INTRODUCTION TO QUANTUM INFORMATION SCIENCE

ARTUR EKERT

Lecture 1

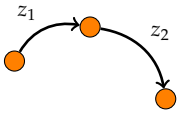
It is all about quantum interference

About complex numbers, called probability amplitudes, that, unlike probabilities, can cancel each other out, leading to quantum interference and qualitatively new ways of processing information. About impossible logic operations, such as $\sqrt{\text{NOT}}$, which nonetheless can be implemented. And about qubits and a single qubit interference. Actually, it is pretty much all about quantum interference.

The classical theory of computation usually does not refer to physics. Pioneers such as Turing, Church, Post and Gödel managed to capture the correct classical theory by intuition alone and, as a result, it is often falsely assumed that its foundations are self-evident and purely abstract. They are not! Computers are physical objects and computation is a physical process. Indeed, any computation, classical or quantum, can be viewed in terms of physical experiments, which produce outputs that depend on initial preparations called inputs. But what makes quantum computation so different? Let us start with the basics.

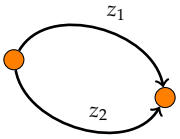
Computation is a physical process!

1.1. Quantum mechanics, at least at some instrumental level, can be viewed as a modification of the probability theory. We replace positive numbers (probabilities) with complex numbers z (probability amplitudes) such that the squares of their absolute values, $|z|^2$, are interpreted as probabilities. The rules for combining amplitudes are very reminiscent of the rules for combining probabilities..



$z = z_1 z_2$

Whenever something can happen in a sequence of independent steps we multiply the amplitudes of each step.



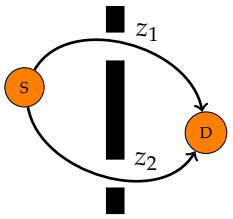
$z = z_1 + z_2$

Whenever something can happen in several alternative ways we add amplitudes for each way considered separately.

That's it! The two rules are basically all you need to manipulate amplitudes in any, no matter how complicated, physical process (we will amend the two rules later on when we touch upon the particle statistics). The two simple rules are universal and apply to any physical system, to the big and to the small, from elementary particles through atoms and molecules to white dwarfs stars. They also apply to information for information is physical; it is both represented and processed by physical means. Here we will use the two rules to explain a distinctive power of quantum information processing.

No information without physical representation! No information processing without a physical process!

1.2. Quantum Interference. In order to see the need for quantum theory let us consider a simple experiment in which probability theory fails to give the right predictions. In a double slit experiment a particle emitted from a source S can reach detector D by taking either an upper or a lower slit, with amplitudes z_1 and z_2 respectively. We may say that the upper slit is taken with probability $p_1 = |z_1|^2$ and the lower slit with probability $p_2 = |z_2|^2$. These are two mutually exclusive events. With the two slits open, probability theory declares, the particle will reach the detector with probability $p_1 + p_2 = |z_1|^2 + |z_2|^2$. Wrong! The particle will reach the detector with probability

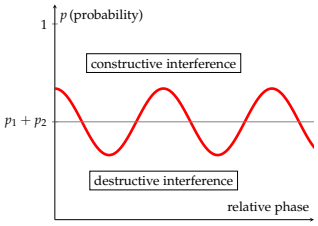


$z = z_1 + z_2$

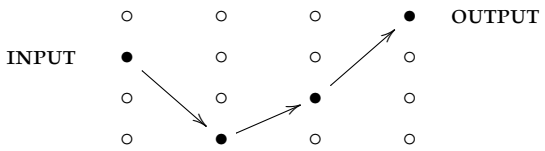
$$
\begin{aligned}
p = |z|^2 = |z_1 + z_2|^2 &= |z_1|^2 + |z_2|^2 + z_1^\star z_2 + z_1 z_2^\star, \\
&= p_1 + p_2 + |z_1||z_2|(e^{-i(\phi_2-\phi_1)} + e^{i(\phi_2-\phi_1)}), \\
&= p_1 + p_2 + 2\sqrt{p_1 p_2}\,\cos(\phi_2 - \phi_1), \\
&= p_1 + p_2 + \text{interference terms}, \qquad (1)
\end{aligned}
$$

where we have expressed the amplitudes in their polar form $z_1 = |z_1|e^{i\phi_1}$ and $z_2 = |z_2|e^{i\phi_2}$. The appearance of the interference terms marks the departure from the classical theory of probability. The probability of any two seemingly mutually exclusive events is the sum of the probabilities of the individual events, $p_1 + p_2$, *modified* by the interference term, $2\sqrt{p_1 p_2}\,\cos(\phi_2 - \phi_1)$. Depending on the relative phase $\phi_2 - \phi_1$, the interference term can be either negative (destructive interference) or positive (constructive interference), leading to either suppression or enhancement of the total probability p. If we can control relative phases we can take advantage of this effect. For example, quantum computation can be viewed as a complex multiparticle quantum interference, involving many computational paths, which is designed to enhance probabilities of correct outputs and to suppresses probabilities of the wrong ones.

Add amplitudes, not probabilities. It seems that nobody told nature about the Kolmogorov additivity axiom.

