

Topological Quantum Computation

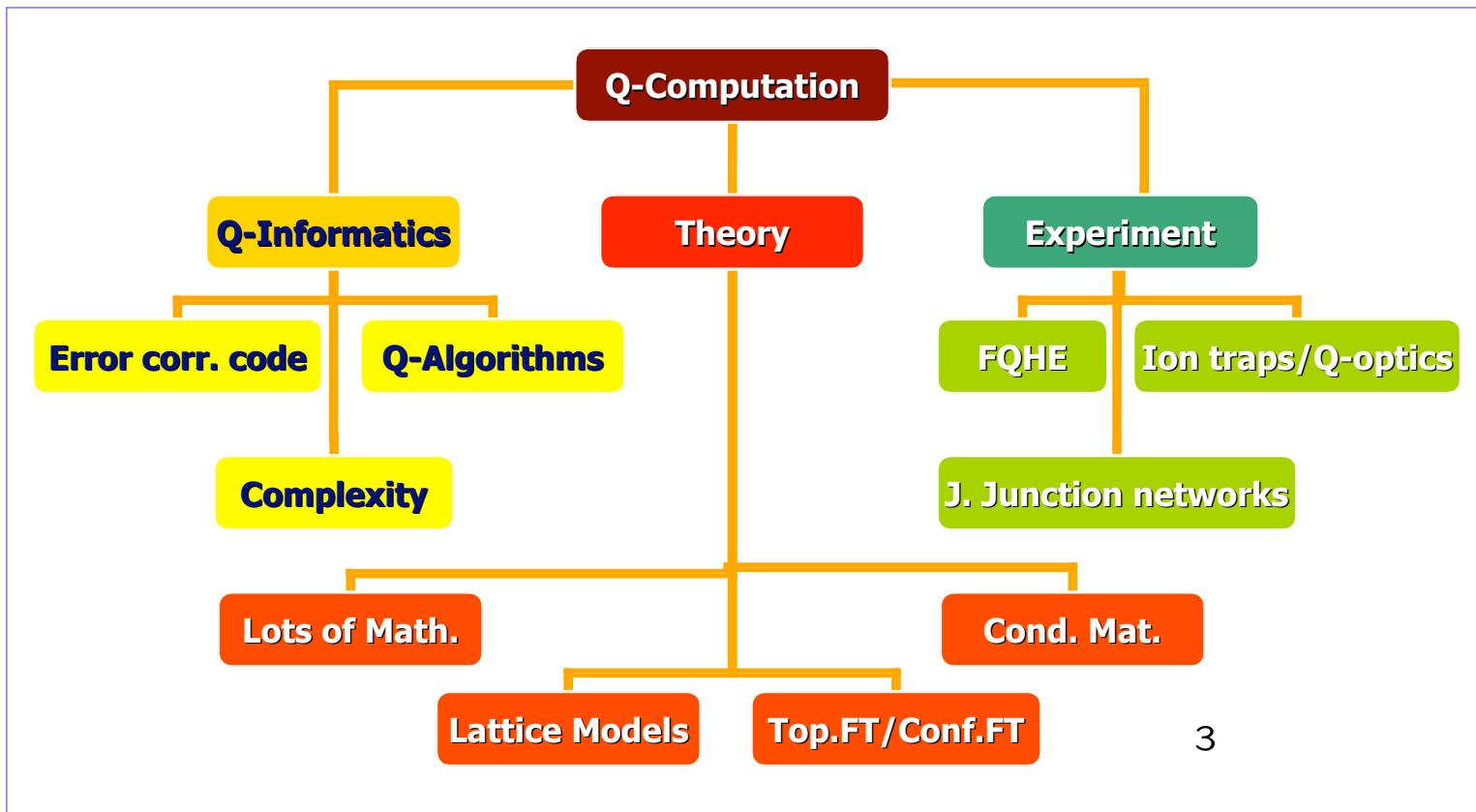
Sander Bais
Institute for Theoretical Physics
University of Amsterdam

November 26, 2007



”Until recently, most people thought of quantum mechanics in terms of the uncertainty principle and unavoidable limitations on measurement. Einstein and Schrödinger understood early on the importance of entanglement, but most people failed to notice, thinking of the EPR paradox as a question for philosophers. The appreciation of the positive application of quantum effects to information processing grew slowly.”

