with x, then since (unproven fact) Φ is multiplicative, $\Phi(pq) = (p-1)(q-1)$.

The theorem says that for any P, $P^\Phi \equiv 1 \mod N$. If $ed \equiv 1 \mod \Phi$ then $ed = k\Phi + 1$ for some $k \in \mathbb{N}$. So:

$$P^{ed} = P^{k\Phi+1} \equiv P \mod N \tag{23.16}$$

So we can decrypt our message $C = P^e$ by calculating $C^d = P^{ed}$.

In order to break the encryption we just need to factor N: if we have its factors then we can calculate Φ, after which it is easy to find a suitable d.

Factoring N is equivalent to finding the period of a function: the *order* r is the smallest number such that $x^r = 1 \mod N$: if we define a function $f(r) = x^r \mod N$, then r is also the period of that function, since the condition reads $f(r) = f(0)$.

If r is even, then $y = x^{r/2}$, so $y^2 = 1 \mod N$ therefore $(y+1)(y-1) = 0 \mod N$.

Therefore $(y+1)(y-1) = kN$ for some $k \in \mathbb{N}$, so we have found the factors.

Shor's algorithm Given $N = pq$, we have the following steps:

1. Choose $x < N$. If it divides N, we are done;
2. if they are not coprime (the check can be made quickly with Euclid's algorithm) start over;
3. find the order r of the function $f(r) = x^r \mod N$;
4. if r is even, we have the factors. If it is not, start over.

The quantum part is in step 3, which can be done using the QFT.

Hypotheses These are not actually needed but they make treating the problem much simpler, and there is not much to learn in generalizing: we assume $N = 2^n$ and $N/r = m \in \mathbb{N}$.

As always we cannot directly encode our function as a unitary transformation since it will be periodic, therefore not injective, therefore not unitary. So we encode it taking the input along, as

$$U : |x\rangle |0\rangle \longmapsto |x\rangle |f(x)\rangle \tag{23.17}$$

We start from $|0\rangle^{\otimes 2n}$, apply n Hadamards and get $|\psi_0\rangle$ = superposition of all possible states $\otimes |0\rangle^{\otimes n}$, and with this we prepare

$$|\psi_1\rangle = U |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{N} |x\rangle |f(x)\rangle \tag{23.18}$$

Step 2 We measure the second registry, and obtain $\left|\overline{f(x_0)}\right\rangle$ for some x_0. Then the first registry must contain all the combinations which generate that state: so:

$$|\psi_2\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle \left|\overline{f(x_0)}\right\rangle \tag{23.19a}$$

$$= \left[\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |x_0 + jr\rangle\right] \otimes \left|\overline{f(x_0)}\right\rangle \tag{23.19b}$$

Now we can discard the last n qubits.

Step 3 We want to find r, so we can do a quantum Fourier transform. It can be slow to actually measure the full transform for generic functions but in our case the transform is applied to a function which is already periodic

$$|\psi_3\rangle = \text{QFT}\Big\{|\psi_2\rangle\Big\} = \frac{1}{\sqrt{mN}} \sum_{y=0}^{N-1} \sum_{j=0}^{m-1} \exp\big(2\pi i(x_0 + jr)y/N\big) |y\rangle \tag{23.20}$$

Step 4 We compute the probability of obtaining a specific value $\overline{y}$ from a measure of the registry:

$$\mathbb{P}(\overline{y}) = \frac{1}{Nm} \left| \sum_{j=0}^{m-1} \exp\big(2\pi i(x_0 + jr)\overline{y}/N\big) \right| \tag{23.21a}$$

$$= \frac{1}{r} \left| \frac{1}{m} \sum_{j} \exp\big(2\pi i j \overline{y}/m\big) \right| \tag{23.21b}$$

where we used the fact that $N = mr$, and removed a global phase from the square.

Claim 23.1. *The states with nonzero probability to be found are those with $\overline{y} = km$, where $k \in 0, \dots, r$.*

Proof. If $\overline{y} = km$ then the exponential is always equal to one. Recall that $N = mr$, so we have exactly r possible values of k for which this is true, since $\overline{y} < N$.

So, for each of these we have $P(\overline{y} = km) = 1/r\Big|1/m \sum_j 1\Big| = 1/r$: the probability is saturated. □

So all the states we get are in the form $\overline{y} = km = kN/r$. We know N, we measured $\overline{y}$, so:

- if $k = 0$, we failed;
- if $k \neq 0$, we set $\overline{y}/N = \overline{k}/r$ and find the solution in polynomial time.

It can be shown that $\mathbb{P}(\text{success}) \sim 1$ after $O(\log(\log(r)))$ tries.

Recall $n = \log N$: the complexity of Shor's algorithm scales as $O(n^2 \log n \log\log n)$, whereas the classical algorithm scales as $\exp\Big(O(\sqrt[3]{n \log n})\Big)$.

It is important to emphasize that no classical algorithm has been found which runs in polynomial time, but it has *not* been proven that it is impossible for one to be found.

23.5 Phase estimation algorithm

Take a unitary transformation U such that it gives a phase to a specific autoket: $U|u\rangle = \exp(i\varphi)|u\rangle$, where $0 \leq \varphi \leq 2\pi$: we want to estimate φ.

Hypotheses We assume we are able to prepare $|u\rangle$, and that we have a blackbox $\left(C - U^{2^J}\right)$ for all $0 \leq J \leq n-1$: that is, a "control - U applied 2^J times", such that $\left(C - U^{2^J}\right) |0\rangle |u\rangle = |0\rangle |u\rangle$ and $\left(C - U^{2^J}\right) |1\rangle |u\rangle = \exp\left(i 2^J \varphi\right) |1\rangle |u\rangle$.

We write φ as

$$\varphi = 2\pi \left(\frac{a}{2^n} + \delta \right) = \overline{\varphi} + \delta\varphi \tag{23.22}$$

with $0 \leq \delta \leq 2^{-n-1}$ and $a = a_{n-1} a_{n-2} a_{n-3} \dots a_1 a_0$: we expressed it in binary, with some error.

Algorithm We introduce an ancillary registry of n qubits initialized to $|0\rangle$, while our main registry is made of m qubits, in which we encode $|u\rangle$. Their product is $|\psi_0\rangle$

We apply a H to each of the qubits in the first registry, and then the gates $\left(C - U^{2^J}\right)$ for each $0 \leq J < n$ controlling on the J-th qubit each time.

The result of this operation is $|\psi_1\rangle$. We apply a QFT to the n control bits, and the result is $|\psi_2\rangle$.

What is the result of applying $C - U^{2^J} \overset{\text{def}}{=} W$? It rotates u, but the phase can only be measured on the first registry:

$$\begin{aligned} \left(C - U^{2^J}\right) \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |u\rangle \right] &= \frac{1}{\sqrt{2}} [W |0\rangle |u\rangle + W |1\rangle |u\rangle] && (23.23a) \\ &= \frac{1}{\sqrt{2}} \left[|0\rangle |u\rangle + \exp\left(i 2^J \varphi\right) |1\rangle |u\rangle \right] && (23.23b) \\ &= \frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(i 2^J \varphi\right) |1\rangle \right] \otimes |u\rangle && (23.23c) \end{aligned}$$

Now we can see what is the phase by measuring the ancillary qubits, for example if the phase was just -1 we could apply a Hadamard gate and measure along the ± .

So the state $|\psi_1\rangle$ is

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \left(\bigotimes_{J=0}^{n-1} \left(|0\rangle + \exp\left(i\varphi 2^J\right) |1\rangle \right) \right) \otimes |u\rangle \tag{23.24}$$

which can be written as

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{N-1} \exp(i\varphi y) |y\rangle |u\rangle \tag{23.25}$$

We recall

$$\text{QFT}^{-1}\left\{ |y\rangle \right\} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \exp\left(-\frac{2\pi i x y}{2^n} \right) |x\rangle \tag{23.26}$$

therefore

$$|\psi_2\rangle = \text{QFT}^{-1} |\psi_1\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \exp\left(2\pi i (a - x) \frac{y}{2^n} \right) \exp(2\pi i \delta y) |x\rangle |u\rangle \tag{23.27a}$$

so

$$\mathbb{P}(b) = \left| \langle b| \frac{1}{2^n} \sum_x \sum_y \exp\left(2\pi i (a - x) \frac{y}{2^n} \right) \exp(2\pi i \delta y) |x\rangle \right|^2 \tag{23.28a}$$

$$= \left| \frac{1}{2^n} \sum_y \exp\left(\frac{-2\pi i y(a-b)}{2^n} \right) \exp\big(2\pi i \delta y\big) \right|^2 \tag{23.28b}$$

where $\langle b| = 011101...$ from the computational basis.

Now, if the potential error $\delta = 0$, the probability of measuring "$b = a$" is just 1.

If, instead, $\delta \neq 0$, we can ask the probability of measuring $b = a$.

$$\mathbb{P}(a) = \frac{1}{2^{2n}} \left| \sum_y \exp\big(2\pi i \delta y\big) \right|^2 \tag{23.29a}$$

$$= \frac{1}{2^{2n}} \left| \sum_y \big(\exp(2\pi i \delta)\big)^y \right|^2 \tag{23.29b}$$

$$= \frac{1}{2^{2n}} \left| \frac{1 - \alpha^{2^n}}{1 - \alpha} \right|^2 \tag{23.29c}$$

$$= \frac{1}{2^{2n}} \left| \frac{1 - \exp(2\pi i \delta)^{2^n}}{1 - \exp(2\pi i \delta)} \right|^2 \tag{23.29d}$$

$$= \frac{1}{2^{2n}} \left| \frac{\sin(\pi 2^n \delta)}{\sin(\pi \delta)} \right|^2 \tag{23.29e}$$

So, since $\forall z \in [0, 1/2] : 2z \leq \sin(\pi z) \leq \pi z$, then $\mathbb{P}a \geq 4/\pi^2 \approx 0.4$.

Actually we can achieve $\mathbb{P}(a) > 1 - \varepsilon$ with $n = l + O(\log(1/\varepsilon))$.

23.6 Eigensolver

We want to solve the Schrödinger equation

$$i\hbar \frac{\partial \psi}{\partial t} = H\psi \tag{23.30}$$

with our time evolution operator being $U(t) = \exp\left(\frac{-iHt}{\hbar}\right)$.

The eigenvalues evolve like

$$\exp\left(\frac{-iE_\alpha t}{\hbar} \right) |E_\alpha\rangle \tag{23.31}$$

This is a phase! we can apply the methods from before.

Spectroscopic method This is a classical method, implemented on a classical computer. There is no measurement involved, this is all done on a computer, our Hamiltonian is just a black box program.

Starting from any state $\big|\psi_0\big\rangle$, the eigenvalue equation is $H\phi_\alpha = E_\alpha \phi_\alpha$.