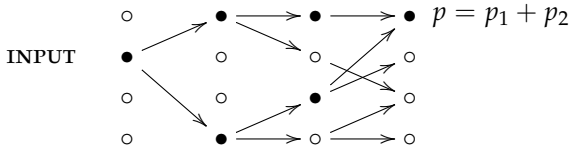


1.3. Deterministic, probabilistic and quantum. Think about computation as a physical process that evolves a prescribed initial configuration of a computing machine, called input, into some final configuration, called output. The diagram below shows three consecutive computational steps performed on four distinct configurations.



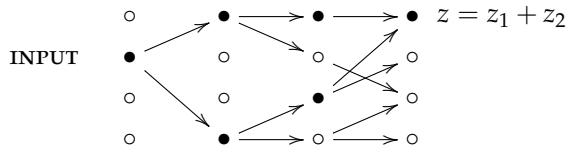
Such a computation does not have to be deterministic. We can augment a computing machine by allowing it "to toss an unbiased coin" and to choose its steps randomly. It can then be viewed as a directed, tree-like graph where each node corresponds to a configuration of the machine, and each edge represents one step of the computation.

Randomised algorithms can be more powerful than deterministic ones



The computation starts from the root node representing the initial configuration and it subsequently branches into other nodes representing configurations reachable with non-zero probability from the initial configuration. The probability of a particular final configuration being reached is equal to the sum of the probabilities along all mutually exclusive paths which connect the initial configuration with that particular configuration. The snag is that it does not always work this way. As we have mentioned, there are many physical phenomena, usually involving atoms or photons, which blatantly ignore the additivity axiom. Thus, in order to make statistical predictions that agree with experiments, probability theory had to be modified. This brings us to quantum computation, which can be represented by a graph similar to that of a probabilistic computation.

Quantum algorithms can be more powerful than randomised ones. Quantum interference is an extra tool to our disposal.

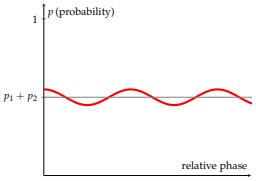


Following the rules of quantum theory we associate with each edge in the graph the probability *amplitude* that the computation follows that edge. The probability amplitude of a particular final configuration being reached is equal to the sum of the amplitudes along all mutually exclusive paths which connect the initial configuration with that particular configuration. The resulting probability, as we have just seen, reads $p_1 + p_2 + 2\sqrt{p_1 p_2}\ \cos(\phi_2 - \phi_1)$. The basic idea behind quantum algorithms is to use quantum interference to amplify the correct outputs and to suppress all other outcomes of computations. It requires a significant control over relative phases in a quantum computer for the phase settings control the interference and hence the computation.

1.4. What is wrong with the additivity axiom? You may be wondering what has happened to the axiom of additivity in probability theory, which says that if E_1 and E_2 are mutually exclusive events then the probability of the event $(E_1$ **or** $E_2)$ is the sum of the probabilities of the constituent events, E_1, E_2. So what is wrong with the additivity axiom? One thing that is wrong is the assumption that the processes of taking the upper or the lower slit are mutually exclusive. In reality, the two transitions *both occur*, simultaneously. We cannot learn about this fact from probability theory or any other a priori mathematical construct. We learn it from the best physical theory available at present, namely quantum theory. This knowledge was created as the result of conjectures, experimentation, and refutations.

Here I shamelessly reveal my philosophical leaning: Karl Popper and his *Conjectures and Refutations: The Growth of Scientific Knowledge*

1.5. Relative Phase. Note that the important quantity here is the relative phase $\phi_1 - \phi_2$ rather than the absolute values ϕ_1 and ϕ_2. This observation is not trivial at all. In simplistic terms - if a particle reacts only to the difference of the two phases, each pertaining to a separate path, then it must have, somehow, experienced the two paths, right? Thus we cannot say that the particle has travelled either through the upper or the lower slit, it has travelled through *both*. In the same way quantum computers follow, in some tangible way, all computational paths simultaneously, producing answers that depend on all these alternative calculations. Weird but this is how it is!



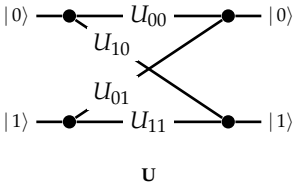
Decoherence suppresses quantum interference.

1.6. Decoherence. If this is how it is, so why we do not see quantum interference on a daily basis? I will discuss this issue later on, for now let me just say that this is because phases of probability amplitudes tend to be very fragile and may fluctuate rapidly due to spurious interactions with the environment. This has influence on the interference term; it may average to zero and we recover the classical addition of probabilities. This phenomenon is known as *decoherence*. We will discuss the origin of decoherence later on, for now let me only mention that it is very conspicuous in physical systems made out of many interacting components and it is chiefly responsible for our classical description of the world – without interference terms we may as well add probabilities instead of amplitudes. Decoherence, as you can imagine, is a serious impediment to building quantum computers; it deprives us of the power of quantum interference. This said, it is not all doom and gloom, there are clever ways around decoherence and later on we will touch upon quantum error corrections and quantum fault-tolerant computations.

