Decoherence and quantum error correction

Artur Ekert and Alastair Kay

In principle we know how to build a quantum computer; we can start with simple quantum logic gates and try to integrate them together into quantum networks. However, if we keep on putting quantum gates together into networks we will quickly run into some serious practical problems. The more interacting qubits are involved the harder it is to prevent them from getting entangled with the environment. This unwelcome entanglement, also known as decoherence, destroys the interference and the power of quantum computing.

I. DECOHERENCE

Consider the following qubit-environment interaction,

$$|0\rangle|e\rangle \mapsto |0\rangle|e_0\rangle, \quad |1\rangle|e\rangle \mapsto |1\rangle|e_1\rangle$$

where $|e\rangle$, $|e_0\rangle$ and $|e_1\rangle$ are the states of the environment, which not need to be orthogonal. Here, the environment is trying to measure the qubit and the two get entangled,

$$(\alpha|\,0\rangle + \beta|1\rangle)\,|e\rangle \mapsto \alpha|\,0\rangle|e_0\rangle + \beta|\,1\rangle|e_1\rangle.$$

This can also be written as

$$\begin{aligned}(\alpha|0\rangle + \beta|1\rangle)\,|e\rangle \mapsto & (\alpha|0\rangle + \beta|1\rangle)\,\frac{|e_0\rangle + |e_1\rangle}{2} \\ & + (\alpha|0\rangle - \beta|1\rangle)\,\frac{|e_0\rangle - |e_1\rangle}{2}.\end{aligned}$$

We may interpret this expression by saying that two things can happen to the qubit: nothing (first term) or phase-flip (second term). The qubit alone evolves from a pure to a mixed state. In terms of density operators, after taking the partial trace over the environment, we obtain

$$\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \mapsto \begin{pmatrix} |\alpha|^2 & \alpha\beta^*\langle e_1|\,e_0\rangle \\ \alpha^*\beta\langle e_0|\,e_1\rangle & |\beta|^2 \end{pmatrix}.$$

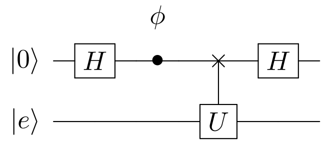
The off-diagonal elements, originally called "coherences", vanish as $\langle\, e_0\,|\,e_1\,\rangle$ approaches zero. This is why this particular interaction is called decoherence. Assuming that $\langle\, e_0\,|\,e_1\,\rangle$ is real, we can also write the evolution of the single qubit density matrix as

$$|\psi\rangle\langle\psi| \mapsto (1-p)|\psi\rangle\langle\psi| + pZ|\psi\rangle\langle\psi|Z,$$

where $|\psi\rangle$ is the initial state of the qubit, Z is the phase flip operation and we choose p so that $1-2p = \langle\, e_0\,|\,e_1\,\rangle$. This is a statistical mixture of the original pure state and the phase flipped version.

II. DECOHERENCE DESTROYS INTERFERENCE

Suppose our qubit undergoes the usual interference experiment but in between the two Hadamard gates it is affected by the decoherence, represented here, without any loss of generality, by some controlled-U operation.



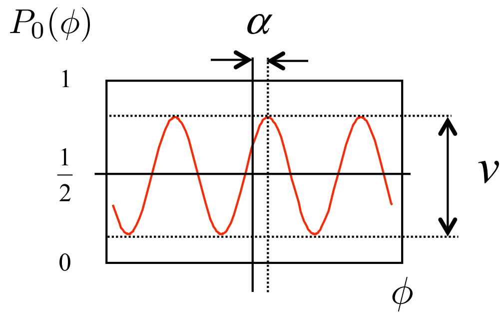
The environment, initially in state $|e\rangle$, tries to learn whether the qubit is in state $|0\rangle$ or $|1\rangle$,

$$\begin{aligned}|0\rangle|e\rangle &\overset{H}{\mapsto} (|0\rangle + |1\rangle)|e\rangle \\ &\overset{\phi}{\mapsto} (|0\rangle + e^{i\phi}|1\rangle)|e\rangle \\ &\overset{\times}{\mapsto} |0\rangle|e_0\rangle + e^{i\phi}|1\rangle|e_1\rangle \\ &\overset{H}{\mapsto} |0\rangle(|e_0\rangle + e^{i\phi}|1\rangle) + |1\rangle(|e_0\rangle - e^{i\phi}|1\rangle).\end{aligned}$$

If we write $\langle\, e_0\,|\,e_1\,\rangle = ve^{i\alpha}$ then the final probabilities of 0 and 1 oscillate with ϕ as

$$\begin{aligned}P_0(\phi) &= \tfrac{1}{2}\left(1 + v\cos(\phi+\alpha)\right), \\ P_1(\phi) &= \tfrac{1}{2}\left(1 - v\cos(\phi+\alpha)\right).\end{aligned}$$

As we can see on the diagram below, the interference pattern is suppressed by factor v, called visibility.



As $v = |\,\langle\, e_0\,|\,e_1\,\rangle\,|$ decreases we loose all the advantages of quantum interference. For example, in Deutsch's algorithm we obtain the correct answer with probability at most $(1+v)/2$. For $\langle e_0|\,e_1\rangle = 0$, the perfect decoherence case, the network outputs 0 or 1 with equal probabilities, *i.e.* it is useless as a computing device. It is clear that we want to avoid decoherence, or at least diminish its impact on our computing device. For this we need quantum error correction; we encode the state of a single (logical) qubit across several (physical) qubits.