We can decompose our state like $\psi_0(x) = \sum_\alpha a_\alpha \phi_\alpha$. Then it evolves like

$$\psi_0(t) = \sum_\alpha a_\alpha \exp\left(\frac{-iE_\alpha t}{\hbar} \right) \phi_\alpha(x) \tag{23.32}$$

We can do a Fourier transform, defining $\omega_\alpha \hbar = E_\alpha$:

$$\widetilde{\psi_0}(x_0, \omega) = \int \exp(i\omega t) \sum a_\alpha \exp(-i\omega_\alpha t) \phi_\alpha(x_0) \, \mathrm{d}t \tag{23.33a}$$

$$= \sum_\alpha a_\alpha \int_0^T \exp\big(i(\omega - \omega_\alpha)t\big) \phi_\alpha(x) \, \mathrm{d}t \tag{23.33b}$$

$$\approx a_{\overline{\alpha}} \phi_{\overline{\alpha}} T + O(T^0) \tag{23.33c}$$

but this is peaked only at $\omega = \omega_{\overline{\alpha}}$ for large T. We can measure $a_{\overline{\alpha}} \phi_{\overline{\alpha}} T$ at different x positions, and find the eigenfunction at any point:

$$\phi_{\overline{\alpha}}(x_2) = \frac{\widetilde{\psi}(x_2, \omega_{\overline{\alpha}})}{\widetilde{\psi}(x_1, \omega_{\overline{\alpha}})} \phi_{\overline{\alpha}}(x_1) \tag{23.34}$$

In some cases doing this is easier than diagonalizing the Hamiltonian.

Quantizing it How to quantum-digitalize the problem? We start with a $\psi(x)$ with $x \in [-L, L]$. We can discretize the points: we divide the interval into $\Delta x = 2L/(2^n - 1)$ long steps.

Our function will then be $\psi(i) = \psi(-L + i\Delta x)$, $i \in \mathbb{N}$.

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \psi(i) |i\rangle \tag{23.35}$$

We can already see that we will have exponentially less memory usage than in the classical case.

We prepare $|\psi_0\rangle = \overline{J}$. We need our infinitesimal evolution operator $U = \exp(-iH\Delta t/\hbar)$.

Our ancilla qubits are initialized to

$$\frac{1}{\sqrt{2^n}} \sum_{J=0} |J\rangle \tag{23.36}$$

(mapping to times $0, \Delta t, 2\Delta t, \dots 2^{n-1}\Delta t$). With the same procedure as in 'Phase estimation algorithm' on page 31 we assume we have the control-U^{2^J} gates and apply them all. We get all the possible time evolutions:

$$\frac{1}{\sqrt{2^n}} \sum |J\rangle\, U^J |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum |J\rangle\, |\psi(J\Delta t)\rangle \tag{23.37a}$$

$$= \frac{1}{\sqrt{2^n}} \sum |J\rangle \sum a_\alpha \exp(-i\omega_\alpha J\Delta t)\, |\phi_\alpha\rangle \tag{23.37b}$$

We apply QFT^{-1}, measure the first registry and get a certain eigenvalue ω_α; also, we have collapsed the second registry into the corresponding wavefunction ϕ_α, which we can then measure.

This enables us to get many eigenvalues by running this several times.

24 Error mitigation

Redundancy is the key to error mitigation: if the probability of error is $\varepsilon \ll 1$, if we have a duplicate the probability they both fail is proportional to $\varepsilon^2 \ll \varepsilon$.

Classical error correction Redundancy + votation.

Alice wants to send a bit of information to Bob. To prevent mistakes, she sends three. If there is a probability ε of error, and that error happens, Bob gets two equal bits and a third different bit: so he can assume that the different bit is wrong.

We have several cases, if the sent message is 0 → 000, shown in figure 2.

Number	Received message	Probability	Failure
1	000	$(1-\varepsilon)^3$	No
2	001, 010, 100	$3\varepsilon(1-\varepsilon)^2$	No
3	011, 101, 110	$3\varepsilon^2(1-\varepsilon)$	Yes
4	111	ε^3	Yes

Figure 2: Error correction probabilities

The probability of failure is then $O(\varepsilon^2)$.

Trying to quantize it

1. We wish to do $|\psi\rangle \to |\psi\rangle |\psi\rangle |\psi\rangle$: this is not allowed; it can be done if we can prepare the state $|\psi\rangle$ (say, it is one of the base states), but we cannot do so in general.
2. We want to do a votation: but this means we have to measure it. Maybe we can do a projection?
3. For classical bits we want to correct $|0\rangle \leftrightarrow |1\rangle$, but this is not the only possibility for quantum states.

24.1 3-qubit bit-flip code

We encode

$$|0\rangle \to \left|\widetilde{0}\right\rangle = |0\rangle |0\rangle |0\rangle \tag{24.1a}$$

$$|1\rangle \to \left|\widetilde{1}\right\rangle = |1\rangle |1\rangle |1\rangle \tag{24.1b}$$

and in general do

$$|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle \to \alpha \left|\widetilde{0}\right\rangle + \beta \left|\widetilde{1}\right\rangle = \alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle \tag{24.2}$$

This can be physically made with two CNOTs.
We did not clone the state! That would have been $\big(\alpha |0\rangle + \beta |1\rangle\big)^{\otimes 3}$.

Number	Received message	Probability	Final state
1	$\alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle$	$(1-\varepsilon)^3$	$\alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle$
2	perms. of $\alpha |1\rangle |0\rangle |0\rangle + \beta |0\rangle |1\rangle |1\rangle$	$3\varepsilon(1-\varepsilon)^2$	$\alpha |0\rangle |0\rangle |0\rangle + \beta |1\rangle |1\rangle |1\rangle$
3	perms. of $\alpha |1\rangle |1\rangle |0\rangle + \beta |0\rangle |0\rangle |1\rangle$	$3\varepsilon^2(1-\varepsilon)$	$\alpha |1\rangle |1\rangle |1\rangle + \beta |0\rangle |0\rangle |0\rangle$
4	$\alpha |1\rangle |1\rangle |1\rangle + \beta |0\rangle |0\rangle |0\rangle$	ε^3	$\alpha |1\rangle |1\rangle |1\rangle + \beta |0\rangle |0\rangle |0\rangle$

Figure 3: Error correction probabilities for the quantum version

We can do the correction by measuring correlations, without doing a projective measurement: $x_0 = \left\langle \sigma_z^1 \sigma_z^2 \right\rangle$, $x_1 = \left\langle \sigma_z^1 \sigma_z^3 \right\rangle$.

These can be measured by introducing two ancillary qubits and applying a CNOT to them: for example, to measure $\sigma_z^1 \sigma_z^2$ we apply two CNOTs to the first ancillary qubit, first controlling on 1, then controlling on 2: in the end, we have four different possibilities for $|x_0 x_1\rangle$: so, we measure these along the computational basis and apply to the main qubits a gate, selected according to table 4.

$x_0 x_1$	operation
00	$\mathbb{1}$
01	σ_x^3
10	σ_x^2
11	σ_x^1

Figure 4: Error correction protocol

We also get $x_0 x_1 = 00$ for the case where all the bits are flipped, but it is all right since it is $O(\varepsilon^3)$.

24.2 3-qubit phase-flip code

What if our error is a phase flip instead of a bit flip? Something like that could be caused by an unknown magnetic field making our state rotate, like $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$. This can be corrected with a Hadamard gate, and then applying the 3 qubit-flip code.

24.3 9-qubit Shor code

To account for all kinds of (unitary) errors, we can use

$$|0\rangle \to \left|\widetilde{0}\right\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)^{\otimes 3} \tag{24.3a}$$

$$|1\rangle \to \left|\widetilde{1}\right\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)^{\otimes 3} \tag{24.3b}$$

This of course is very resource-heavy.

Experts think we should be able to achieve fault-free computation with $\varepsilon \sim 10^{-3\div 4}$.

Example We have an error like $|0\rangle \to |0\rangle$, $|1\rangle \to \exp(i\varphi)\,|1\rangle$.

We encode 1 of these qubits with two qubits, like $|01\rangle \equiv |0\rangle$ and $|10\rangle \equiv |1\rangle$: now these both take a phase of $\exp(i\varphi)$: we moved to a smaller subspace which is invariant under this transformation.

25 Time-dependent perturbation theory

We have an atom or some quantum system, and we manipulate it by sending an EM pulse against it. How will it change?

Say we have some discrete energy levels, and a continuous spectrum after some threshold energy. The photon can excite the ground state $|i\rangle$ to some excited state $|f\rangle$, or vice versa. This can happen between discrete energies, or with the continuous energies.

We need to solve the time-dep Schrödinger equation:

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} |\psi(t)\rangle = \left[H_0 + \lambda W(t)\right] |\psi(t)\rangle \tag{25.1}$$

We work with the unperturbed eigenstates $H_0 |\varphi_n\rangle = E_n |\varphi_n\rangle$, we assume $\lambda \ll 1$, and we say that the starting state at $t = 0$ is an unperturbed eigenstate.

What is the probability of getting a state f?

$$\mathbb{P}_{if}(t) = \left|\left\langle \varphi_f \middle| \psi(t) \right\rangle\right|^2 \tag{25.2}$$

we can get resonance. For continuous states this changes a bit but we can generalize.

We expand

$$|\psi(t)\rangle = \sum c_n(t) |\varphi_n\rangle \qquad c_n(t) = \langle \varphi_n | \psi(t) \rangle \tag{25.3}$$

We can compute the matrix elements of the perturbation: $\langle \varphi_n | W(t) | \varphi_k \rangle = W_{nk}(t)$ and of the Hamiltonian: $\langle \varphi_n | H_0 | \varphi_k \rangle = \delta_{nk} E_n$. Putting these in the Schrödinger equation, we get

$$i\hbar \frac{\mathrm{d}}{\mathrm{d}t} c_n(t) = E_n c_n(t) + \sum_k \lambda W_{nk} c_k(t) \tag{25.4}$$

We go in interaction picture: $b_n(t) = c_n(t) \exp(+iE_n t/\hbar)$, which nullifies the unperturbed evolution. Putting this inside the equation we get

$$i\hbar \dot{b}_n(t) = \lambda \sum_k \exp(i\omega_{nk} t) W_{nk} b_k(t) \tag{25.5}$$

with $\omega_{nk} = (E_n - E_k)/\hbar$. We can expand the $b_n(t)$ in λ:

$$b_n(t) = \sum_i b_n^{(i)} \lambda^i(t) \tag{25.6}$$

We know that for some i we must have $b_n^{(r)}(t = 0) = \delta_{ni}\delta_{r0}$ since we assume the system starts in an eigenstate i of the unperturbed Hamiltonian.

$$
\begin{aligned}
i\hbar\dot{b}_n^{(0)}(t) &= 0 \qquad (25.7)\\
i\hbar\dot{b}_n^{(r)}(t) &= \sum_k \exp(i\omega_{nk}t)W_{nk}b_n^{r-1}(t) \qquad (25.8)
\end{aligned}
$$

Then to order λ^1 we only have one term in the sum:

$$
i\hbar\dot{b}_n(t) = \exp(i\omega_{ni}t)W_{ni}(t) \tag{25.9}
$$

or, in integral form:

$$
b_n^{(1)}(t) = \frac{1}{i\hbar}\int^t \mathrm{d}\tau \exp(i\omega_{ni}\tau)W_{ni}(\tau) \tag{25.10}
$$