1.7. Keep it simple. In order to understand something in its full complexity it is always good to start with the simplest case. Let us take a closer look at quantum interference in the simplest possible computing machine, the one that has only two distinguishable configurations — two quantum states — which we label as $|0\rangle$ and $|1\rangle$. We prepare the machine in some input state, usually $|0\rangle$, and let it evolve. The machine undergoes a prescribed sequence of computational steps, each of which induces transitions between the two "computational states", $|0\rangle$ and $|1\rangle$. The machine then ends in the output state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, meaning the two outputs, $|0\rangle$ and $|1\rangle$, are reached with probability amplitudes α_0 and α_1,

respectively. In the process of computation each computational step U sends state $|k\rangle$ to state $|l\rangle$, where $k,l = 0,1$, but only with some *amplitude* U_{lk}. We write this as

$$|k\rangle \to \sum_l U_{lk}\,|l\rangle\,. \tag{2}$$

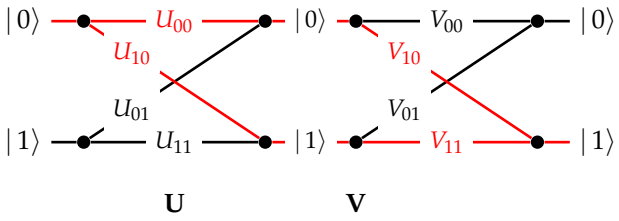


(watch the order of indices). Thus any computational step U of this machine can be described by a matrix which tabulates all the transition amplitudes,

$$U = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix}.$$

The matrix element U_{lk} represents the amplitude of transition from state $|k\rangle$ to state $|l\rangle$ (again, watch the order of indices). To be sure, the entries in this matrix are not any random complex numbers; their moduli squared represent transition probabilities which in turn implies that such matrices must be unitary (see prerequisite material). Where is the interference? Consider two computational steps, U and V,

Recall that matrix U is called unitary if $U^\dagger U = UU^\dagger = \mathbb{1}$, where the *adjoint* or *Hermitian conjugate* $U^\dagger$ of any matrix U with complex entries U_{ij} is obtained by taking the complex conjugate of every element in the matrix and then interchanging rows and columns ($U^\dagger_{kl} = U^\star_{lk}$).



What is the amplitude that input $|k\rangle$ will generate output $|m\rangle$? We have to check all computational paths leading from input $|k\rangle$ to output $|m\rangle$ and add the corresponding amplitudes. For example, as you can see in the diagram above, input $|0\rangle$ and output $|1\rangle$ are connected by the two computational paths, $|0\rangle \mapsto |0\rangle \mapsto |1\rangle$ (amplitude $V_{10}U_{00}$) and $|0\rangle \mapsto |1\rangle \mapsto |1\rangle$ (amplitude $V_{11}U_{10}$). Thus the total amplitude that input $|0\rangle$ gives ouput $|1\rangle$ is the sum $V_{10}U_{00} + V_{11}U_{10}$, and when we take the mod square of this expression we will see the interference term. In general, given U and V,

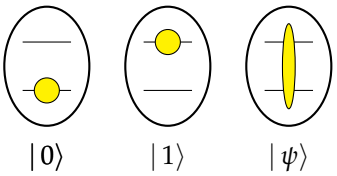
$$|k\rangle \to \sum_l U_{lk}\,|l\rangle\,, \quad |l\rangle \to \sum_m V_{ml}\,|m\rangle\,, \tag{3}$$

we compose the two operations, we apply first U and then V, to obtain

$$|k\rangle \to \sum_l U_{lk}\left(\sum_m V_{ml}\,|m\rangle\right) = \sum_m \left(\sum_l V_{ml}U_{lk}\right)|m\rangle = \sum_m (VU)_{mk}\,|m\rangle\,. \tag{4}$$

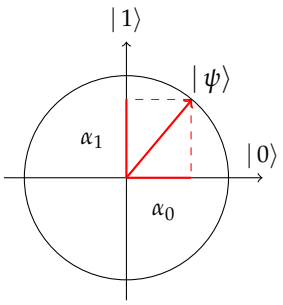
If you want to hone your quantum intuition think about it this way. The amplitude that input $|k\rangle$ evolves to $|m\rangle$ via a specific intermediate state $|l\rangle$ is given by $V_{ml}U_{lk}$ (evolutions are independent so the amplitudes are multiplied). This done we have to sum over all possible values of l (the transition can occur in several mutually exclusive ways so the amplitudes are added) to obtain $\sum_l V_{ml}U_{lk}$. Thus the matrix multiplication VU (watch the order of matrices) in one swoop takes care of multiplication and addition of amplitudes corresponding to different computational paths.

1.8. Quantum bits called qubits. A two-state machine that we have just described in abstract terms is usually realised as a controlled evolution of a two state system, called a quantum bit or a qubit. For example, state $|0\rangle$ may be chosen to be the lowest energy state of an atom, the ground state, and state $|1\rangle$ a higher energy state, the excited state. Pulses of light of appropriate frequency, duration and intensity can take the atom back and forth between the basis states $|0\rangle$ and $|1\rangle$ (implementing logical NOT). Some other pulses, say, half the duration or intensity will take the atom into states that have no classical analogue. Such states are called *coherent superpositions* of $|0\rangle$ and $|1\rangle$ and represent a qubit in state $|0\rangle$ with some amplitude



α_0 and in state $|1\rangle$ with some other amplitude α_1. This is conveniently represented by a state vector

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \leftrightarrow \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}. \tag{5}$$



$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$

A *qubit* is a quantum system in which the Boolean states 0 and 1 are represented by a prescribed pair of normalised and mutually orthogonal quantum states labeled as $\{|0\rangle, |1\rangle\}$. The two states form a 'computational basis' or a 'standard basis' and any other state of an isolated qubit can be written as a coherent superposition $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ for some α_0 and α_1 such that $|\alpha_0|^2 + |\alpha_1|^2 = 1$. A qubit is typically a microscopic system, such as an atom, a nuclear spin, or a polarised photon.