III. QUANTUM ERRORS

The most general qubit-environment interaction,

$$|0\rangle|e\rangle \mapsto |0\rangle|e_0\rangle + |1\rangle|d_0\rangle,\ |1\rangle|e\rangle \mapsto |1\rangle|e_1\rangle + |0\rangle|d_1\rangle,$$

where the states of the environment are neither normalised nor orthogonal, leads to decoherence

$$\begin{aligned}(\alpha|0\rangle + \beta|1\rangle)\,|e\rangle \mapsto & (\alpha|0\rangle + \beta|1\rangle)\,\frac{|e_0\rangle + |e_1\rangle}{2}\\ & +(\alpha|0\rangle - \beta|1\rangle)\,\frac{|e_0\rangle - |e_1\rangle}{2}\\ & +(\alpha|1\rangle + \beta|0\rangle)\,\frac{|d_0\rangle + |d_1\rangle}{2}\\ & +(\alpha|1\rangle - \beta|0\rangle)\,\frac{|d_0\rangle - |d_1\rangle}{2}.\end{aligned}$$

Four things can happen to the qubit: nothing, phase-flip, bit-flip or both bit-flip and phase-flip. Essentially we have to deal with two types of quantum errors: bit-flips and phase-flips.

IV. REPETITION CODES

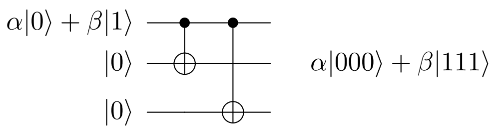
In order to give a sense of how quantum error correction actually works let us begin with a classical example of a repetition code. Suppose a transmission channel flips each bit in transit with probability p. If this error rate is considered too high then it can be decreased by encoding each bit into, say, three bits,

$$0 \mapsto 000, \quad 1 \mapsto 111.$$

That is, each time we want to send logical 0 we send three physical bits, all in state 0 and each time we want to send logical 1 we send three physical bits, all in state 1. The receiver decodes the bit value by a "majority vote" of the three bits. If only one error occurs then this error correction procedure is foolproof. In general the net probability of error is just the likelihood that two or three errors occur, which is $3p^2(1-p)+p^3 \leq p$. Thus, the three bit code improves the reliability of the information transfer. Quantum case is more complicated because we have both bit-flip and phase-flip errors.

V. QUANTUM ERROR CORRECTION

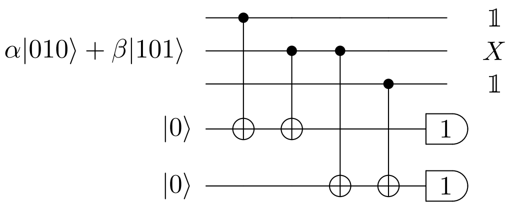
In order to protect a qubit against bit-flips (incoherent X rotations), we rely on the same repetition code, but both encoding and error correction is now done by quantum operations. We take a qubit in some unknown pure state $\alpha|0\rangle + \beta|1\rangle$, bring two auxiliary qubits, and encode it into the three qubits as



Suppose at most one qubit is then flipped, say the second one. The encoded state becomes

$$\alpha|010\rangle + \beta|101\rangle.$$

Decoding requires some care. Note that if we measured the three qubits directly, that would destroy the superposition of states which we are working so hard to protect. Instead we bring two additional qubits, both in state $|0\rangle$, and apply the following network



We measure the two auxiliary qubits, also known as ancillas, and the result of the measurement, known as the error syndrome, tells us how to reset the three qubits of the code. The theory behind this network runs as follows. If qubits one and two, counting from the top, are the same, then the first ancilla is in the $|0\rangle$ state. Similarly, if qubits two and three are the same, then the second ancilla is in the $|0\rangle$ state. However, if they are different, the corresponding ancilla is in the $|1\rangle$ state. Hence, the four possible error syndromes $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ each indicate a different possibility – no errors, an error in the third, first or second qubits respectively. In our example, we would measure $|11\rangle$, revealing that both qubits 1 and 2, and qubits 2 and 3, are different. Thus, it is qubit 2 that has an error on it. Knowing the error, we can go back and fix it, simply by applying X to qubit 2. The net result is the state $\alpha|000\rangle + \beta|111\rangle$, which is then turned into $(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle$ by running the mirror image of the encoding network.

The three-qubit code that we have just demonstrated is sufficient to protect a qubit against single bit-flips, but not phase-flips. But this is good enough. Recall that $HZH = X$, hence it is enough to sandwich the decoherence area in between the Hadamard gates - they will turn phase flips into bit flips - and we can protect our qubits against Z-errors. The encoded state $\alpha|0\rangle + \beta|1\rangle$ now reads $\alpha|+++\rangle + \beta|---\rangle$, where $|\pm\rangle = |0\rangle \pm |-\rangle$.

We can now put the bit-flip and phase-flip codes together: first we encode the qubit using the phase-flip code and then we encode each of the three qubits of the code using the bit-flip code. This gives an error correction scheme that allows us to protect against both types of error, thus yielding a code that encodes a single logical qubit across nine physical qubits, protecting against a single quantum error on any of the nine qubits.

If we want to preserve a quantum state for a long time without doing any calculations, or if we want to send it through a noisy communications channel, we can just encode the state using a quantum code and decode it when we are done. Computation on encoded states using noisy gates requires few more tricks.