So $\mathbb{P}_{if}(t) = \left|c_f(t)\right|^2 = \left|b_f(t)\right|^2$

$$
\mathbb{P}_{if}(t) = \frac{\lambda^2}{\hbar^2}\left|\int^t \mathrm{d}\tau \exp\left(i\omega_{fi}\tau\right)W_{gi}(\tau)\right|^2 \tag{25.11}
$$

Example Let us take a $W(t) = -W\sin(\omega t)[t \geq 0]$. Then, up to a phase the following sequence of equalities holds:

$$
\begin{aligned}
b_n^{(1)}(t) &= -\frac{W_{ni}}{2i\hbar}\int_0^t \mathrm{d}\tau \left(\exp\left(i(\omega_{ni}+\omega)\tau\right) - \exp\left(i(\omega_{ni}-\omega)\tau\right)\right) \qquad (25.12a)\\
&= -\frac{W_{ni}}{2i\hbar}\left[\cancelto{0}{\frac{e^{i(\omega_{if}+\omega)t}-1}{i(\omega_{if}+\omega)}} - \frac{e^{i(\omega_{if}-\omega)t}-1}{i(\omega_{if}-\omega)}\right] \qquad (25.12b)\\
&= +\frac{W_{ni}}{2i\hbar}\left[\frac{e^{i(\Delta\omega)t/2} - e^{-i(\Delta\omega)t/2}}{i(\Delta\omega)}\right] \qquad (25.12c)\\
&= +\frac{W_{ni}}{2\hbar}\frac{\sin(\Delta\omega t/2)}{\Delta\omega/2} \qquad (25.12d)
\end{aligned}
$$

So,

$$
\mathbb{P}_{if}(t,\omega) = \frac{\left|W_{if}\right|^2}{4\hbar^2}F(t,\omega-\omega_{fi}) \tag{25.13}
$$

where

$$
F(\omega,t) = \left(\frac{\sin(\omega t/2)}{\omega/2}\right)^2 \tag{25.14}
$$

This is a sinc squared.

25.1 Fermi's golden rule

Is applying what we saw to continuous spectrums. Now we have some states described by eigenvalues α, with $\left\langle\alpha\middle|\alpha'\right\rangle = \delta(\alpha-\alpha')$. We want to see what is the probability of the final state being in a neighbourhood of α.

We define the state density by $\mathrm{d}\alpha = \rho(\beta,E)\,\mathrm{d}\beta\,\mathrm{d}E$ where the index β takes account of the degeneracy, which can be continuous, while E is the energy.

The probability of the final being in a neighbourhood D_f is given by:

$$
\delta\mathbb{P}\left(\alpha_f,t\right) = \int \mathrm{d}\alpha\left|\left\langle\alpha\middle|\psi(t)\right\rangle\right|^2[\alpha\in D_f] \tag{25.15}
$$

So, we can change variable into

$$
\delta\mathbb{P}\left(\alpha_f,t\right) = \int \left|\left\langle\beta,E\middle|\psi(t)\right\rangle\right|^2\rho(E,\beta)\,\mathrm{d}E\,\mathrm{d}\beta \tag{25.16}
$$

Sinusoidal perturbation We can express the transition probability density in the form of (25.13):

$$\left|\left\langle \beta, E \middle| \psi(t) \right\rangle\right|^2 = \frac{\left|\left\langle \beta, E \right| W \left| \varphi_i \right\rangle\right|^2}{\hbar^2} F\left(t, \frac{E - E_i}{\hbar}\right) \tag{25.17}$$

Let us integrate wrt energy in the $t \to \infty$ limit:

$$\int \mathrm{d}E\, F = \int \mathrm{d}E\, \frac{\sin^2(\Delta\omega t/2)}{(\Delta\omega t/2)^2} t^2 \tag{25.18}$$

we change variable, using $\mathrm{d}E = \mathrm{d}\Delta E = \hbar\, \mathrm{d}\Delta\omega$ we will integrate wrt $x = \Delta\omega t/2$:

$$\int \mathrm{d}E\, \frac{\sin^2(\Delta\omega t/2)}{(\Delta\omega t/2)^2} t^2 = \int \mathrm{d}x\, \frac{\sin^2(x)}{x^2} t^2 \frac{2\hbar}{t} \tag{25.19a}$$

$$= 2\hbar t \pi \tag{25.19b}$$

So, we know the integral of F. Now, since we are going to integrate it anyway, to simplify calculations we will assume it looks like $\lim_{t\to\infty} F(t, \Delta\omega) = ht\delta(\Delta E)$. Note that this ΔE is *not* the difference between the initial and final energies, but corresponds to the difference between the excitation energy $\omega\hbar$ and the difference between the final and initial energies.

We can substitute in:

$$\delta\mathbb{P}(\varphi_i, \alpha_f, t) = \delta\beta_f \frac{2\pi t}{\hbar} \left|\left\langle \beta_f, E_f \right| W \left| \varphi_i \right\rangle\right|^2 \rho(\beta, E_f)\delta(\Delta E) \tag{25.20}$$

Then we express this more explicitly, and insert a ± to account for the possibility of stimulated *emission* instead of *absorption*. Since $\mathbb{P}$ depends linearly on t, we compute the *rate* of emission.

$$W(\varphi_i, \alpha_f) = \frac{1}{t}\frac{\delta\mathbb{P}}{\delta\beta} = \frac{2\pi}{\hbar} \left|\left\langle \beta_f, E_f = E_i \pm \hbar\omega \right| W \left| \varphi_i \right\rangle\right|^2 \rho(\beta_f, E_f = E_i \pm \hbar\omega) \tag{25.21}$$

The more states we have in the final configuration, the greater the probability. We are assuming here that the state density is constant in the degeneracy, and we can split the degeneracy and energy contributions.

Constant perturbation The formula we get is similar, but the energies are equal in the initial and final state:

$$W(\varphi_i, \alpha_f) = \frac{2\pi}{\hbar} \left|\left\langle \beta_f, E_f = E_i \right| W \left| \varphi_i \right\rangle\right|^2 \rho(\beta_f, E_f = E_i) \tag{25.22}$$

26 How to build a quantum computer

Di Vincenzo criteria (2000): what is needed to have a true quantum computer.

1. Scalability, well defined and reproducible qubits;
2. Reset: we must be able to reset the computer surely into a state $|0\rangle$;
3. Long coherence time wrt gate duration: if our decoherence time is τ_d and our gate time is τ_g, we need $\tau_d/\tau_g \gtrsim 10^4$ in order to have time to do error correction;
4. Universal set of gates;
5. Efficient (reliable) readout;

Proposals:

- Cavity: QED;
- Solid-state electron spins;

- Cold atoms;
- Trapped ions;
- Superconductive circuits.

26.1 Trapped ions

We can trap them with electric fields, in what is called a *Pauli trap*. We cannot have a stable equilibrium in 3D with a static electric field, because of Gauss's law: the divergence would be negative there. This generalizes to magnetic fields.

We can work around it by making them time-dependent. Think of it like this: saddle which spins, an object in the saddle point will be stable if the rotation is fast enough.

We get three harmonic oscillators, with $\omega_{x,y} \gg \omega_z$. The z direction is the 'quantum' degree of freedom: the state comes from the atom state i and the oscillator state n.

Can we put many qubits in there? Our Hamiltonian will be

$$H = \sum \frac{p_i^2}{2m} + \sum \frac{1}{2}\omega_z^2 z_i^2 + \sum_i \sum_{j<i} \frac{q^2}{4\pi\varepsilon_0 \left| r_i - r_j \right|} \tag{26.1}$$

They repel each other, we can diagonalize this matrix and get the modes of oscillation.

So we have $|\alpha_1\alpha_2 \ldots \alpha_N, n\rangle$ where the n is the global oscillation. Our single qubit is $|\alpha_i, n\rangle$. We have the states $\left|g, 0\right\rangle$, $\left|g, 1\right\rangle$, $\left|g, 2\right\rangle$ ...and $|e, 0\rangle$, $|e, 1\rangle$ ...

We can use a laser to excite the ground state into a vibrational excited state... we choose the right frequency to go from $\left|g, k\right\rangle$ to $|e, k-1\rangle$ which spontaneously decays into $\left|g, k-1\right\rangle$. This is *side-band cooling*: it allows us to prepare $|0\rangle$ with $\mathbb{P} > 99.9\%$.

We can have Zeeman-like perturbations of our qubits, but it is an issue we can fix as outlined in 'Example' on page 36.

Gates Cirac-Zoller Gate: allows us to entangle states with stuff like a CPHASE by interacting with the global vibration.

26.2 Superconductive qubit

Something like Bose-condensing electrons: Cooper pairs, with opposing momentums: so the entanglement is in the Fourier space, they are very delocalized in the position space. Cooper pair currents are the superconductive currents.

We use Josephson juctions inside regular circuits: two superconductors, separated by a thin insulant. Cooper pairs can tunnel through the insulant.

Charge qubit: quantum numbers inside the superconductor are n, $\varphi = i\partial_n$, with $[n, \varphi] = i$.

$$H = E_C \left(n - n_g\right)^2 - E_J \cos\varphi \tag{26.2}$$

with $n_g = c_g V/(2e)$, and $E_C = (2e)^2/(2(C_J + C_g))$. We can write the eigenstates as $|n\rangle$, and

$$H = E_C \sum (n - n_g) |n\rangle\langle n| - \frac{1}{2} E_J \sum \left(|n+1\rangle\langle n| + |n\rangle\langle n+1|\right) \tag{26.3}$$

So, at the crossing points corresponding to $n_g \in \mathbb{N} + 1/2$ the perturbation makes it so that the parabolas do not actually cross: there is a gap, which forms the charge qubit.

27 Laboratory experiences

27.1 Photon indivisibility

We wish to prove that the photon is an indivisible particle.

Setup Our *main* experimental setup is an incoming light wave, a beamsplitter and two photodetectors on either side, labelled 1 and 2.

We call the number of times the i-th detector goes off N_i, and the amount of times two detectors go off together N_{ij}.

Parametric down-conversion We wish to get to the single-photon level: therefore, we have the laser impact a birefractive crystal which, around 10^{-6} to 10^{-8} of the times it is hit with a photon, creates a pair of coherently polarized photons.

This is because an incoming photon with energy ω can excite a resonance corresponding to the second-order term in the series expansion of the polarization with respect to the electric field strength: this will have energy 2ω and will spontaneously down-convert to a pair of photons with energy ω.

These are emitted in a state like:

$$\int_0^\pi \mathrm{d}\varphi \left|\theta_C, \varphi, V\right\rangle \otimes \left|\theta_C, \pi + \varphi, V\right\rangle \tag{27.1}$$

where the first two quantum numbers are angles denoting the direction of emission (in standard spherical coordinates, with the z axis along the direction of propagation of the photons which are not deflected), $\theta_C \sim 4°$.