As we have already mentioned, any computational step, that is, any physically admissible operation U on a qubit, is described by a 2×2 unitary matrix U. It modifies the state of the qubit

$$|\psi\rangle \to |\psi'\rangle = U|\psi\rangle,$$

which we can write explicitly as

$$\begin{bmatrix} \alpha'_0 \\ \alpha'_1 \end{bmatrix} = \begin{bmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}.$$

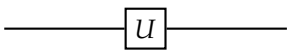
That is, operation U sends state $|\psi\rangle$, with components α_k, into state $|\psi'\rangle = U|\psi\rangle$, with components $\alpha'_l = \sum_k U_{lk}\alpha_k$.

Here we are talking about isolated systems. As you will learn soon, a larger class of physically admissible operations is described by completely positive maps.

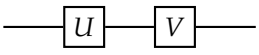
1.9. Quantum gates and circuits. Atoms, trapped ions, molecules, nuclear spins and many other quantum objects, which we call qubits, can be used to implement simple quantum interference, and hence simple quantum computation. There is no need to learn about physics behind these diverse technologies if all you want is to understand the basics of quantum computation. We may now conveniently forget about any specific experimental realisation of a qubit and just remember that any manipulations on qubits have to be performed by physically admissible operations, and that such operations are represented by unitary transformations.

A *quantum logic gate* is a device which performs a fixed unitary operation on selected qubits in a fixed period of time and a *quantum circuit* is a device consisting of quantum logic gates whose computational steps are synchronised in time. The *size* of the circuit is the number of gates it contains.

Unitary U acting on a single qubit is represented diagrammatically as

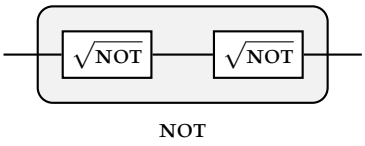


This diagram should be read from left to right. The horizontal line represents a qubit that is inertly carried from one quantum operation to another. We often call this line a quantum wire. The wire may describe translation in space, e.g. atoms traveling through cavities, or translation in time, e.g. a sequence of operations performed on a trapped ion. A sequence of two gates acting on the same qubit, say U followed by V,



is described by the matrix product VU (note the order in which we multiply the matrices).

1.10. The square root of NOT. Now that we have poked our heads into the quantum world, let us see how quantum interference challenges conventional logic and leads to qualitatively different computations. Consider a following task: design a logic gate that operates on a single bit and such that when it is followed by another, identical, logic gate the output is always the negation of the input. Let us call this logic gate the square root of NOT ($\sqrt{\text{NOT}}$). A simple check – such as an attempt to construct a truth table – should persuade you that there is no such operation in logic. It may seem reasonable to argue that since there is no such operation in logic, $\sqrt{\text{NOT}}$ is impossible. But it does exist! Experimental physicists routinely construct such "impossible" gates in their laboratories. It is a physically admissible operation described by the unitary



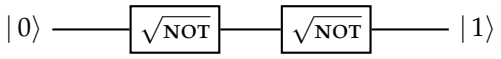
$$\sqrt{\text{NOT}} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1}{2}\begin{bmatrix} e^{i\frac{\pi}{4}} & e^{-i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} & e^{i\frac{\pi}{4}} \end{bmatrix}.$$

Indeed,

$$\frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

There are infinitely many unitary operations that effects the square root of NOT. Can you find any other? In fact, the $\sqrt{\text{NOT}}$ can be as simple as a beam-splitter (see Complement 1)

You can also step through the circuit diagram and follow the evolution of the state vector, e.g.



$$|0\rangle \overset{\sqrt{\text{NOT}}}{\longrightarrow} \frac{1}{2}\left[e^{i\frac{\pi}{4}}|0\rangle + e^{-i\frac{\pi}{4}}|1\rangle\right] \overset{\sqrt{\text{NOT}}}{\mapsto} |1\rangle. \tag{6}$$

If you prefer to work with column vectors and matrices, you can write the two consecutive application of $\sqrt{\text{NOT}}$ to state $|0\rangle$ as

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \tfrac{1}{2}\begin{bmatrix} e^{i\frac{\pi}{4}} & e^{-i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} & e^{i\frac{\pi}{4}} \end{bmatrix}\tfrac{1}{2}\begin{bmatrix} e^{i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} \end{bmatrix} \leftarrow \tfrac{1}{2}\begin{bmatrix} e^{i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} \end{bmatrix} = \tfrac{1}{2}\begin{bmatrix} e^{i\frac{\pi}{4}} & e^{-i\frac{\pi}{4}} \\ e^{-i\frac{\pi}{4}} & e^{i\frac{\pi}{4}} \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

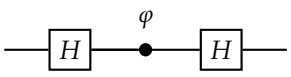
Following a well established convention the formulae above should be read from right to left. Confused? Well, you are not the only one. Just remember that circuits diagrams are read from left to right and vector and matrix operations go from right to left. This way or another, quantum theory explains the behaviour of $\sqrt{\text{NOT}}$, hence, reassured by the physical experiments that corroborate this theory, logicians are now entitled to propose a new logical operation $\sqrt{\text{NOT}}$. Why? Because a faithful physical model for it exists in nature!