Nicolas Gisin



Outline: 5 lectures

1. Quantum information
2. Anyons and topological order
3. Topological quantum computation
4. The Quantum Hall Effect

Some references

- FAB and J.D. Farmer, *The Physics of Information*, arXiv:0708.2837
- M. de Wild Propitius and FAB, *Discrete Gauge Theories*, arXiv:hep-th9511201
- S. Das Sarma, M. Freedman, C. Nayak, S.H. Simon and A. Stern, *Non-abelian Anyons and Topological Quantum Computation*, arXiv:0707.1989

Textbook on QC:

- M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University press, 1990

Quantum information

- Quantum generalities
- Qubits
- Measurement
- Separable vs Entangled and Pure versus Mixed states
- Density matrix and Von Neuman entropy
- No cloning
- Teleportation
- Quantum computation

Promises and expectations...

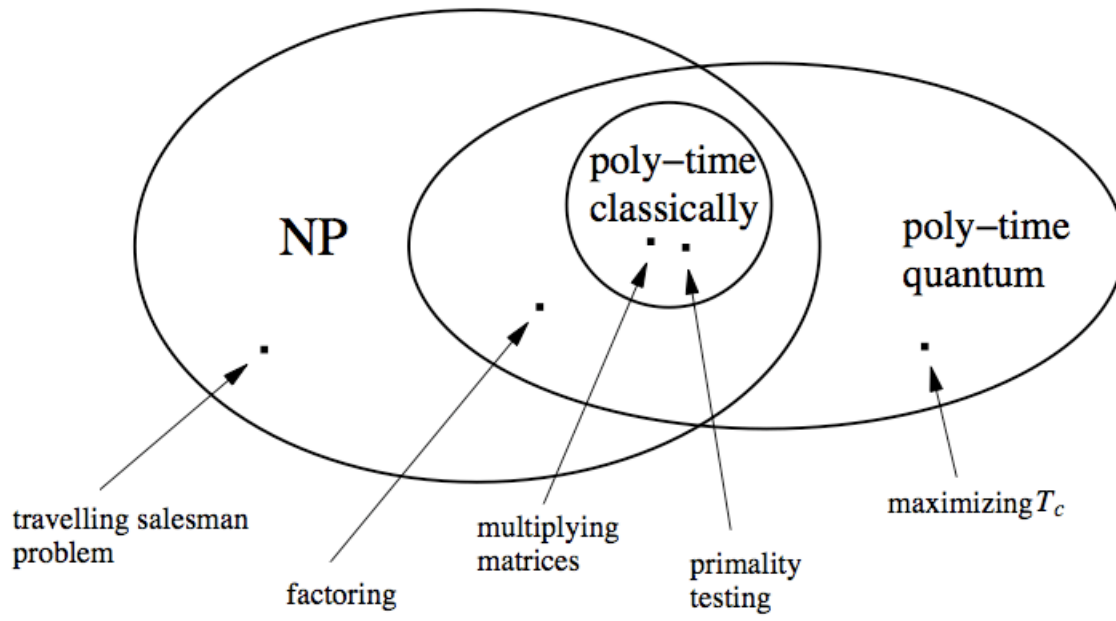
Why cannot we write the entire 24 volumes of the Encyclopedia Britannica on the head of a pin?

R.P. Feynman (1959)

- In our quest for more volume and speed in storing and processing information we are led to the smallest scales we can physically manipulate. Currently commercially available processors work at scales of 60 nm. In 2006, IBM announced circuitry on a 30 nm scale, which indeed makes it possible to write the Encyclopedia Britannica on the head of a pin. To see how close this is to the atomic scale: a square with sides of length 30 nm contains about 1000 atoms.

- Under the historical pattern of Moore's law, integrated circuitry halves in size every 2 years. If we continue on the same trajectory of improvement, within about 20 years the components will be the size of individual atoms, and it is difficult to imagine that computers will be able to get any smaller.
- There is a certain poetry to this: Once a computer has components on a quantum scale, the motion of its atoms will no longer be random, and in a certain sense will not be described by classical statistical mechanics, at the same time that it will be used to process information on a macroscopic scale.