So, they are emitted in pairs which form a cone. The third quantum number denotes the polarization, which is the same for the two photons.

In two antipodal positions on the cone we position the beam splitter and the entrance of a fiber optic cable; the latter should be as long as the distance between the beam splitter and the detectors. At the end of this cable we put a third detector, whose count will be called N_3.

In this way, light will reach any detector in the same time from the crystal.

Now, we want to calculate probabilities like $N_{12}/(N_1 N_2)$, but in order to have much less noise we condition all of these on the event of the third detector firing. This is since, to give an order of magnitude, one of these detectors will go off 10^6 times a second, and have a dark count (detecting nonexistent light) of something like 10^2 Hz.

So, denoting with a $|$ the conditional counts:

$$N_{12|3} = \frac{N_{123}}{N_3} \qquad N_{1|3} = \frac{N_{13}}{N_3} \qquad N_{2|3} = \frac{N_{23}}{N_3} \tag{27.2}$$

Theoretical considerations: wave vs particle We wish to put bounds on the quantity experimentally calculated as

$$g = \frac{\left\langle N_{12|3} \right\rangle}{\left\langle N_{1|3} \right\rangle \left\langle N_{2|3} \right\rangle} = \frac{\langle N_{123} \rangle}{\langle N_{13} \rangle \langle N_{23} \rangle} \langle N_3 \rangle \tag{27.3}$$

where the average is temporal. We hereafter drop the "|3" from the detection numbers, but always imply it.

Indivisible particle theory predicts that, if the photons come slow enough to be seen as "one at a time" by the detectors, $N_{12} = 0$ since the photon cannot be detected on both sides. So, $g = 0$; realistically it will be higher than 0 because of noise.

Classical wave theory predicts that the number of times the detector will go off is proportional to the intensity of the incoming light ($N_i \propto I_i$); also the light is split by the beamsplitter into two lower-intensity beams, which are constant in time, therefore the probabilities of the two detectors going off are independent: $N_{12} = N_1 N_2 \propto I_1 I_2$.

The intensity is split according to the coefficients $\mathcal{R}$, $\mathcal{T}$ with $\mathcal{R} + \mathcal{T} = 1$:

$$I = \underbrace{\mathcal{T} I}_{\text{going to detector 1}} + \underbrace{\mathcal{R} I}_{\text{going to detector 2}} \tag{27.4}$$

We can put these into the computation of g; since they are constants they can be taken out of the averages. Also, the constants in the proportionality relations between N and I simplify.

$$g = \frac{\langle \mathcal{R} I \mathcal{T} I \rangle}{\langle \mathcal{R} I \rangle \langle \mathcal{T} I \rangle} = \frac{\left\langle I^2 \right\rangle}{\langle I \rangle \langle I \rangle} \geq 1 \tag{27.5}$$

because of the Cauchy-Schwarz inequality: $\int I^2 \,\mathrm{d}t \geq \left(\int I \,\mathrm{d}t\right)^2$.

This allows us to falsify the classical wave hypothesis with results of $g < 1$.

27.2 Experimental Bell violation

We wish to violate a CHSH inequality, as theoretically explained in 'Bell Inequalities' on page 23.

In order to do it, we need an entangled state: how do we create it using birefractive crystals? We know that we can orient the crystal such that if a photon comes in with V (vertical) polarization, it can come out in a state like $|\theta, H\rangle_A \otimes |\pi + \theta, H\rangle_B$. Also, we can orient it such that if a photon comes in with H (horizontal) polarization, it can come out in a state like $|\theta, V\rangle_A \otimes |\pi + \theta, V\rangle_B$. In both cases, if the light comes in with the other polarization it just goes straight through. Also, both of these processes are coherent.

These are both separable states, but we can create entangled ones by putting two of these crystals one after another, at right angles to each other, and having the light come in at $\pi/4$ radians with respect to both. So, the state we get is:

$$\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \to \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B) \tag{27.6}$$

Half-wave plate The state of an incoming photon can be represented as $|\psi\rangle = \alpha |H\rangle + \beta |V\rangle$; then in this basis a Half-Wave Plate at an angle θ wrt the H direction operates[1] as the unitary gate

$$\text{HWP} = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ -\sin(2\theta) & \cos(2\theta) \end{bmatrix} \tag{27.7}$$

Polarizing beamsplitter It sends incoming light in two different directions depending on its polarization: it effectively is our projective measuring device.

Putting a HWP at an angle $\theta/2$ before the polarizing beam splitter we can measure along the basis at an angle θ from HV. We have two detectors corresponding to the the two directions along which the BS sends photons.

CHSH violation The basis we choose, $a_{1,2}$ and $b_{1,2}$ correspond to two pairs of angles for the Half-Wave Plates. Since our state is not a singlet, the result in (19.7c) has a plus instead of a minus, therefore our two choices for a will be the same, corresponding to $2\theta^a_{1,2} = 0, \pi/2$ but the choices for b will correspond to $2\theta^b_{1,2} = \pi/4, -\pi/4$ instead. This ensures that the only negative scalar product is the one between a_1 and b_1.

The way we measure these correlations is just counting up the result to estimate the probabilities: since the eigenvalues of the measurements are $A_i, B_j = \pm 1$:

$$\langle A \otimes B \rangle = \sum A_i B_j \mathbb{P}(A_i B_j) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}} \tag{27.8}$$

where the $+$ and $-$ subscripts indicate the result of the measurement: N_{+-} is the number of times we obtained a positive result from the measurement of the A photon and a negative one from the B photon.

Experimentally, with this setup we can obtain a value of

$$|S| = \left| \langle A \otimes B \rangle + \left\langle A \otimes B' \right\rangle + \left\langle A' \otimes B \right\rangle - \left\langle A' \otimes B' \right\rangle \right| > 2 \tag{27.9}$$

where A, A' are the bases corresponding to $\theta^a_{1,2} = 0, \pi/4$, while B, B' are the bases corresponding to $\theta^b_{1,2} = \pi/8, -\pi/8$.

28 Distances in state space

Creating convex combinations of states should always be allowed, and we see this in the fact that the space of states is convex: if we can have the state ρ_1 with probability μ and ρ_2 with probability $1 - \mu$, and both states are characterized by a Bloch vector $\vec{\lambda}_{1,2}$ then the total state will be represented by a density matrix like

$$\rho = \mu\rho_1 + (1-\mu)\rho_2 = \frac{1}{2}\mathbb{1} + \frac{1}{2}\left(\mu\vec{\lambda}_1 + (1-\mu)\vec{\lambda}_2\right) \cdot \vec{\sigma} \tag{28.1}$$

Where we can see that we get a convex combination of the Bloch vectors.

[1] See http://quantum.info/publications/theses/Robert_Prevedel_Diplomand_thesis.pdf

States are usually decomposable as probabilistic mixtures, which are convex combinations in some generalized "Bloch space".

28.1 Telling states apart

We are given two states $\rho_{1,2}$: what is the measurement which maximizes the probability we will be able to tell one from the other?

In the classical version of the problem, the two density matrices always “share an eigenbasis” — or, more simply, classical probability theory deals with probabilities of well-defined and common sets of events — so we can work with the probability vectors: $\vec{p} = (p_i)$, $\vec{q} = (q_i)$, which represent probabilities of the *same states*. We can use the "ℓ_1" metric:

$$d(p,q) = \sum_i \left| p_i - q_i \right| \tag{28.2}$$

Claim 28.1. *This is a distance.*

Proof. Symmetry and positivity are easy to see, and the triangular inequality is satisfied for any element of the sum: $\left| p_i - q_i \right| \leq \left| p_i - f_i \right| + \left| f_i - q_i \right|$ for any i. □

In general, however, $[\rho_1, \rho_2] \neq 0$ and we do not have a common eigenbasis.

Any metric defines an *evaluation* map from observables to numbers: $A \to \text{Tr}\left(\rho A\right) = \langle A \rangle_\rho$.

We can define our distance to be $\sup_A \left| \langle A \rangle_{\rho_1} - \langle A \rangle_{\rho_2} \right|$. To avoid meaningless divergences we could get by scaling the operators, we restrict ourselves to $\|A\| = 1$, where the operator norm is defined by

$$\|A\| = \sup_{\psi \neq 0} \frac{\|A\psi\|}{\|\psi\|} \tag{28.3}$$

So our distance is

$$\boxed{d = \sup_{\|A\|=1} \left| \text{Tr}\left[A(\rho_1 - \rho_2) \right] \right|} \tag{28.4}$$

We can put bounds on this norm as such:

$$\left| \text{Tr}\left(AB\right) \right| = \sum_i b_i \langle i|A|i\rangle \tag{28.5a}$$
$$\leq \sum_i |b_i| \langle i|A|i\rangle \tag{28.5b}$$
$$\leq \|A\| \sum_i |b_i| \tag{28.5c}$$
$$\leq \|A\| \, \text{Tr}\,|B| \tag{28.5d}$$

Where $B = \sum_i b_i |i\rangle\langle i|)$, and we call $\|B\|_1 = \text{Tr}\,|B|$, where the modulus of the operator can be thought of eigenvalue-wise (diagonalizing the operator, and then flipping the sign of all the negative eigenvalues).

So

$$d \leq \|A\| \left\| \rho_1 - \rho_2 \right\|_1 = \left\| \rho_1 - \rho_2 \right\|_1 \tag{28.6}$$

since $\|A\| = 1$.

Claim 28.2. *This in an equality (there* always *exists an A to do the job).*

Proof. Let us call $B = \rho_1 - \rho_2$. We wish to find an A such that $\text{Tr}(AB) = \|B\|_1$.

First we diagonalize $B = \sum_i b_i |i\rangle\langle i|$. We pick:

$$A = \sum_i (-)^{[b_i<0]} |i\rangle\langle i| \tag{28.7}$$

Then we will get

$$\operatorname{Tr}(AB) = \sum_j \langle j| \left(\sum_i (-)^{[b_i<0]} |i\rangle\langle i| \right) \left(B \sum_k b_k |k\rangle\langle k| \right) |j\rangle \tag{28.8a}$$

$$= \sum_k (-)^{[b_k<0]} b_k = \sum_k |b_k| = \|B\|_1 \tag{28.8b}$$

□

Claim 28.3. *We get back the classical case if the matrices commute.*

Proof. In that case we can just write $\rho_1 - \rho_2$ in the common eigenbasis as $\sum_i (p_{i,1} - p_{i,2}) |i\rangle\langle i|$. The result follows. □

We define $D(\rho_1, \rho_2) = \frac{1}{2} \|\rho_1 - \rho_2\|_1$, since the d we used before is upper-bounded by 2, by the triangular inequality.

Measurements Take a 2-element POVM:[1] $E_{1,2} \geq 0$ and the states from before: $\rho_{1,2}$.

