Lecture 1. Impossible logic

Artur Ekert and Alastair Kay

How some weird logic gates can be constructed using the power of quantum interference.

I. IMPOSSIBLE LOGIC

Consider the most basic logic gate in a computer, NOT. Suppose you were given the following assignment: design the square root of NOT, that is, a logic gate that, acting twice on an input, negates it.

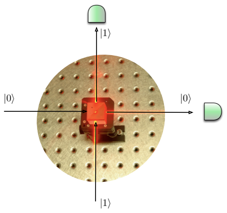
$$-\boxed{\sqrt{\text{NOT}}}-\boxed{\sqrt{\text{NOT}}}- \;\equiv\; -\boxed{\text{NOT}}-$$

It is perfectly reasonable to assume that *the most general* logic gate is completely specified by its stochastic matrix. Suppose that the square root of NOT does exist and is described by some stochastic matrix P. Then the matrix product $PP = P^2$ should give a stochastic matrix corresponding to the logical NOT, but this, given that all entries in stochastic matrices are nonnegative, is impossible.

It may seem reasonable to argue that since there are no such operations in logic, the $\sqrt{\text{NOT}}$ gate cannot exist. But it does exist! Experimental physicists routinely construct such "impossible" gates in their laboratories. In fact the $\sqrt{\text{NOT}}$ can be as simple as a beam-splitter.

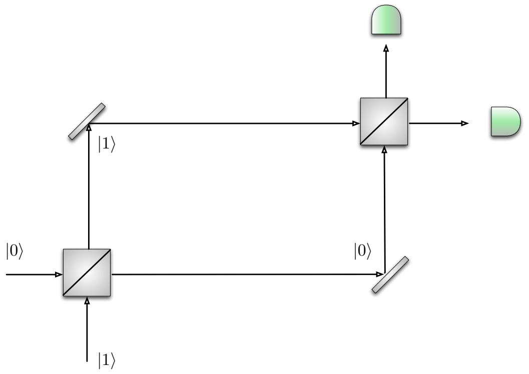
II. PHYSICS AGAINST LOGIC

You can convince yourself that the square root of NOT does exist by *experimenting* with beam-splitters. 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 labeled 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 let us place two normal mirrors so that both paths intersect at the second beam-splitter



Now, the axiom of additivity in probability theory, 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,

$$P = P_1 + P_2.$$

Again, we might argue that the detector 0 can be reached in two *mutually exclusive* ways: either by two consecutive reflections (event E_1) or by two consecutive transmissions (event E_2). 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 and the probability of the two consecutive transmissions, $P_{00} = \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{1}{2}$. And 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! It turns out that in the arrangement shown above, i.e. when the optical paths between the two beam-splitters are the same, the photon *always* strikes detector 1 and *never* detector 0. Thus a beam-splitter acts as the square root of NOT gate. But what is wrong with our reasoning here? Why does probability theory fail to predict the outcome of this simple experiment?

One thing that is wrong is the assumption that the processes that lead the photon from the initial state to the detector 0 are *mutually exclusive.* In reality, the photon must, in some sense, have traveled both routes at once! Another thing is the status of probability theory. There is no reason why probability theory or any other a priori mathematical construct should make any meaningful statements about outcomes of physical experiments. For this we need the best physical theory available at present, namely quantum mechanics. Quantum theory explains the behavior of $\sqrt{\text{NOT}}$, $\sqrt{\text{SWAP}}$ and many other gates, and correctly predicts the probabilities of all the possible outputs no matter how we concatenate the gates. This knowledge was created as the result of conjectures, experimentation, and refutations. Genuine scientific knowledge cannot be certain, nor can it be justified a priori. Instead, it must be conjectured, and then tested by experiment.

Hence, reassured by the physical experiments that corroborate this theory, logicians are now entitled to propose new logical operations $\sqrt{\text{NOT}}$ and $\sqrt{\text{SWAP}}$. Why? Because faithful physical models for them exist in nature!

III. AMPLITUDES AND INTERFERENCE

In order to calculate probabilities that agree with experimental data quantum mechanics, the result of conjectures, experimentation and refutations, we must introduce the concept of *probability amplitudes* – complex numbers α such that the quantities $|\alpha|^2$ are interpreted as probabilities. When a transition, such as "a photon impinges the first beam-splitter in the interferometer and ends up in the detector 0, and affects nothing else in the process", can occur in several alternative ways, the overall probability amplitude for the transition is the sum, not of the probabilities, but of the probability amplitudes for each of the constituent transitions considered separately,

$$\alpha = \alpha_1 + \alpha_2. \tag{1}$$

The associated probability is then given by

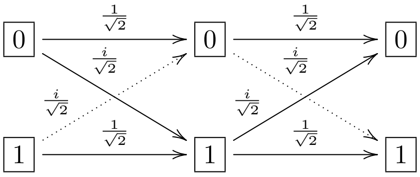
$$\begin{aligned} P = |\alpha|^2 = |\alpha_1 + \alpha_2|^2 &= |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1^\star \alpha_2 + \alpha_1 \alpha_2^\star \\ &= P_1 + P_2 + |\alpha_1||\alpha_2|(e^{i(\phi_1-\phi_2)} + e^{-i(\phi_1-\phi_2)}) \\ &= P_1 + P_2 + 2\sqrt{P_1 P_2}\ \cos(\phi_1 - \phi_2). \end{aligned}$$

where we have expressed the amplitudes in their polar form $\alpha_1 = |\alpha_1|e^{i\phi_1}$ and $\alpha_2 = |\alpha_2|e^{i\phi_2}$. The phases ϕ_1 and ϕ_2 depend on the lengths of the respective optical paths. The last term on the r.h.s. marks the departure from the classical theory of probability. It blatantly ignores the additivity axiom. The probability of any two mutually exclusive events is the sum of the probabilities of the individual events, $P_1 + P_2$, modified by what is called the interference term, $2\sqrt{P_1 P_2}\ \cos(\phi_1 - \phi_2)$. Depending on the relative phase $\phi_1 - \phi_2$, 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 this is how the universe works why we do not see quantum interference on a daily basis? The thing is, phases of probability amplitudes tend to be very fragile and may fluctuate rapidly due to spurious interactions with the environment. In this case, the interference term may average to zero and we recover the classical addition of probabilities. This phenomenon is known as *decoherence.* It is very conspicuous in physical systems made out of many interacting components and is chiefly responsible for our classical description of the world – without interference terms we may as well add probabilities instead of amplitudes.

IV. IMPOSSIBLE LOGIC EXPLAINED

It should be clear now that our previous analysis was incomplete for *the most general* computing machine must be described in terms of *amplitudes*, not probabilities. Amplitudes can cancel each other out and make some transitions less likely, or they can interfere constructively and make some other transitions more likely. The diagram below shows the transitions and the corresponding transition amplitudes in a sequence of two beam-splitters



The transition matrix of the beamsplitter can be read directly from the diagram

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

The corresponding transition probabilities are obtained by squaring the absolute values of the transition amplitudes, which, in this particular case, gives the stochastic matrix with all entries equal to 1/2. Thus a single beam-splitter behaves as a random switch, generating 0 or 1 with equal probability regardless the input. However, in this case a random switch followed by a random switch is not another random switch!

Instead of going through all the paths in the diagram that lead from a specific input to specific output and add corresponding amplitudes we can simply multiply the transition matrices,

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

Again, the corresponding transition probabilities are obtained by squaring the absolute values of the transition amplitudes. The new stochastic matrix represents operation NOT. But this means that the machine described by matrix U is the square root of NOT!