Computational complexity (conjectural)



Polynomial versus exponential

Suppose an elementary computational step takes Δt seconds. If the number of steps increases exponentially, factorizing a number with N digits will take $\Delta t \exp(aN)$ seconds, where a is a constant that depends on the details of the algorithm. For example, if $\Delta t = 10^{-6}$ and $a = 10^{-2}$, factorizing a number with $N = 10,000$ digits will take 10^{37} seconds, which is much, much longer than the lifetime of the universe (which is a mere 4.6×10^{17} seconds). In contrast, if the number of steps scales as the third power of the number of digits, the same computation takes $a' \Delta t N^3$ seconds, which with $a' = 10^{-2}$, is 10^4 seconds or a little under three hours. Of course the constants a , a' and Δt are implementation dependent, but because of the dramatic difference between exponential vs. polynomial scaling, for sufficiently large N there is always a fundamental difference in speed.

The qubit

The state of a qubit is described by a wavefunction or state vector $|\psi\rangle$, which can be written as

$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \text{ with } |\alpha|^2 + |\beta|^2 = 1.$$

$|\psi\rangle$ is a normalized vector in the 2-dimensional complex "ket" space, denoted \mathbf{C}^2 , and we can represent the state as a column vector

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

The dual vector or "bra" space in \mathbb{C}^2 can be represented as row vectors or alternatively be written

$$\langle \psi | = \langle 0 | \alpha^* + \langle 1 | \beta^* .$$

This allows us to define the inner product between two state vectors $|\psi\rangle$ and $|\phi\rangle = \gamma|1\rangle + \delta|0\rangle$ as

$$\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^* = \gamma^* \alpha + \delta^* \beta .$$

The constraint $|\alpha|^2 + |\beta|^2 = 1$ says that the state vector has unit length: it defines the complex unit circle in \mathbf{C}^2 .

In terms of real and imaginary parts

$$\alpha = a_1 + ia_2 \text{ and } \beta = b_1 + ib_2$$

we have

$$|a_1 + a_2i|^2 + |b_1 + b_2i|^2 = a_1^2 + a_2^2 + b_1^2 + b_2^2 = 1.$$

The geometry of the space described by the latter equation is just the three dimensional unit sphere S^3 embedded in a four dimensional Euclidean space, \mathbf{R}^4 .

Each additional state (or configuration) in the classical system yields an additional orthogonal dimension (complex parameter) in the quantum system. Hence a finite state classical system will lead to a finite dimensional complex vector space for the corresponding quantum system.

Any two level quantum system can potentially be considered as a qubit. It is not surprising that many alternative realisations are investigated: Quantum computation has become the Holy Grail of condensed matter physics, quantum optics etc.

Many qubits

The mathematical space in which the n qubits live is the tensor product of the individual qubit spaces:

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}.$$

For example, the Hilbert space for two qubits is $\mathbb{C}^2 \otimes \mathbb{C}^2$. This is a four dimensional complex vector space spanned by the vectors $|1\rangle \otimes |1\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|0\rangle \otimes |0\rangle$.

For convenience we will often abbreviate the tensor product by omitting the tensor product symbols, or by simply listing the spins. For example

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle.$$

The tensor product of two qubits with wave functions $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ and $|\phi\rangle = \gamma|1\rangle + \delta|0\rangle$ is

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = \alpha\gamma|11\rangle + \gamma\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|00\rangle.$$

The tensor product is that it is multi-linear:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |\psi\rangle = \alpha|0\rangle \otimes |\psi\rangle + \beta|1\rangle \otimes |\psi\rangle.$$

Again we emphasize that whereas the classical n -bit system has 2^n states, the n -qubit system corresponds to a vector of unit length in a 2^n dimensional complex space, with twice as many degrees of freedom. For example a three-qubit can be expanded as:

$$|\psi\rangle = \alpha_1|000\rangle + \alpha_2|001\rangle + \alpha_3|010\rangle + \alpha_4|011\rangle \\ + \alpha_5|100\rangle + \alpha_6|101\rangle + \alpha_7|110\rangle + \alpha_8|111\rangle$$

Sometimes it is convenient to denote the state vector by the column vector of its components $\alpha_1, \alpha_2, \dots, \alpha_{2^n}$.

Observables

In the quantum formalism observables are defined as *hermitian* operators acting on the state space. In quantum mechanics an *operator* is a linear transformation that maps one state into another, which providing the state space is finite dimensional, can be represented by a matrix. A hermitian operator or matrix satisfies the condition $A = A^\dagger$, where $A^\dagger = (A^{tr})^*$ is the complex conjugate of the transpose of A .

The physical observables are the components of the spin along the x , y or z directions, which are by convention written $s_x = \frac{1}{2}\sigma_x$, $s_y = \frac{1}{2}\sigma_y$, etc.