Say we get the states ρ_i with 50% probability each, and we wish to select the POVM which best allows us to distinguish them and figure out which is which: we want E_i to correspond to ρ_i. Then

$$\mathbb{P}(\text{success}) = \frac{1}{2} \left[\operatorname{Tr}(E_1 \rho_1) + \operatorname{Tr}(E_2 \rho_2) \right] \tag{28.9a}$$

$$\mathbb{P}(\text{error}) = \frac{1}{2} \left[\operatorname{Tr}(E_1 \rho_2) + \operatorname{Tr}(E_2 \rho_1) \right] \tag{28.9b}$$

We want to maximize $\mathbb{P}(\text{success})$. We can rewrite it as:

$$\mathbb{P}(\text{success}) = \frac{1}{2} \left[\operatorname{Tr}(E_1 \rho_1) + \operatorname{Tr}\left((\mathbb{1} - E_1) \rho_2 \right) \right] \tag{28.10a}$$

$$= \frac{1}{2} \left[1 + \operatorname{Tr}\left(E_1 (\rho_1 - \rho_2) \right) \right] \tag{28.10b}$$

to maximize over E_1.

Claim 28.4. *The optimum* (Hellstrom optimal measurement) *is*

$$\mathbb{P}(\text{success}) = \frac{1}{2} \left[1 + \frac{1}{2} \|\rho_1 - \rho_2\|_1 \right] \tag{28.11}$$

This is 1 if they are maximally different, $1/2$ *if they are indistinguishable.*

Proof. The difference from the operator we used in (28.7) is that now we must have $E_1 \geq 0$, so it cannot have negative eigenvalues: so, we pick it to be the projection over the positive eigenvalues of the difference between the matrices.

If $\delta\rho = \rho_1 - \rho_2 = \sum_i p_i |i\rangle\langle i|$, then $E_1 = \sum_i [p_i \geq 0] |i\rangle\langle i|$.

So, the trace of $E_1 \delta\rho$ will be given by the sum of the positive eigenvalues of $\delta\rho$.

By linearity of the trace we know that $\operatorname{Tr}(\delta\rho) = 0$. Then, the sum of its positive eigenvalues must be half of the sum of all the eigenvalues' absolute values. □

[1] See 'POVMs' on page 18

Bhattacharyya distance We have two probability vectors $\vec{p} = (p_i)$, $\vec{q} = (q_i)$. We want them to be normalized in the euclidean metric, so we take the square root component by component, defining $V_p = \left(\sqrt{p_i}\right)$.

We define the distance

$$d_B(\vec{p}, \vec{q}) = \cos^{-1}(\vec{V}_p \cdot \vec{V}_q) = \cos^{-1}\left(\sum_i \sqrt{p_i q_i}\right) \tag{28.12}$$

Claim 28.5. *This is a distance.*

Proof. As usual, positivity and symmetry are easy. The triangular inequality amounts to seeing that, if we pick three points on S^n, an angle between two of them must be less than the sum of the other two angles.

This can be proven WLOG in 3D space, since we can restrict ourselves to the span of the three vectors. Then, it is a boring calculation: you write out the Gramian matrix for the euclidean scalar product, which must have a positive determinant, and the result comes from the fact that $\cos^{-1}$ is decreasing.[1] □

Quantize it! We have a POVM $\mathbb{E} = \{E_i\}$, and two probability distributions ρ and σ. We can define the probability vectors

$$P_{\rho,i} \overset{\text{def}}{=} \operatorname{Tr}(E_i \rho) \qquad P_{\sigma,i} \overset{\text{def}}{=} \operatorname{Tr}(E_i \sigma) \tag{28.13}$$

and apply the Bhattacharyya distance to them:

$$d_B(\rho, \sigma) = \sup_{\mathbb{E}} d_B\left(\vec{P}_\rho, \vec{P}_\sigma\right) \tag{28.14}$$

Claim 28.6. *In the pure state case, where $\rho = |\phi\rangle\langle\phi|$, $\sigma = |\psi\rangle\langle\psi|$:*

$$d_B(\rho, \sigma) = \cos^{-1}\left|\langle\phi|\psi\rangle\right| \tag{28.15}$$

This is the *Fubini-Study metric* over a projective Hilbert space.

Proof. Proving this is useful because it shows us techniques, tools. We wish to prove

$$\cos^{-1}\left|\langle\phi|\psi\rangle\right| = \sup_{\mathbb{E}} \cos^{-1}\left(\sum_i \sqrt{p_i^{\mathbb{E}}(\phi)}\sqrt{p_i(\psi)^{\mathbb{E}}}\right) \tag{28.16}$$

We can derive an inequality for the arguments of the arccosines:

$$\begin{aligned}
\left|\langle\phi|\psi\rangle\right| &= \left|\sum_i \langle\phi| E_i |\psi\rangle\right| &\text{(28.17a)}\\
&\leq \sum_i \left|\langle\phi| \sqrt{E_i}\sqrt{E_i} |\psi\rangle\right| &\text{(28.17b)}\\
&= \sum_i \left|\langle\hat{\phi}_i|\hat{\psi}_i\rangle\right| &\text{(28.17c)}\\
&\leq \sum_i \left\|\sqrt{E_i}\,|\phi\rangle\right\| \left\|\sqrt{E_i}\,|\psi\rangle\right\| &\text{(28.17d)}\\
&= \sum_i \sqrt{\langle\phi|E_i|\phi\rangle}\sqrt{\langle\psi|E_i|\psi\rangle} &\text{(28.17e)}\\
&= \sum_i \sqrt{p_i^{\mathbb{E}}(\phi)}\sqrt{p_i(\psi)^{\mathbb{E}}} &\text{(28.17f)}
\end{aligned}$$

so we just apply the $\cos^{-1}$ to both sides. We have the inequality, but is it actually reached? We can take

[1] See https://math.stackexchange.com/questions/1924742/prove-the-triangle-inequality-on-the-sphere-s2-in-mathbbr3/1925049

$$\mathbb{E} = \left\{ |\phi\rangle\langle\phi|\,|, \left\{ |\phi_i\rangle\langle\phi_i| \right\}\text{span } |\phi\rangle\langle\phi|^{\perp} \right\} \tag{28.18}$$

so the first term just gives us the upper bound, the other terms in the sum are 0: the inequality is saturated. We can just measure the projector associated with the state we want to know about. □

Infinitesimal distance What is the expression of our line element $\mathrm{d}s = \mathrm{d}_B(\vec{p}, \vec{p} + \mathrm{d}\vec{p})$? Recall $\sqrt{1-x} \sim 1 - x/2 - x^2/8$:

$$\cos^{-1}\left(\sum_i \sqrt{p_i(p_i + \mathrm{d}p_i)}\right) = \cos^{-1}\left(\sum_i p_i \sqrt{1 + \frac{\mathrm{d}p_i}{p_i}}\right) \tag{28.19}$$

$$\sim \cos^{-1}\left(\sum_i p_i \left(1 - \cancelto{0}{\frac{1}{2}\frac{\mathrm{d}p_i}{p_i}} - \frac{1}{8}\left(\frac{\mathrm{d}p_i}{p_i}\right)^2\right)\right) \tag{28.20}$$

since the terms proportional to $\sum_i \mathrm{d}p_i$ must vanish for the normalization to be preserved, so we have

$$\cos \mathrm{d}s = 1 - \frac{1}{8}\frac{\mathrm{d}p_i^2}{p_i} \tag{28.21}$$

but $\cos \mathrm{d}s \sim 1 - 1/2\,\mathrm{d}s_B^2$, so

$$\boxed{\mathrm{d}s_B^2 = \frac{1}{4}\sum_i \frac{(\mathrm{d}p_i)^2}{p_i}} \tag{28.22}$$

This is the *Fisher metric*.

Take some $\lambda \in \mathcal{M} = \{\text{manifold of control parameters of dimension N}\}$, such that $p_i = p_i(\lambda)$ and $\mathrm{d}p_i = \sum_\mu (\partial_\mu p_i)\,\mathrm{d}\lambda_\mu$.

Then we can write the expression for the metric directly on the parameter manifold:

$$\boxed{g_{\mu\nu} = \frac{1}{4}\sum_i \frac{(\partial_\mu p_i)(\partial_\nu p_i)}{p_i}} \tag{28.23}$$

$$\mathrm{d}s_B^2 = g_{\mu\nu}\,\mathrm{d}\lambda_\mu\,\mathrm{d}\lambda_\nu \tag{28.24}$$

Parameter estimation Take a random variable x distributed according to $p_\theta(x)$ (a one-parameter distribution, with θ as the parameter), and let Θ be an estimator for the parameter θ: then $\langle\Theta\rangle = \theta = \int p_\theta(x)\Theta(x)\,\mathrm{d}x$.

We prove a super-famous bound. Differentiate the previous equation wrt θ.

$$1 = \int p'_\theta(x)\Theta(x)\,\mathrm{d}x \tag{28.25a}$$

$$= \left\langle \frac{p'_\theta}{p_\theta} \middle| \Theta \right\rangle_p \tag{28.25b}$$

Claim 28.7. *The notation* $\langle f|g\rangle_p = \int p_\theta f g\,\mathrm{d}x$ *defines a scalar product.*

Proof. The axioms for a real scalar product are symmetry, linearity, and positive definiteness. The first two come from the properties of the regular product fg; the interesting one to prove is the third. It is true since $p_\theta \geq 0$, and then $\forall f : \int p_\theta f^2\,\mathrm{d}x \geq 0$, also (modulo equality almost everywhere) $\langle f|f\rangle = 0 \iff f = 0$. □

We can subtract θ from $\Theta \to \overline{\Theta} = \Theta - \theta$ leaving the result unchanged, since it holds for any estimator: we restrict ourselves to *zero-mean* ones. This amounts to shifting the x variable, an operation which leaves the scalar product unchanged. We do this because we will get a lower bound on the of the integral of the square of Θ, which is larger than the variance in general but equal to it in the zero mean case, so we want the tightest bound.

$$1 \leq \left\| \frac{p'_\theta}{p_\theta} \right\|_p^2 \|\Theta\|_p^2 \tag{28.26}$$

$$= \left(\int p_\theta \frac{(p'_\theta)^2}{p_\theta^2} \, \mathrm{d}x \right) \left(\int p_\theta (\Theta(x) - \theta)^2 \, \mathrm{d}x \right) \tag{28.27}$$

$$= F \mathrm{var} \Theta \tag{28.28}$$

Where F is just the Fischer metric: in this one parameter case it just has one component. There is a factor-of-four difference between this definition and the one from before: let us accept it and move on.

$$F = \int p_\theta \frac{(p'_\theta)^2}{p_\theta^2} \, \mathrm{d}x \tag{28.29}$$

This means $\boxed{\mathrm{var}\Theta \geq F^{-1}}$: this is the *Cramer-Rao* inequality.

Quantize it! We would like to repeat the procedure from before, and to express the derivative of $\mathrm{Tr}(\rho_\theta \hat{\Theta}) = \theta$ as the trace of ρ times *something*, but it is difficult: we could do $\mathrm{Tr}(\rho_\theta \rho_\theta^{-1} \rho'_\theta \hat{\Theta}) = 1$, but the derivative and the inverse of ρ do not commute!