HADAMARD

$$H = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

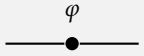
$$|0\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

1.11. Single qubit interference. Let me now describe what is probably the most important sequence of operations performed on a single qubit, namely a generic single qubit interference. It is typically constructed as a sequence of three elementary operations: the Hadamard gate, followed by a phase shift gate, and followed by the Hadamard gate. We represent it graphically as



PHASE

$$P_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

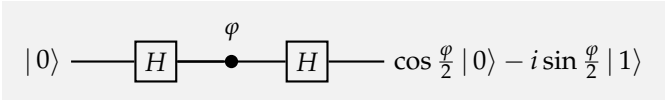


$$|0\rangle \to |0\rangle$$
$$|1\rangle \to e^{i\varphi}|1\rangle$$

You will see it over and over again, for it is quantum interference that gives quantum computation additional capabilities. The product of the three matrices $HP_\varphi H$ describes the action of the whole circuit; it gives the transition amplitudes between states $|0\rangle$ and $|1\rangle$ at the input and the output,

$$e^{i\frac{\varphi}{2}}\begin{bmatrix} \cos\varphi/2 & -i\sin\varphi/2 \\ -i\sin\varphi/2 & \cos\varphi/2 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Given that our input state is almost always $|0\rangle$ it is sometimes much easier and more instructive to step through the execution of this circuit and follow the evolving state. The interference circuit effects the following sequence of transformations,



$$|0\rangle \overset{H}{\mapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{P_\phi}{\mapsto} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right) \overset{H}{\mapsto} \cos\frac{\phi}{2}|0\rangle - i\sin\frac{\phi}{2}|1\rangle. \quad (7)$$

We have ignored the global phase factor $e^{i\frac{\varphi}{2}}$

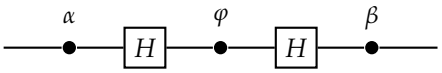
The first Hadamard gate prepares an equally weighted superposition of $|0\rangle$ and $|1\rangle$ and the second one closes the interference by brining the interfering paths together. The phase shift φ effectively controls the evolution and determines the output. The probabilities of finding the qubit in state $|0\rangle$ or $|1\rangle$ at the output are, respectively,

$$\Pr(0) = \cos^2\frac{\phi}{2}, \quad \Pr(1) = \sin^2\frac{\phi}{2}. \quad (8)$$

This simple quantum process contains, in a nutshell, the essential ingredients of quantum computation. The sequence, Hadamard - phase shift - Hadamard, will appear over and over again. It reflects a natural progression of quantum computation: first we prepare different computational paths, then we evaluate a function which effectively introduces phase shifts into different computational paths, then we bring the computational paths together at the output.

1.12. Any unitary operation on a single qubit. There are infinitely many unitary operations that can be performed on a single qubit. In general, any complex $n \times n$ matrix has n^2 complex entires, hence it can be specified by $2n^2$ real independent parameters. The unitarity constraint removes n^2 of these hence any unitary $n \times n$ matrix has n^2 real independent parameters. In particular, we need four real parameters to specify a 2×2 unitary matrix. If we are prepared to ignore global phase factors, which we are, there are only three real parameters left. Can we construct and implement any unitary on a single qubit in some simple way. Yes, we can. We have talked a lot about the Hadamard and phase gates, and for good reason. Any unitary operation on a qubit (up to an overall multiplicative phase factor) can be implemented by a circuit containing just two Hadamards and three phase gates, with adjustable phase settings,

The set of all 2×2 unitary matrices forms a non-abelian group under the matrix multiplication. The group is denoted $U(2)$.It turns out that compositions of single qubit unitaries behave pretty much the same as compositions of rotations in three dimensions. Technically speaking, $U(2)/U(1) \cong SO(3)$, that is, 2×2 unitaries, up to global phase, form a group which is isomorphic to the group of rotations in three dimensions, denoted $SO(3)$. This isomorphism helps to visualise the actions of single qubit gates.



If we multiply the matrices corresponding to each gate in the network (remember that the order of matrix multiplication is reversed) we obtain

$$U(\alpha,\beta,\gamma) = \begin{bmatrix} e^{-i\left(\frac{\alpha+\beta}{2}\right)}\cos\varphi/2 & -ie^{i\left(\frac{\alpha-\beta}{2}\right)}\sin\varphi/2 \\ -ie^{-i\left(\frac{\alpha-\beta}{2}\right)}\sin\varphi/2 & e^{i\left(\frac{\alpha+\beta}{2}\right)}\cos\varphi/2 \end{bmatrix}.$$

Any 2×2 unitary matrix (up to global phase) can be expressed in this form using the three independent real parameters, α, β, and φ, which take values from 0 to 2π.