The operators σ_i are the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

\Rightarrow Observables are in general *noncommuting!*

Time evolution

The time evolution of the system is governed by the Schrödinger equation:

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle.$$

This is a linear differential equation expressing the property that the time evolution of a quantum system is generated by its energy operator. Assuming that H is constant, given an initial state $|\psi(0)\rangle$ the solution is simply

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \text{ with } U(t) = e^{-iHt/\hbar}.$$

The time evolution is *unitary*, meaning that the operator $U(t)$ satisfies $UU^\dagger = 1$.

$$\begin{aligned} U^\dagger &= \exp(-iHt/\hbar)^\dagger = \\ &= \exp(iH^\dagger t/\hbar) = \exp(iHt/\hbar) = U^{-1}. \end{aligned}$$

A unitary transformation indeed preserves the norm, so time evolution moves the wavefunction around on the unit circle (three sphere).

A single qubit example

For the simple example of a single qubit, suppose the initial state is

$$|\psi(0)\rangle = \sqrt{\frac{1}{2}}(|1\rangle + |0\rangle) \equiv \sqrt{\frac{1}{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Consider the energy of a spin in a magnetic field B directed along the positive z -axis*.

*Quantum spins necessarily have a magnetic moment, so in addition to carrying angular momentum they also interact with a magnetic field.

In this case H is given by $H = B s_z$, so

$$U(t) = \exp\left(\frac{-iBt}{2\hbar}\sigma_z\right) = \begin{pmatrix} \exp(-iBt/2\hbar) & 0 \\ 0 & \exp(iBt/2\hbar) \end{pmatrix}.$$

Leading to an oscillatory time dependence for the state, i.e.

$$\begin{aligned} |\psi(t)\rangle &= \sqrt{\frac{1}{2}} \begin{pmatrix} e^{-iBt/2\hbar} \\ e^{iBt/2\hbar} \end{pmatrix} \\ &= \sqrt{\frac{1}{2}} \left[\cos\frac{Bt}{2\hbar} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + i \sin\frac{Bt}{2\hbar} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right]. \end{aligned}$$

\Rightarrow Interactions can be used to manipulate quantum information.

Measurements

In general the probability of finding the system in a given state in a measurement is computed by first expanding the given state $|\psi\rangle$ into the eigenstates $|\chi_k\rangle$ of the matrix A corresponding to the observable, i.e.

$$|\psi\rangle = \sum_k \alpha_k |\chi_k\rangle \quad \text{where} \quad \alpha_k = \langle \chi_k | \psi \rangle. \quad (1)$$

The probability of measuring the system in the state corresponding to eigenvalue λ_k is $p_k = |\alpha_k|^2$.

Labelling of states

As the operators A_i are in general not commuting, so the outcome of a sequence of measurements depends on the order in which the measurements of operators that do not commute, are performed. There are maximal subsets of mutually commuting operators these can be measured simultaneously. These sets of operators can be used to label a basis for the Hilbertspace of the system.

Probabilistic nature of measurement

We see that the predictions of quantum mechanics are probabilistic but the theory is essentially different from classical probability theory.

On the one hand it is clear that a given operator defines a probability measure on Hilbert space, however as the operators are non-commuting (like matrices) one is dealing with a non-commutative probability theory. It is the non-commutativity of observables that gives rise to the intricacies in the quantum theory of measurement.

Collaps of the wavefunction

The act of measurement influences the state of the system. If we measure $s_x = +\frac{1}{2}$ and then measure it again immediately afterward, we will get the same value with certainty. Doing the measurement forces the system into the eigenstate $|\chi_+\rangle$, and in the absence of further interactions, it stays there. This strange property of measurement, in which the wavefunction *collapses* onto the observed eigenstate, was originally added to the theory in an ad hoc manner, and is called the *projection postulate*.

Projection postulate

This postulate introduces a rather arbitrary element into the theory that appears to be inconsistent: The system evolves under quantum mechanics according to the Schrödinger equation until a measurement is made, at which point some kind of magic associated with the classical measurement apparatus takes place, which lies completely outside the rest of the theory.

Feynman (Lectures III):

"We would like to emphasize a very important difference between classical and quantum mechanics. We have been talking about the probability that the electron will arrive in a given circumstance. We have implied that in an experimental arrangement (even in the best possible one) it would be impossible to predict exactly what would happen. We can only predict the odds! This would mean, if it were true, that physics has given up on the problem of trying to predict exactly what will happen in a given circumstance. Yes! Physics has given up. We do not know how to predict what would happen in a given circumstance, and we believe now that it is impossible that the only thing that can be predicted is the probability of different events. It must be recognized that this is a retrenchment in our earlier ideal of understanding nature. It may be a backward step, but no one has seen a way to avoid it."