So, we define the *Symmetric Logarithmic Derivative*: there is a single solution L to the differential equation

$$\frac{1}{2} (\rho L + L\rho) = \rho' \tag{28.30}$$

and we call L the SLD operator. It can be easily seen that this L satisfies $\mathrm{Tr}(\rho L) = \langle L \rangle = 0$. The name comes from the regular logarithmic derivative $\rho'/\rho = \mathrm{d} \log \rho / \mathrm{d}x$.

Now we can sobstitute in the expression for ρ':

$$\frac{1}{2} \mathrm{Tr} \left[(\rho L + L\rho) \bar{\Theta} \right] = \mathrm{Re} \, \mathrm{Tr}(\rho L \bar{\Theta}) \tag{28.31}$$

Where we separated the two parts by linearity, and to express them both in terms of $\rho L \bar{\Theta}$ we took the adjunct of the second and applied the trace cyclic identity. Now we can take this equation in absolute value:

$$1 \leq \left| \mathrm{Tr}(\rho L \bar{\Theta}) \right|^2 = \left| \left\langle L \bar{\Theta} \right\rangle_\rho \right|^2 \tag{28.32}$$

And like before we can use the Cauchy-Schwarz inequality wrt the inner product defined by: $\langle a, b \rangle_\rho = \mathrm{Tr}(\rho a b)$.

$$\boxed{1 \leq \|L\|_\rho^2 \|\bar{\Theta}\|_\rho^2 = \mathrm{Tr}(\rho L^2) Tr(\rho (\bar{\Theta} - \theta)^2)} \tag{28.33}$$

so then $\mathrm{var}\bar{\Theta} \geq 1/F_Q$ if we define $F_Q = \mathrm{Tr}(\rho L^2)$.

Claim 28.8. *Take $\rho = \sum_i p_i |i\rangle\langle i|$, then $L_{ij} = 2 \langle i| \rho' |j\rangle / \left(p_i + p_j \right)$.*

Proof. We take the components of $1/2(\rho L + L\rho) = \rho'$ in the eigenbasis of ρ:

$$\frac{1}{2} \langle i| \left(\rho L + L\rho \right) |j\rangle = \langle i| \rho' |j\rangle \tag{28.34a}$$

$$\langle i| \rho L |j\rangle + \langle i| L\rho |j\rangle = 2 \langle i| \rho' |j\rangle \tag{28.34b}$$

$$p_i \langle i| L |j\rangle + p_j \langle i| L |j\rangle = 2 \langle i| \rho' |j\rangle \tag{28.34c}$$

from which the result follows. □

So we can compute

$$F_Q = \mathrm{Tr}(\rho L^2) = \sum_i p_i \langle i|L^2|i\rangle \tag{28.35a}$$

$$= \sum_{ij} p_i \langle i| L |j\rangle\langle j| L |i\rangle \tag{28.35b}$$

$$= \sum_{ij} p_i \frac{2}{p_i + p_j} \langle i| \rho' |j\rangle\langle j| \rho' |i\rangle \frac{2}{p_i + p_j} \tag{28.35c}$$

$$= 4 \sum_{ij} p_i \frac{\left|\langle i| \rho' |j\rangle\right|^2}{(p_i + p_j)^2} \tag{28.35d}$$

$$= 2 \sum_{ij} \frac{\left|\langle i| \rho' |j\rangle\right|^2}{p_i + p_j} \tag{28.35e}$$

Step (28.35e) is justified because the identity is satisfied pair-by-pair by the summands:

$$4\left(p_i \frac{\left|\langle i| \rho' |j\rangle\right|^2}{(p_i + p_j)^2} + p_j \frac{\left|\langle j| \rho' |i\rangle\right|^2}{(p_i + p_j)^2} \right) = 2\left(\frac{\left|\langle i| \rho' |j\rangle\right|^2}{p_i + p_j} + \frac{\left|\langle j| \rho' |i\rangle\right|^2}{p_j + p_i} \right) \tag{28.36a}$$

$$2\left(p_i \frac{1}{(p_i + p_j)^2} + p_j \frac{1}{(p_i + p_j)^2} \right) = \frac{1}{p_i + p_j} + \frac{1}{p_j + p_i} \tag{28.36b}$$

This is Quantum Fischer. It really is the result of *classical* optimization over all the possible POVMs $\mathbb{E}$. The denominator diverges! We can do something if our ρ is pure, though.

Fischer information for pure states Take $\rho_\theta = |\psi_\theta\rangle\langle\psi_\theta|$ gound-eigenstate of a many-body system. Then:

Claim 28.9. *We can calculate* $F_Q = \mathrm{Tr}\left(\rho(\rho')^2\right)$*, which comes out to be:*

$$F_Q^{pure} \propto \left\langle \psi'_\theta \middle| \psi'_\theta \right\rangle - \left| \left\langle \psi'_\theta \middle| \psi_\theta \right\rangle \right|^2 \tag{28.37}$$

where $\psi' = \partial_\theta \psi$.[1]

Proof. Call $\rho = |\psi\rangle\langle\psi|$. Then $\rho^2 = \rho$, we can differentiate it and get $\rho'\rho + \rho\rho' = \rho'$: so, in the pure state case, the solution L to the Lyapunov equation is just $\rho' = L/2$.

The derivative of ρ is $\rho' = |\psi\rangle\langle\psi'| + |\psi'\rangle\langle\psi|$. We also know, by differentiating $1 = \langle\psi|\psi\rangle$, that $\langle\psi|\psi'\rangle = -\langle\psi'|\psi\rangle$. Therefore $\langle\psi|\psi'\rangle = s$ is purely imaginary,

$$s = -s^* \tag{28.38}$$

We compute $\mathrm{Tr}(\rho\rho'\rho') = {}^1\!/\!_4 F_Q$ (in a basis consisting of $|\psi\rangle$ and other perpendicular vectors, whose contribution is null because of the first term ρ) we get:

$$\mathrm{Tr}(\rho\rho'\rho') = \langle\psi| \left(\Big|\psi\Big\rangle\Big\langle\psi'\Big| + \Big|\psi'\Big\rangle\Big\langle\psi\Big| \right)^2 |\psi\rangle \tag{28.39a}$$

$$= \cancelto{1}{\langle\psi|\psi\rangle} \left\langle \psi' \middle| \psi \right\rangle \left\langle \psi' \middle| \psi \right\rangle + \cancelto{1}{\langle\psi|\psi\rangle} \left\langle \psi' \middle| \psi' \right\rangle \cancelto{1}{\langle\psi|\psi\rangle}$$

[1] $|\psi'\rangle$ is not a normalized wavefunction in general!

$$
\begin{aligned}
&+ \left\langle \psi \middle| \psi' \right\rangle \cancelto{1}{\langle \psi | \psi \rangle} \left\langle \psi' \middle| \psi \right\rangle + \left\langle \psi \middle| \psi' \right\rangle \left\langle \psi \middle| \psi' \right\rangle \cancelto{1}{\langle \psi | \psi \rangle} && \text{(28.39b)}\\
&= \left\langle \psi' \middle| \psi \right\rangle^2 + \left\langle \psi' \middle| \psi' \right\rangle + \left\langle \psi \middle| \psi' \right\rangle \left\langle \psi' \middle| \psi \right\rangle + \left\langle \psi \middle| \psi' \right\rangle^2 && \text{(28.39c)}\\
&= \left\langle \psi' \middle| \psi' \right\rangle + s^2 + (-s)^2 + s(-s) && \text{(28.39d)}\\
&= \left\langle \psi' \middle| \psi' \right\rangle + s^2 && \text{(28.39e)}\\
&= \left\langle \psi' \middle| \psi' \right\rangle - \left| \left\langle \psi \middle| \psi' \right\rangle \right|^2 && \text{(28.39f)}
\end{aligned}
$$

since s^2 must be real and negative.

□

28.2 Quantum Fischer metric

We found:

$$F_Q \propto \sum_{ij=1}^{d} \frac{\left| \langle i | \rho' | j \rangle \right|^2}{p_i + p_j} = \sup_{\mathbb{E}} F_{\text{class}} \tag{28.40}$$

with $F_{\text{class}} = \int \mathrm{d}x \, {}^{(p')^2}/_{p}$

We did not prove this! How is F_Q the sup of F_{class}?

If $\rho = |\psi\rangle\langle\psi|$ is pure, we found

$$
\begin{aligned}
F^Q_{\text{pure}} \propto \langle \psi | L^2 | \psi \rangle &= \left\langle \psi' \middle| \psi' \right\rangle - \left| \left\langle \psi \middle| \psi' \right\rangle \right|^2 && \text{(28.41a)}\\
&= \left\| \left| \psi' \right\rangle \right\| - \left| \left\langle \psi \middle| \psi' \right\rangle \right|^2 = \left\| \left| \psi'_\perp \right\rangle \right\|^2 && \text{(28.41b)}
\end{aligned}
$$

with $\left|\psi'_\perp\right\rangle = (1 - |\psi\rangle\langle\psi|) \left|\psi'\right\rangle$.

We can get the Fisher information in the pure state case from the Fubini-Study metric as well: recall equation (28.15): it defines a metric on the projective space $\mathcal{PH}$.

We call the scalar product $\mathcal{F} = \left| \langle \psi | \phi \rangle \right|$ which appears as the argument of the arccosine *Fidelity*.

Let us consider two infinitesimally close states, $\phi = \psi + \Delta\psi(\lambda)$ depending on some near-zero parameter λ, consider their Fubini-Study distance by (28.15) and invert the arccosine:

$$\cos \mathrm{d}_{FS} = \left| \langle \psi | \psi + \Delta\psi \rangle \right| \tag{28.42}$$

We can expand this to second order around $\mathrm{d}s \sim 0$, denoting differentiation wrt λ with primes:

$$1 - \frac{1}{2}\mathrm{d}s^2 = \left| \left\langle \psi \middle| \psi + \psi' d\lambda + \frac{1}{2}\psi'' d\lambda^2 \right\rangle \right| \tag{28.43}$$

And expand the scalar product by linearity:

$$1 - \frac{1}{2}\mathrm{d}s^2 = \left| \underbrace{\langle \psi | \psi \rangle}_{=1} + \left\langle \psi \middle| \psi' \right\rangle \mathrm{d}\lambda + \frac{1}{2} \left\langle \psi \middle| \psi'' \right\rangle \mathrm{d}\lambda^2 \right| \tag{28.44}$$

Recalling equation (28.38) and differentiating twice we get:

$$\left\langle \psi \middle| \psi' \right\rangle + \left\langle \psi' \middle| \psi \right\rangle = 0 \xRightarrow{\partial/\partial\lambda} \left\langle \psi' \middle| \psi' \right\rangle + \left\langle \psi \middle| \psi'' \right\rangle + \left\langle \psi'' \middle| \psi \right\rangle + \left\langle \psi' \middle| \psi' \right\rangle = 0 \tag{28.45}$$

which we can rearrange into:

$$\underbrace{\left\langle \psi \middle| \psi'' \right\rangle + \left\langle \psi'' \middle| \psi \right\rangle}_{2\,\mathrm{Re}\left\langle \psi \middle| \psi'' \right\rangle} = -2 \left\langle \psi' \middle| \psi' \right\rangle \tag{28.46a}$$

$$\mathrm{Re} \left\langle \psi \middle| \psi'' \right\rangle + \left\langle \psi' \middle| \psi' \right\rangle = 0 \tag{28.46b}$$