The phase gate α is defined up to global phase. We write its matrix as

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} \text{ or } \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix}$$

Notes & Exercises

(1) Back in 1926 Max Born simply postulated the connection between amplitudes and probabilities. However, it is worth pointing out, that he did not get it quite right on his first approach. In the original paper proposing the probability interpretation of the state vector (wavefunction) he wrote:

> ...If one translates this result into terms of particles only one interpretation is possible. $\Theta_{\eta,\tau,m}(\alpha,\beta,\gamma)$ [the wavefunction for the particular problem he is considering] gives the probability* for the electron arriving from the z direction to be thrown out into the direction designated by the angles α,β,γ... .
>
> * Addition in proof: More careful considerations show that the probability is proportional to the square of the quantity $\Theta_{\eta,\tau,m}(\alpha,\beta,\gamma)$.

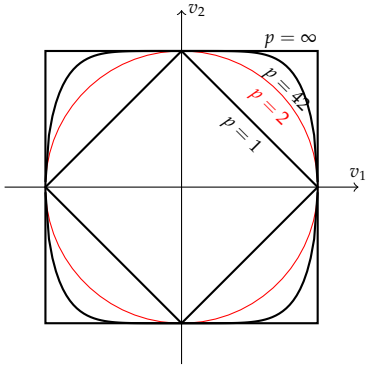
Max Born, Zur Quantenmechanik der Stoßvorgänge, *Zeitschrift für Physik*, 37, 863–867 (1926).

(2) All physical evolutions U are represented by operators that map unit state vectors $\sum_k \alpha_k |k\rangle$ into unit state vectors $\sum_l \alpha'_l |l\rangle$, hence

$$1 = \sum_l |\alpha'_l|^2 = \sum_l \left(\sum_m U_{lm}\alpha_m\right)\left(\sum_n U_{ln}\alpha_n\right)^\star = \sum_{m,n}\left(\sum_l U_{lm}U^\star_{ln}\right)\alpha_m\alpha^\star_n. \qquad (9)$$

This equality must hold for all admissible values of α_m and $\alpha^\star_n$. This is possible only if $\sum_l U_{lm}U^\star_{ln} = \sum_l U^\dagger_{nl}U_{lm} = \delta_{mn}$, i.e. the operators must be unitary.

(3) Suppose probabilities are given by the absolute values of amplitudes raised to power p. The admissible physical evolutions must preserve the normalisation of probability. Mathematically speaking, they must be isometries of p-norms. Recall that the p-norm of vector v, with components $v_1, v_2, ..., v_n$, is defined as $\sqrt[p]{|v_1|^p + |v_2|^p + ...|v_n|^p}$. It is clear that any permutation of vector components and multiplication by phase factors (unit complex numbers) will leave any p-norm unchanged. It turns out that these complex permutations are the only isometries, except one special case! For $p = 2$, the isometries are unitary operations, which form a continuous group. In all other cases we are restricted to discrete permutations. We do not have to go into details of the proof for we can *see* this result. The picture in the margin shows unit spheres in different p norms, e.g. for $p = 1, 2, 42$, and ∞. The image of the unit sphere must be preserved under probability preserving operations. As we can see the 2-norm is special because of its rotational invariance – the probability measure picks out no preferred basis in the space of state vectors. Moreover, it respects unitary operations and does not restrict them in any way. If the admissible physical evolutions were restricted to discrete symmetries, e.g. permutations, there would be no continuity and no time as we know it.



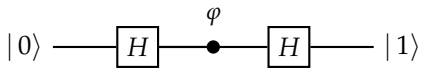
(4) A quantum computer starts calculations in some initial state, then follows n different computational paths which lead to the final output. The computational paths are followed with probability amplitudes $\frac{1}{\sqrt{n}}e^{ik\varphi}$, where φ is a fixed angle $0 < \varphi < 2\pi$ and $k = 0, 1, ...n-1$. Show that the probability of generating the output is

$1 + z + z^2 + \ldots + z^n = \frac{1-z^{n+1}}{1-z}$

$$\frac{1}{n}\left|\frac{1-e^{in\varphi}}{1-e^{i\varphi}}\right|^2 = \frac{1}{n}\frac{\sin^2(n\frac{\varphi}{2})}{\sin^2(\frac{\varphi}{2})}.$$

for $0 < \varphi < 2\pi$ and 1 for $\varphi = 0$. Plot the probability as a function of φ.

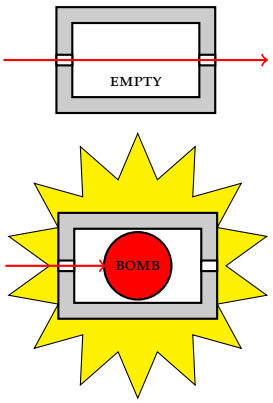
(5) **Guess the phase** Consider the usual quantum interference circuit,



Suppose you can control the input of the circuit and measure the output, but you do not know the phase shift φ introduced by the phase gate. You prepare input $|0\rangle$ and register output $|1\rangle$, what can you say about φ? Now you are promised that φ is either 0 or π. You can run the circuit only once to find out which of the two phases was chosen. Can you do that?