Classical versus quantum

- Note that a measurement does not allow one to completely determine the state. A complete measurement of the two-qubit system yields at most two classical bits of information, whereas determining the full quantum state requires knowing seven real numbers (four complex numbers subject to a normalization condition).
- In this sense one cannot just say that a quantum state "contains" much more information than its classical counterpart. In fact

strictly speaking one is only able by making simultaneous measurements to extract less information than from the corresponding classical system, due to the non-commutativity of the observables. In conclusion one may say that there are two ways to talk about quantum theory.

- If one insists that it is a theory of a single system, then one has to live with the fact that it only predicts the probability of things to happen and as such is a retrenchment from the ideal of classical physics.

- Alternatively one may claim that quantum theory is only a theory that applies to ensembles of particles. To measure the actual probability distributions one has to make many measurements on "identically prepared" quantum systems.
- In this perspective one has to compare the dimensionality of Hilbert space with that of classical distributions over the classical phase space, which makes the difference far less dramatic.

Beyond quantum theory?

For some this raises the quest for a theory underlying quantum mechanics which applies to a single system.

However, so far nobody has succeeded in providing clues to what such a theory would look like however, in the contrary, attempts to build such theories on the concept of "hidden variables" have failed, in view of the observed violations of the Bell inequalities.

Multi qubit pure states

Quantum mechanically qubits can be coupled in subtle ways that produce consequences for measurement that are very different from classical bits. Understanding this has proved to be important for the problems of computation and information transmission. To explain this we need to introduce the opposing concepts of *separability* and *entanglement*, which describe whether measurements on different qubits are statistically independent or statistically dependent.

Separable states

An n -qubit state is *separable* if it can be factored into n -single qubit states. An example of a separable two-qubit is

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle). \end{aligned}$$

If an n -qubit state is separable then measurements on individual qubits are statistically independent

Measuring on a separable state

For the separable state, measuring the first spin "up", transforms the wave function as

$$\begin{aligned} & \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \rightarrow \\ & \rightarrow \frac{1}{\sqrt{2}}(|1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle). \end{aligned}$$

Now measuring the second spin, the probability of finding spin up or spin down is still 50%. The first measurement has no effect on the second measurement.

Entangled states

An n -qubit state is *entangled* if it is not separable. An example of an entangled two-qubit state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (2)$$

which cannot be factored into a single product. For entangled states measurements on individual qubits depend on each other.

Measuring on an entangled state

A similar experiment on the entangled state with observing spin "up" in the first measurement, transforms the wave function as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \longrightarrow |11\rangle. \quad (3)$$

(Disappearance of $1/\sqrt{2}$ due to normalization). Measuring the second spin we find spin up! For the entangled example above the successive measurements are 100% correlated.

Mixed states

Consider a mixed state in which there is a probability p_i for the system to have wavefunction ψ_i and an observable characterized by operator A . The average value measured for the observable (also called its expectation value) is

$$\langle A \rangle = \sum_i p_i \langle \psi_i | A | \psi_i \rangle. \quad (4)$$

We can expand each wavefunction ψ_i in terms of a basis $|\chi_j\rangle$ in the form

$$|\psi_i\rangle = \sum_j \langle \chi_j | \psi_i \rangle |\chi_j\rangle,$$

where in our earlier notation $\langle \chi_j | \psi_i \rangle = \alpha_j^{(i)}$. Substituting into (4) and interchanging the order of summation yields:

$$\begin{aligned} \langle A \rangle &= \sum_{j,k} \left(\sum_i p_i \langle \chi_j | \psi_i \rangle \langle \psi_i | \chi_k \rangle \right) \langle \chi_k | A | \chi_j \rangle \\ &= \sum_{j,k} \langle \chi_j | \rho | \chi_k \rangle \langle \chi_k | A | \chi_j \rangle \\ &= \text{tr}(\rho A), \end{aligned}$$

where ρ is the *density matrix*.