Now we can expand the absolute value in (28.44), which will equal the sum of the squares of the real and imaginary parts. Keeping only the terms of order $\mathrm{d}\lambda^2$ or less (that means we can discard the imaginary part of $\left\langle \psi \middle| \psi'' \right\rangle$) we get:

$$1 - \frac{\mathrm{d}s^2}{2} = \sqrt{\left(1 + \frac{1}{2}\,\mathrm{Re}\,\langle \psi | \psi'' \rangle\right)^2 + \left|\langle \psi | \psi' \rangle\right|^2 d\lambda^2 + O(\mathrm{d}\lambda^3)} \tag{28.47a}$$

$$\sim \sqrt{\left(1 - \frac{1}{2}\,\langle \psi' | \psi' \rangle\,\mathrm{d}\lambda^2\right)^2 + \left|\langle \psi | \psi' \rangle\right|^2 \mathrm{d}\lambda^2} \tag{28.47b}$$

$$\sim \sqrt{1 - \langle \psi' | \psi' \rangle\,\mathrm{d}\lambda^2 + \left|\langle \psi | \psi' \rangle\right|^2 \mathrm{d}\lambda^2} \tag{28.47c}$$

$$\sim 1 - \frac{1}{2}\left(\left\langle \psi' \middle| \psi' \right\rangle + \left|\left\langle \psi \middle| \psi' \right\rangle\right|^2\right) \mathrm{d}\lambda^2 \tag{28.47d}$$

Therefore we have found the expression for the **Quantum Fisher Metric** in the $\dim\left[\mathrm{supp}\,\rho\right] = 1$ case:

$$\mathrm{d}s^2 = \left(\left\langle \psi' \middle| \psi' \right\rangle + \left|\left\langle \psi \middle| \psi' \right\rangle\right|^2\right) \mathrm{d}\lambda^2 = F_Q^{\text{pure}}\,\mathrm{d}\lambda^2 \tag{28.48}$$

Now, we have assumed λ to be our control parameter belonging to a smooth manifold: if $\psi = \psi(\lambda)$ is the Ground State of a hamiltonian $H(\lambda)$ we have a map like: $\lambda \to H(\lambda) \to$ Ground State .

What does $\mathbb{P}H$ mean?

So, we can look at this as a perturbative problem: $H(\lambda) = H_0 + \lambda V$.
We remember the perturbative expression

$$\left|\widetilde{\psi}_0\right\rangle = |\psi_0\rangle + \lambda \left|\psi_0^{(1)}\right\rangle + O(\lambda^2) \tag{28.49}$$

where

$$\lambda \left|\psi_0^{(1)}\right\rangle = \lambda \sum_{n>0} \frac{\left|\psi_n^{(0)}\right\rangle \left\langle \psi_n^{(0)}\right| V \left|\psi_0^{(0)}\right\rangle}{E_n^{(0)} - E_0^{(0)}} \perp |\psi_0\rangle \tag{28.50}$$

and $H_0 \left|\psi_n\right\rangle = E_n \left|\psi_n\right\rangle$. Since this is a first-order expression in λ the derivative wrt λ is just the sum.
With this, we can get a new formula for the metric. We write $\mathrm{d}H = V\mathrm{d}\lambda$. Now, in the expression for the Fisher Metric the term $\langle \psi_0 | \psi_0' \rangle = 0$. So:

$$\mathrm{d}s^2 = \left\|\left|\psi_0'\right\rangle\right\|^2 \mathrm{d}\lambda^2 = \sum_{n>0} \frac{\left|\langle \psi_n | \,\mathrm{d}H\, | \psi_0 \rangle\right|^2}{(E_n - E_0)^2} \tag{28.51}$$

This is different from regular second order perturbation theory because of the square in the denominator. It is the Fubini-Study metric pulled back over the parameter manifold.

We want to do the "GR thing". We have a pseudorimannian parameter manifold, and the divergences of the metric are where the interesting physics happens: if the metric is large, some very close events are distinguishable by a very large measurement.

If the first excited state is very close to the ground state, which happens in quantum phase transitions, we have a blow-up of the metric. Let us call the difference in energy between the first excited state and the ground state Δ. We look at the thermodinamical limit, where the system size $N \to \infty$.

$$\lim_{N\to\infty} \Delta_N(\lambda) \begin{cases} > 0\colon & \text{Gapped} \\ = 0\colon & \text{Gap-less: a Quantum controlled Phase Transition} \end{cases} \tag{28.52}$$

Claim 28.10. *A* gapped *system with a Hamiltonian $H(\lambda)$ parametrized by $\lambda \in M$ has a metric which is is at most extensive: for some c we have* ($\mathrm{d}s^2 \leq cN = O(N)$)*.*

From this it follows that if $\mathrm{d}s^2 = N^\alpha$ with $\alpha > 1$ the system is gapless.

Proof. We start by writing out the metric component $g_{\lambda\lambda}$, and we bound it from above using the gapped system hypothesis:

$$\begin{aligned} g_{\lambda\lambda} = \frac{\mathrm{d}s^2}{\mathrm{d}\lambda^2} &= \sum_{n>0} \frac{\left|\langle\psi_n|\, V\, |\psi_0\rangle\right|^2}{(E_n - E_0)^2} && \text{(28.53a)} \\ &\leq \frac{1}{\Delta^2} \sum_{n>0} \left|\langle\psi_n|\, V\, |\psi_0\rangle\right|^2 && \text{(28.53b)} \\ &= \frac{1}{\Delta^2} \langle\psi_0|\, V \underbrace{\left(\sum_{n>0} |\psi_n\rangle\!\langle\psi_n|\right)}_{\mathbb{1}-|\psi_0\rangle\langle\psi_0|} V\, |\psi_0\rangle && \text{(28.53c)} \\ &= \frac{1}{\Delta^2}\left(\langle\psi_0|V^2|\psi_0\rangle - \left|\langle\psi_0|V|\psi_0\rangle\right|^2 \right) && \text{(28.53d)} \\ &= \frac{G(V)}{\Delta^2} && \text{(28.53e)} \end{aligned}$$

and if we consider a local perturbation Hamiltonian $V = \sum_j V_j$, where j runs over the particles in the system we get $G_{ij} = \left\langle V_i V_j \right\rangle - \langle V_i\rangle \left\langle V_j \right\rangle$. We are interested in the contribution of the whole system, $\sum_{ij} G_{ij}$. Under hypotheses of translational invarance this can be written as a sum of N correlation terms, since the element G_{ij} only depends on the difference between i and j:

$$\sum_{ij} G_{ij} = \sum_i \sum_k \langle V_i V_{i+k}\rangle - \langle V_i\rangle \langle V_{i+k}\rangle = N \sum_k G(k) \tag{28.54}$$

where N is the number of particles. So,

$$\left(\frac{\mathrm{d}s}{\mathrm{d}\lambda}\right)^2 \leq \frac{1}{\Delta^2} N \sum_k G(k) \tag{28.55}$$

but it is known that for gapped systems G decays eponentially; so

$$\left(\frac{\mathrm{d}s}{\mathrm{d}\lambda}\right)^2 \leq \frac{1}{\Delta^2} N \sum_k \exp\left(-\frac{k}{\text{something}}\right) \tag{28.56}$$

the point is that the sum of these those exponentials is no more than constant wrt N, so it can be bounded:

$$\left(\frac{\mathrm{d}s}{\mathrm{d}\lambda}\right)^2 \leq \frac{1}{\Delta^2} N \widetilde{C} \tag{28.57}$$

which proves the theorem: $\mathrm{d}s^2 / N$ is bounded in the thermodinamic limit. □

How do these bounds change if we perform a differentiable reparametrization from $H(\lambda) \to H(\widetilde{\lambda})$?

We can slightly rewrite equation (28.51) as

$$\left(\frac{\mathrm{d}s}{\mathrm{d}\lambda}\right)^2 = \sum_{n>0} \frac{\left|\langle\psi_n|\,\partial_\lambda H\,|\psi_0\rangle\right|^2}{(E_n - E_0)^2} \overset{\text{def}}{=} \chi_F \tag{28.58}$$

where we define χ_F, the fidelity susceptibility.

$$F = \left|\langle\psi_0(\lambda)|\psi_0(\lambda + \mathrm{d}\lambda)\rangle\right| \tag{28.59a}$$

$$\sim 1 - \frac{1}{2}\,\mathrm{d}\lambda^2\,\chi_F + \dots \tag{28.59b}$$

$$\sim \exp\left(-\frac{1}{2}\,\mathrm{d}\lambda^2\,\chi_F(\lambda) + \dots\right) \tag{28.59c}$$

So, χ_F can be calculated as

$$\chi_F = \lim_{\Delta\lambda\to 0} \frac{-2\log F}{\Delta\lambda^2} \tag{28.60}$$

We found $\chi_F \leq c\xi^d N/\Delta^2$ where ξ is the correlation length, d is the number of dimensions and $\Delta = \min_{n>0} E_n - E_0$, for a gapped and local Hamiltonian (short-range).

In the general, multi-paramter case, our metric is

$$g_{\mu\nu} = \sum_{n>0} \frac{\left|\langle\psi_0|\,\partial_\mu H\,|\psi_n\rangle\,\langle\psi_n|\,\partial_\nu H\,|\psi_0\rangle\right|}{(E_n - E_0)^2} \tag{28.61}$$

We could do $g_{\mu\nu} \to g'_{\mu\nu}$: this will be linear, and this will not change the N dependence of χ_F unless we do crazy things.

Gap-less Hamiltonians We have $\chi_F = O(N^\alpha)$ with $\alpha > 1$.

If we look at F against λ we see something which is roughly equal to 1 almost everywhere, but has a sharp decrease corresponding to $\lambda \sim \lambda^*$. As N increases, the decrease gets sharper and sharper, up to a singularity for $N \to \infty$.

28.3 XY model

i labels our spin 1/2 particles, $\mathcal{H}_N \simeq \left(\mathbb{C}^2\right)^{\otimes N}$

$$H_{xy} = -\frac{1}{2}\left(\sum_{i=1}^{N} \frac{1+\gamma}{2}\sigma_i^x\sigma_{i+1}^x + \frac{1-\gamma}{2}\sigma_i^y\sigma_{i+1}^y - h\sigma_i^z\right) \tag{28.62}$$

So our parameter is $\vec{\lambda} = (\gamma, h)$. γ is the anisotropy parameter, differentiating the x and y directions, while h is the magnetic field along the z direction.

The hamiltonian (28.62) is exactly solvable, using fermionic operators and second quantization. We try to do this in a way that is understandable.