(6) **Quantum Bomb Tester** You have been drafted by the government to help in the demining effort in a former war-zone. In particular, retreating forces have left very sensitive bombs in some of the sealed rooms. The bombs are configured such that if even one photon of light is absorbed by the fuse (i.e. if someone looks into the room), the bomb will go off. Each room has an input and output port which can be hooked up to external devices. An empty room will let light go from the input to the output ports unaffected, whilst a room with a bomb will explode if light is shone into the input port and the bomb absorbs even just one photon. Your task is to find a way of determining whether a room has a bomb in it without blowing it up, so that specialised (limited and expensive) equipment can be devoted to defusing that particular room. You would like to know with certainty whether a particular room had a bomb in it.

This is a slightly modified version of a bomb testing problem described by Avshalom Elitzur and Lev Vaidman in *Quantum-mechanical interaction-free measurement*, Found. Phys. **47**, 987-997 (1993).



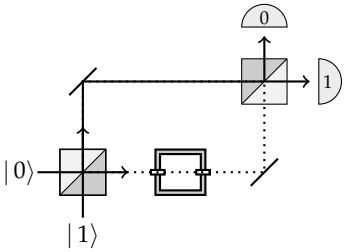
(a) To start with, consider the setup (see the margin) where the input and output ports are hooked up in the lower arm of a Mach-Zehnder interfereometer.

(i) Assume an empty room. Send a photon to input port $|0\rangle$. Which detector, at the output port, will register the photon?

(ii) Now assume that the room does contain a bomb. Again, send a photon to input port $|0\rangle$. Which detector will register the photon and with which probability?

(iii) Design a scheme that allows you – at least part of the time – to decide whether a room has a bomb in it without blowing it up. If you iterate the procedure, what is its overall success rate for the detection of a bomb without blowing it up?

Hint: Consider the setup where the input and output ports are hooked up in one of the arms of a Mach-Zehnder interferometer.



(b) Assume that the two beam splitters in the interferometer are different. Say the first beamsplitter reflects incoming light with probability r and transmits with probability $t = 1 - r$ and the second one transmits with probability r and reflects with probability t. Would the new setup improve the overall success rate of the detection of a bomb without blowing it up?

(c) There exists a scheme, involving many beamsplitters and something called "quantum Zeno effect", such that the success rate for detecting a bomb without blowing it up approaches 100%. Try to work it out or find a solution on internet.

(7) The exponent of matrix A is defined as

$$e^A = \mathbb{1} + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \ldots = \sum_{n=0}^{\infty} \frac{(A)^n}{n!}$$

Show that if H is self-adjoint (Hermitian), that is $H = H^\dagger$, then $U = e^{iHt}$ is unitary for any real t. Many quantum evolutions are expressed in this way. This is because matrix H, known as the Hamiltonian, is related to energies, which are measurable physical quantities, and t stands for time.

(8) Show that for any real α and for any A such that $A^2 = \mathbb{1}$

$$e^{i\alpha A} = \cos\alpha\,\mathbb{1} + i\sin\alpha\, A. \tag{10}$$

(9) A qubit (spin one-half particle) initially in state $|0\rangle$ (spin up) is placed in a uniform magnetic field. The interaction between the field and the qubit is described by the Hamiltonian

In Earth's magnetic field, which is about 0.5 gauss, the value of ω is of the order of 10^6 cycles per second.

$$H = \omega \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

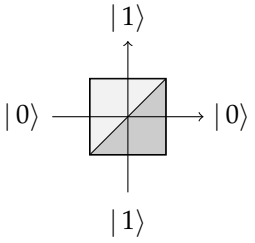
where ω is proportional to the strength of the field. What is the state of the qubit after time $t = \pi/4\omega$?

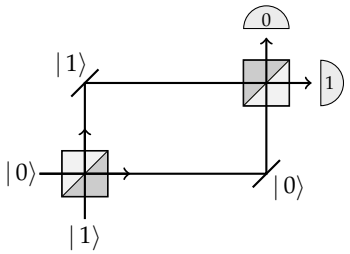
(10) **How to ascertain the values of σ_x and σ_y of a qubit**. Alice prepares a qubit in any state of her choosing and gives it to Bob who secretly measures either σ_x or σ_y. The outcome of the measurement is seen only by Bob. Alice has no clue which measurement was chosen by Bob but right after his measurement she gets her qubit back and she can measure it as well. Some time later Bob tells Alice which of the two measurements was chosen, i.e. whether he measured σ_x or σ_y. Alice then tells him the outcome he obtained in his measurement. Bob is surprised for the two measurements have mutually unbiased bases and yet Alice always gets it right. How does she do it?

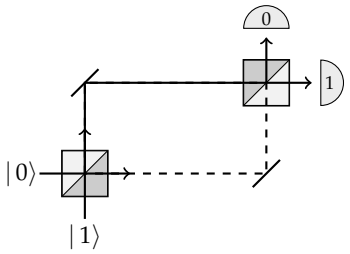
This is a simplified version of a beautiful quantum puzzle proposed in 1987 by Lev Vaidman, Yakir Aharonov, and David Z. Albert in a paper with the somewhat provocative title, "How to ascertain the values of σ_x, σ_y, and σ_z of a spin-$\frac{1}{2}$ particle." For the original see Phys. Rev. Lett. vol. 58, 1385 (1987).