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|, \text{ with } \text{tr}(\rho) = 1 \quad (5)$$

Density matrix

The *density matrix* or *operator* ρ is defined as:

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|, \text{ with } \text{tr}(\rho) = 1$$

- Because the trace $\text{tr}(\rho A)$ is independent of the representation this can be evaluated in any convenient basis, and so provides an easy way to compute expectations.
- For a pure state $p_i = 1$ for some value of i and $p_i = 0$ otherwise.
- Time evolution: $i\partial\rho/\partial t = [H, \rho]$

Examples

- Let $\psi = \psi_1 = |1\rangle$. This is a pure state and the density matrix is just

$$\rho = |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

The expectation of the spin along the z -axis is $\text{tr}(\rho s_z) = 1/2$.

- If the system is in a mixed state (beam of electrons)

$$\rho = \frac{1}{2} (|1\rangle\langle 1| + |0\rangle\langle 0|) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In this case the expectation of the spin along the z -axis is $\text{tr}(\rho s_z) = 0$.

- Another example:

$$\rho = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)$$
$$\xRightarrow{\text{diag.}} \frac{1}{2} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Indeed a pure state: $|\psi\rangle = \sqrt{\frac{1}{2}}(|0\rangle + |1\rangle)$.

Von Neuman entropy

Von Neumann defined the entropy of a quantum state in analogy with the Gibbs entropy for a classical ensemble as

$$S(\rho) = -\text{tr } \rho \log \rho = -\sum_i p_i \log p_i . \quad (6)$$

The entropy of a quantum state provides a quantitative measure of “how mixed” a system is. The entropy of a pure state is equal to zero, whereas the entropy of a mixed state is greater than zero, if maximally mixed then $p_i = 1/d$ and $S = \log d$.

Partial measurements and traces

- In some situations there is a close relationship between entangled and mixed states. An entangled but pure state in a high dimensional multi-qubit space can appear to be a mixed state when viewed from the point of view of a lower dimensional state space. The view of the wavefunction from a lower dimensional subspace is formally taken using a *partial* trace. This is done by summing over all the coordinates associated with the subspaces we want to ignore.

- Consider the entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and trace it with respect to the second qubit. To do this we make use of the fact that $\text{tr}(|\psi\rangle\langle\phi|) = \langle\psi|\phi\rangle$. We get

$$\begin{aligned}
 & \text{tr} (|\psi_{AB}\rangle\langle\psi_{AB}|) \\
 &= \frac{1}{2} \text{tr} (|1\rangle_A\langle 1|_B + |0\rangle_A\langle 0|_B) (\langle 0|_B\langle 0|_A + \langle 1|_B\langle 1|_A) \\
 &= \frac{1}{2} (|1\rangle_A\langle 1|_A\langle 1|_1\rangle_B + |0\rangle_A\langle 0|_A\langle 0|_0\rangle_B) \\
 &= \frac{1}{2} (|1\rangle_A\langle 1|_A + |0\rangle_A\langle 0|_A)
 \end{aligned}$$

\Rightarrow mixed state (for the first qubit) with probability 1/2 to be either spin up or spin down.

- The corresponding entropy is also higher: In base two $S = -\log(1/2) = 1$ bit, while for the original pure state $S = \log 1 = 0$. In general if we begin with a statistically pure separable state and perform a partial trace we will still have a pure state, but if we begin with an entangled state, when we perform a partial trace we will get a mixed state. In the former case the entropy remains zero, but in the latter case it increases.

Thus the von Neumann entropy yields a useful measure of entanglement.

The No-cloning theorem

Given an arbitrary state $|\psi_1\rangle$ on one qubit and some particular state $|\phi\rangle$ on another, there is no quantum device $[A]$ such that,

$$[A] : |\psi_1\rangle \otimes |\phi\rangle \rightarrow |\psi_1\rangle \otimes |\psi_1\rangle.$$

Let U_A be the unitary operator representing the device $[A]$, then

$$|\psi_1\rangle|\psi_1\rangle = U_A|\psi_1\rangle|\phi\rangle$$

For a cloning device this property has to hold for any other state $|\psi_2\rangle$, i.e.