We introduce the operators

$$c_i^\dagger = \left(\prod_{l<i}\sigma_l^z\right)\sigma_i^+ \tag{28.63}$$

$$c_i = \left(\prod_{l<i}\sigma_l^z\right)\sigma_i^- \tag{28.64}$$

Where $\sigma^+ = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $\sigma^- = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

These are fermionic operators, which (**Claim**) satisfy the CAR (Commutation Anticommutation Relations) relations [Jordan-Wigner]

$$\left\{c_i, c_j^\dagger\right\} = \delta_{ij} \tag{28.65a}$$

$$\left\{c_i, c_j\right\} = \left\{c_i^\dagger, c_j^\dagger\right\} = 0 \tag{28.65b}$$

We can define the occupation number $n_i = c_i^\dagger c_i = \sigma_i^+ \sigma_i^- = \left(\mathbb{1} + \sigma_i^z\right)/2$: this is 0 if the spin is $-$, and 1 if it is $+$.

So we moved from spin degrees of freedom to fermionic degrees of freedom. We define the kets $|\alpha_1 \alpha_2 \dots \alpha_N\rangle$ and map them to $|n_1 n_2 \dots n_N\rangle$, where $\alpha_i = \pm 1$ are the spin eigenvalues while $n_i = 0, 1$ are the occupation eigenvalues.

We want to invert this relation (**exercise**). Doing this, the Hamiltonian gets simpler. Going to the Fourier space makes it even simpler, if we add periodic boundary conditions, since then we get translational invariance.

$$\widetilde{c_k} = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} \exp\left(\frac{i2\pi kj}{N}\right) c_j \qquad k = 0, \dots, N-1 \tag{28.66}$$

Claim 28.11. *This is a canonical transformation, the commutation relations stay the same (CAR) for the $\widetilde{c_k}$.*

Then, we can show that the Hamiltonian (28.62) becomes:

$$H_{xy} = \sum_k \left(\varepsilon_k \widetilde{c_k}^\dagger \widetilde{c_k} - i\gamma \sin(2\pi k/N) \left(\widetilde{c}_{-k}^\dagger \widetilde{c_k}^\dagger - \widetilde{c}_{-k} c_k\right)\right) \tag{28.67}$$

with $\varepsilon_k = h - \cos(2\pi k/N)$.

So, the sequence is: spin dof → (JW) Fermi dof → (FT) Fermi dof → (Bogoliubov) reciprocal lattice ground state energy.

$$H_{xy} = \sum_k \Lambda_k \Omega_k^\dagger \Omega_k + \vec{E_0} \tag{28.68}$$

Where the Ω is the new set of fermionic modes, $n_k = \Omega_k^\dagger \Omega_k$, $[n_k, n_{k'}] = 0$. The spectrum then is

$$\sigma(H_{xy}) = \left\{\sum_k \Lambda_k n_k + E_0 : n_k = 0, 1\right\} \tag{28.69}$$

while the

$$\Lambda_k = \sqrt{\left(h - \cos(2\pi k/N)\right)^2 + \gamma^2 \sin^2\left(2\pi k/N\right)} \tag{28.70}$$

It can be shown that $[H_{xy}, \Omega_k] = -\Lambda_k \Omega_k$ and $[H_{xy}, \Omega_k^\dagger] = \Lambda_k \Omega_k^\dagger$, and for the ground state $\Omega_k |\psi_0\rangle = 0$.

So it is like the harmonic oscillator: any eigenstate $|\psi\rangle$ can be formed like

$$|\psi\rangle = \Omega_{k_1}^\dagger \Omega_{k_2}^\dagger \dots \Omega_{k_N}^\dagger |\psi_0\rangle \tag{28.71}$$

and then its energy can be found by equation (28.69).

Then we can see that the gap is given by $\Delta = \min_k \Lambda_k$, since the E_0 is a constant added to all the terms.

$$\Delta = \min_k \sqrt{\left(h - \cos(2\pi k/N)\right)^2 + \gamma^2 \sin^2\left(2\pi k/N\right)} \tag{28.72}$$

can this get arbitrarily small?

We can do a contour plot, over the plane h, γ. We have three critical lines at $h = \pm 1$ and $\gamma = 0$ (as long as $N \to \infty$).

If $|h| < 1$, we have a ferromagnet aligned with the x or y; if $|h| > 1$ instead we have a paramagnet.

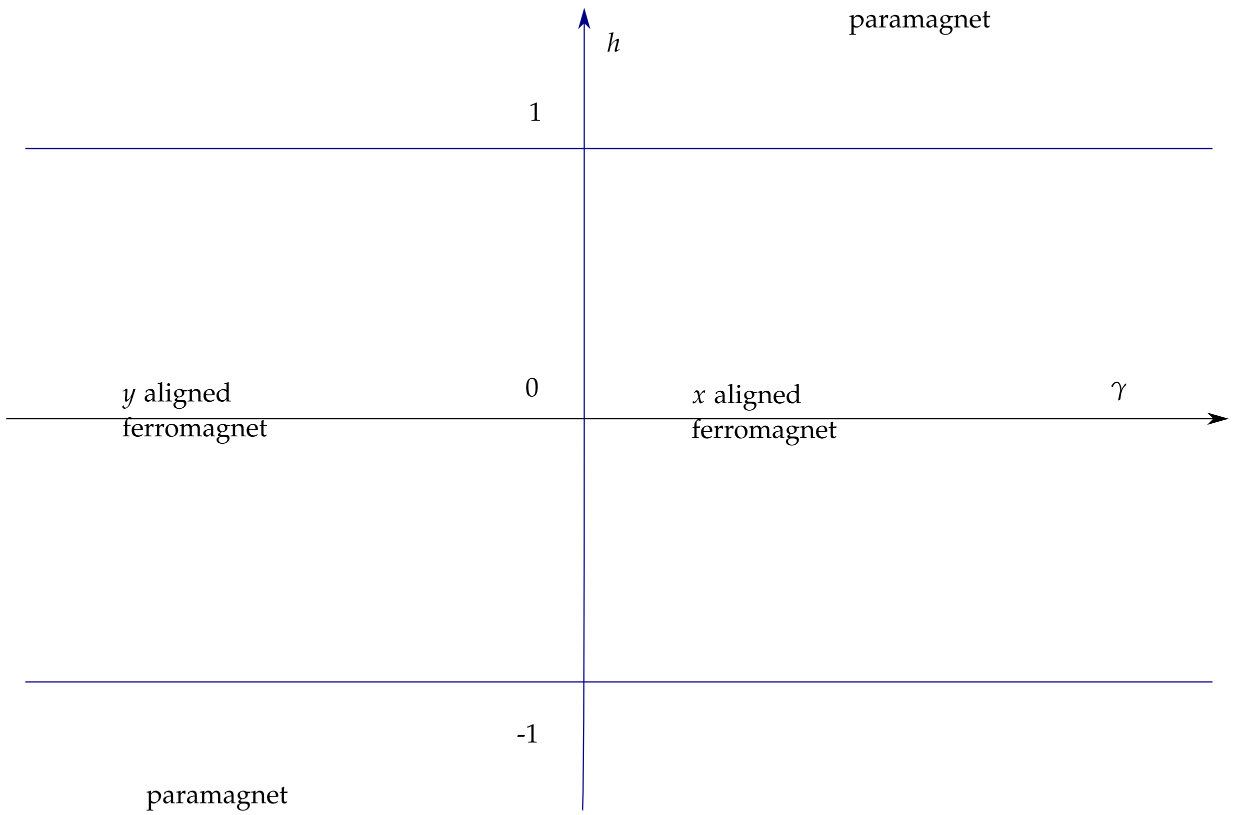

Figure 5: XY model.

There is a coupling between k and $-k$.
The ground state will be

$$\bigotimes_{k>0}\left(\cos\frac{\theta_k}{2}\left|00\right\rangle_{k,-k} - i\sin\frac{\theta_k}{2}\left|11\right\rangle_{k,-k}\right) \tag{28.73}$$

where

$$\theta_k = \tan^{-1}\left(\frac{\gamma\sin(2\pi k/N)}{h-\cos(2\pi k/N)}\right) \tag{28.74}$$

Now, we move in the parameter space and see how the fidelity looks like.

$$F = \left|\left\langle\psi_0(\lambda)\middle|\psi_0(\lambda')\right\rangle\right| = \prod_k\left|\cos\left(\frac{\theta_k-\theta_k'}{2}\right)\right| \tag{28.75}$$

If $\Delta_k\theta \sim 0$ this becomes

$$F \sim \prod_k\left(1-\frac{1}{2}\left(\frac{\Delta\theta_k}{2}\right)^2\right) = \dots \tag{28.76}$$

We look at the scaling of the metric element g_{hh}, that is, we look at the distance between the eigenstates of Hamiltonians between which we change h while leaving γ constant. Let us use the shorthands $S = \sin(2\pi k/N)$ and $C = \cos(2\pi k/N)$.

We will calculate it using equation (28.60):

$$-2\log F \sim -2\sum_k \log\left(1-\frac{1}{2}\left(\frac{\Delta\theta_k}{2}\right)^2\right) \sim \sum_k \left(\frac{\Delta\theta_k}{2}\right)^2 \tag{28.77}$$

So we get for our matrix element, modulo some factors of 2:

$$\mathrm{d}s^2 = \frac{1}{2}\sum_k \left(\frac{\partial\theta_k}{\partial h}\right)^2 \mathrm{d}h^2 \tag{28.78a}$$

$$\left(\frac{\mathrm{d}s}{\mathrm{d}h}\right)^2 = \frac{1}{2}\sum_k \left(\frac{\frac{-\gamma S}{(h-C)^2}}{1+\left(\frac{\gamma S}{h-C}\right)^2}\right)^2 \tag{28.78b}$$

$$= \sum_k \left(\frac{\gamma S}{(h-C)^2+(\gamma S)^2}\right)^2 \tag{28.78c}$$

We can replace the sums with integrals as $N \to \infty$. We now call $\widetilde{k} = 2\pi k/N$.

$$\chi_F \to \frac{N\gamma}{2\pi}\int_0^\pi \mathrm{d}\widetilde{k}\left[\frac{\sin\left(\widetilde{k}\right)}{\left(h-\cos\left(\widetilde{k}\right)\right)^2+\gamma^2\sin^2(\widetilde{k})}\right]^2 \tag{28.79}$$

If there are no singularities, then this is of order N. Let us consider the case $h = 1$, as $\widetilde{k} \to 0$ we get something of the order

$$\frac{N}{\gamma^2 2\pi}\int_{k_{\mathrm{min}}}^{\pi} \frac{\mathrm{d}\widetilde{k}}{\widetilde{k}^2} \tag{28.80}$$

this diverges for $k_{\mathrm{min}} \to 0$, but k_{min} cannot be smaller than $2\pi/N$ (this was an implicit condition on our sums from before): then the leading term becomes

$$\chi_F(h=1) \sim \frac{N^2}{(2\pi\gamma)^2} \tag{28.81}$$

The many-body wavefunction is much more organized (there is a lot of entanglement), and close states are very distinguishable.