2. Physics against logic
Explained with a beamsplitter

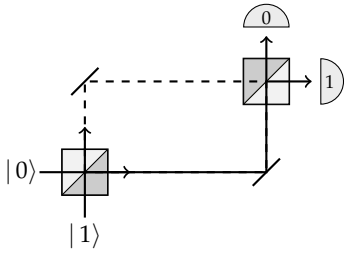
A symmetric beam-splitter is a cube of glass which reflects half the light that impinges upon it, while allowing the remaining half to pass through unaffected. For our purposes it can be viewed as a device which has two input and two output ports which we label as $|0\rangle$ and $|1\rangle$. When we aim a single photon at such a beam-splitter using one of the input ports, we notice that the photon doesn't split in two: we can place photo-detectors wherever we like in the apparatus, fire in a photon, and verify that if any of the photo-detectors registers a hit, none of the others do. In particular, if we place a photo-detector behind the beam-splitter in each of the two possible exit beams, the photon is detected with equal probability at either detector, no matter whether the photon was initially fired from input port $|0\rangle$ or $|1\rangle$. It may seem obvious that at the very least, the photon is *either* in the transmitted beam $|0\rangle$ *or* in the reflected beam $|1\rangle$ during any one run of this experiment. Thus we may be tempted to think of the beam-splitter as a random binary switch which, with equal probability, transforms any binary input into one of the two possible outputs. However, that is not necessarily the case. Let us introduce a second beam-splitter and place two normal mirrors so that both paths intersect at the second beam-splitter (see diagrams in the margin).







Two consecutive reflections give amplitude $\frac{i}{\sqrt{2}}\frac{i}{\sqrt{2}} = -\frac{1}{2}$



Two consecutive transmissions give amplitude $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}} = \frac{1}{2}$

Now, the axiom of additivity in probability theory, says that whenever something can happen in several alternative ways we add probabilities for each way considered separately. We might argue that a photon fired into the input port $|0\rangle$ can reach the detector 0 in two *mutually exclusive* ways: either by two consecutive reflections or by two consecutive transmissions. Each reflection happens with probability $1/2$ and each transmission happens with probability $1/2$ thus the total probability of reaching detector 0 is a sum of the probability of the two consecutive reflections ($1/2 \times 1/2 = 1/4$) and the probability of the two consecutive transmissions ($1/2 \times 1/2 = 1/4$) which gives probability $1/2$. This makes perfect sense – a random switch followed by a random switch should give nothing else but a random switch. However, if we set up such an experiment, that is not what happens! When the optical paths between the two beam-splitters are the same, the photon fired from input port $|0\rangle$ *always* strikes detector 1 and *never* detector 0 (and the photon fired from input port $|1\rangle$ *always* strikes detector 0 and *never* detector 1). Thus a beam-splitter acts as the square root of NOT gate. What is wrong with our reasoning here? Why does probability theory fail to predict the outcome of this simple experiment?

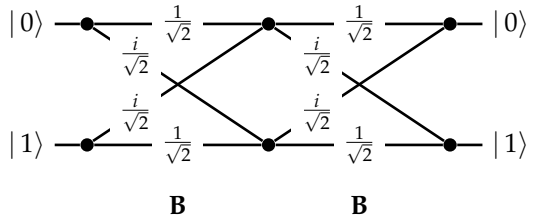
A beamsplitter is a quantum device thus we have to multiply and add amplitudes not probabilities. The action of the beamsplitter – in fact, the action of any quantum device – can be described by tabulating the amplitudes of transitions between its input and output ports.

$$B = \begin{bmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

The matrix element B_{lk}, where $k, l = 0, 1$, represents the amplitude of transition from input $|k\rangle$ to output $|l\rangle$ (watch the order of indices). Each reflection (entries B_{01} and B_{10}) happens with amplitude $i/\sqrt{2}$ and each transmission (entries B_{00} and B_{11}) happens with amplitude $1/\sqrt{2}$. Thus the total amplitude that a photon fired from input port $|0\rangle$ will reach detector 0 is the sum of the amplitude of the two consecutive reflections ($i/\sqrt{2} \times i/\sqrt{2} = -1/2$) and the amplitude of the two consecutive transmissions ($1/\sqrt{2} \times 1/\sqrt{2} = 1/2$) which gives the total amplitude 0. The resulting probability is then zero. Unlike probabilities, amplitudes can cancel out each other out. We can now go on and calculate the amplitude that the photon will reach detector 1. In this case we will get i, which gives probability 1. We

There is no reason why probability theory or any other a priori mathematical construct should make any meaningful statements about outcomes of physical experiments.

can then switch to input $|1\rangle$ and repeat our calculations. All possible paths and associated amplitudes are shown in the diagram below.



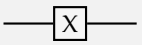
However, instead of going through all the paths in this diagram and linking specific inputs to specific outputs, we can simply multiply the transition matrices,

$$BB = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = iX.$$

As you can see, the matrix multiplication in one swoop takes care of multiplication and addition of amplitudes corresponding to different alternatives. You can now inform you colleagues logicians that they are now entitled to propose a new logical operation $\sqrt{\text{NOT}}$ for a faithful physical model for it exists in nature!

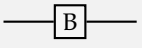
LOGICAL NOT

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



BEAM SPLITTER

$$B = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$



Gate B is not the only quantum operation that effects the square root of NOT. Can you find any other? There are infinitely many of them.