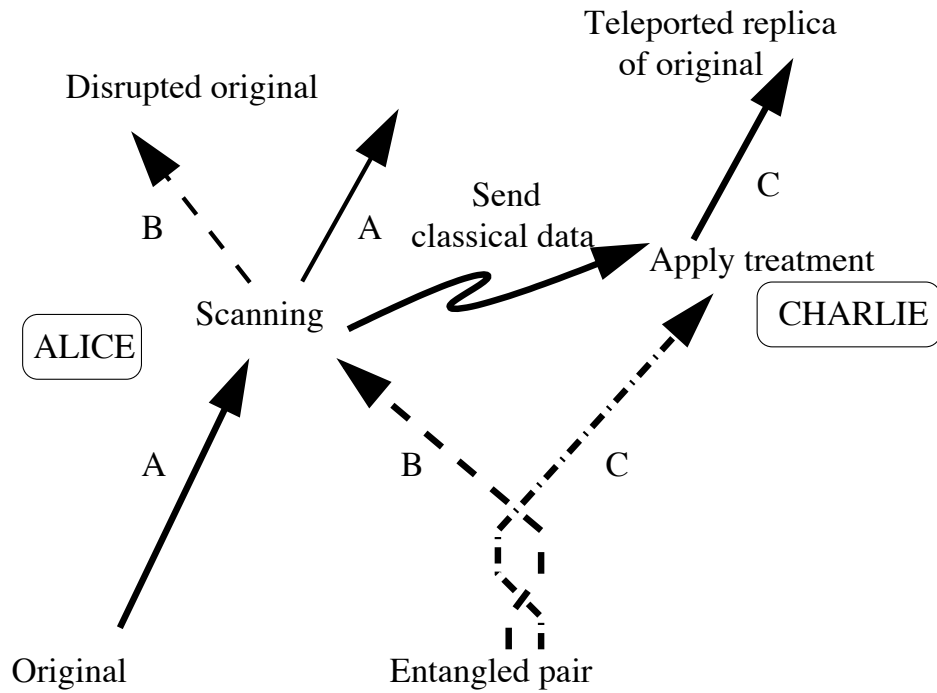
$$|\psi_2\rangle|\psi_2\rangle = U_A|\psi_2\rangle|\phi\rangle.$$

The existence of such a device would lead to a contradiction. Since $\langle \phi | \phi \rangle = 1$ and $U_A^\dagger U_A = 1$, and $U_A |\psi_i\rangle |\phi\rangle = U_A |\phi\rangle |\psi_i\rangle$, the existence of a [A] would imply that

$$\begin{aligned} \langle \psi_1 | \psi_2 \rangle &= (\langle \psi_1 | \langle \phi |) (|\phi\rangle |\psi_2\rangle) \\ &= (\langle \psi_1 | \langle \phi | U_A^\dagger) (U_A |\phi\rangle |\psi_2\rangle) \\ &= (\langle \psi_1 | \langle \psi_1 |) (|\psi_2\rangle |\psi_2\rangle) = \langle \psi_1 | \psi_2 \rangle^2. \end{aligned}$$

The property $\langle \psi_1 | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle^2$ only holds if ψ_1 and ψ_2 are either orthogonal or equal, i.e. does not hold for arbitrary values of ψ_1 and ψ_2 , so there can be no such general purpose cloning device.

Quantum teleportation



Bell states

The teleportation of this state is enabled by an auxiliary two-qubit entangled state. We label these two qubits B and C . For technical reasons it is convenient to represent this in a special basis consisting of four (entangled) states, called *Bell states*:

$$|\Psi_{BC}^{(\pm)}\rangle = \sqrt{\frac{1}{2}}(|1_B\rangle|0_C\rangle \pm |0_B\rangle|1_C\rangle)$$
$$|\Phi_{BC}^{(\pm)}\rangle = \sqrt{\frac{1}{2}}(|1_B\rangle|1_C\rangle \pm |0_B\rangle|0_C\rangle).$$

The teleportation procedure

1. Someone prepares an entangled two qubit state BC (the *Entangled pair* in the diagram).
2. Qubit B is sent to Alice and qubit C is sent to Charlie.
3. In the *Scanning* step, Alice measures in the Bell states basis the combined wavefunction of qubits A (the *original* in the diagram) and the entangled state B , leaving behind the *Disrupted original*.

4. Alice sends two bits of classical data to Charlie telling him the outcome of her measurements (*Send classical data*).
5. Based on the classical information received from Alice, Charlie applies one of four possible operators to qubit C (*Apply treatment*), and thereby reconstructs A , getting a *teleported replica of the original*. If he likes, he can now make a measurement on A to recover the message Alice has sent him.

Suppose the entangled state BC was prepared in state $|\Psi_{BC}^{(-)}\rangle$. In this case the combined wavefunction of the three qubit state is:

$$\begin{aligned}
 |\psi_{ABC}\rangle &= |\psi_A\rangle|\Psi_{BC}^{(-)}\rangle \\
 &= \frac{\alpha}{\sqrt{2}}(|1_A\rangle|1_B\rangle|0_C\rangle - |1_A\rangle|0_B\rangle|1_C\rangle) \\
 &\quad + \frac{\beta}{\sqrt{2}}(|0_A\rangle|1_B\rangle|0_C\rangle - |0_A\rangle|0_B\rangle|1_C\rangle).
 \end{aligned}$$

If this is expanded in the Bell states basis for

the pair AB , it can be written in the form:

$$\begin{aligned} |\psi_{ABC}\rangle = & \frac{1}{2} \left[|\Psi_{AB}^{(-)}\rangle(-\alpha|1_C\rangle - \beta|0_C\rangle) \right. \\ & + |\Psi_{AB}^{(+)}\rangle(-\alpha|1_C\rangle + \beta|0_C\rangle) \\ & + |\Phi_{AB}^{(-)}\rangle(\beta|1_C\rangle + \alpha|0_C\rangle) \\ & \left. + |\Phi_{AB}^{(+)}\rangle(-\beta|1_C\rangle + \alpha|0_C\rangle) \right]. \end{aligned}$$

We see that the two qubit AB has equal probability to be in the four possible states:

$$|\Psi_{AB}^{(-)}\rangle, |\Psi_{AB}^{(+)}\rangle, |\Phi_{AB}^{(-)}\rangle \text{ and } |\Phi_{AB}^{(+)}\rangle.$$

which do not depend on either α or β .

Let $|\phi_C\rangle$ be the state of the C qubit, then it is in one of the four states:

$$|\phi_C\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \begin{pmatrix} -\alpha \\ \beta \end{pmatrix}; \begin{pmatrix} \beta \\ \alpha \end{pmatrix}; \text{ and } \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}.$$

In step (5), Charlie selects one of four possible operators F_i and uses it to measure the C qubit:

$$F = - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then he has reconstructed the state $|\Psi_A\rangle$:

$$|\psi_A\rangle = \alpha|1\rangle + \beta|0\rangle = F_i|\phi_C\rangle.$$

Quantum computation

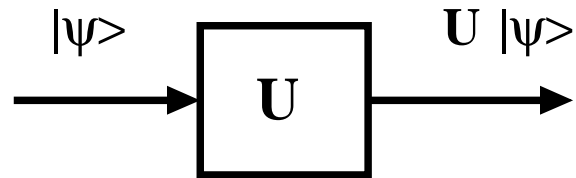
Quantum computation is the preparation, manipulation and readout of systems of qubits.

- 1.** To prepare the initial state of a quantum register we can use certain interactions and/or measurements.
- 2.** The actual computation consists of applying a sequence of quantum gates to the initial state.
- 3.** To readout the result of a calculation one has to make the appropriate measurements.

Quantum gates

One bit classical gate = *NOT* gate.

One qubit quantum gate:



Typical one-qubit logical gates are for example the following:

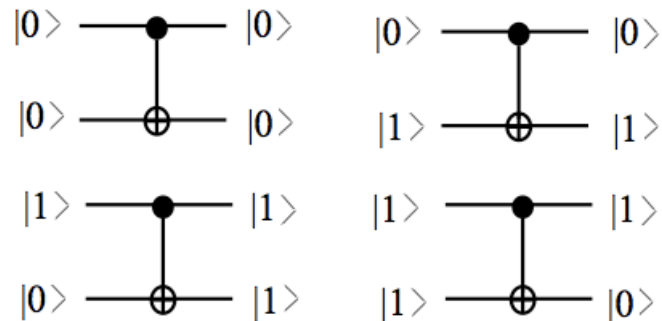
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & \exp^{i\theta} \end{pmatrix}; H = \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The 2-qubit *CNOT* gate

$$CNOT : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(with basis $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$)

It has the circuit diagram:



Why is quantum computation powerful?

The readout gives at most n classical bits of information.

The readout is probabilistic: so one may have to do the "calculation" a few times to get the "right" answer.

At the calculational stage there is a massive parallelism; every gate works on all 2^n basis vectors simultaneously. That's where the gain comes from.

Decoherence

Successful computations are only possible if one can guarantee that the system *does not decohere* during the calculations. For example interactions with the environment, cause perturbations that may destroy the information stored in the state of the system.

This is the central problem that has hampered rapid progress towards any realistic implementation of quantum computation beyond a few qubits for a very limited amount of time...

⇒ **Topological Quantum Computation**