A Theory of Quantum Error-Correcting Codes by Emanuel Knill and Raymond Laflamme

Ella Roselli

April 22nd, 2024

1 Introduction

Quantum computing has proven to have an enormous potential for completely revolutionizing computer science and crypotgraphy, which also has practical implication in national security.

However, these quantum calculations are very sensitive to imperfections, which aren't uncommon with the decoherences that arise from quantum states interacting with the environment, or with the computer hardware itself. Because quantum computing relies on such precision, we need a way to correct these errors. Many have developed methods that are able to correct for specific interactions, and the authors, Knill and Laflamme, were thus able to develop this general theory of quantum error correction.

2 An intuitive approach

There are two main cases where manipulating coherent quantum states is important: in quantum communication and in quantum computation. *Quantum communication* focuses on the transmission of states over potentially noisy channels, often involving multiple parties with limited communication capabilities. *Quantum computation* instead focuses on the unitary transformations resulting in the final state, involving only one part. However, in both of these cases result in the loss of coherence while executing operations or transmitting or storing information. This loss of coherence directly reduces the probability of getting the correct final result, so it's important to avoid such errors. There are two main methods: (1) for short distances or rather simple computations, one can minimize errors by isolating the quantum state and improving the accuracy of the unitary transformation used, and (2) for long distances or complex calculations, error-correction is much more important, as these errors become inevitable with the longer, more complex quantum tasks.

In classical communication and computation, it is possible to introduce redundancy to restore corrupted information. But this doesn't work for quantum states due to the "no-cloning theorem". This theorem shows that because you cannot clone a photon, it is not possible to use redundancy in quantum states. The reasoning is as follows: First, take an incoming photon with polarization state $|s\rangle$: $|A_0\rangle|s\rangle \rightarrow |A_s\rangle|ss\rangle$, where $|A_0\rangle$ is the 'ready' state, $|A_s\rangle$ is the final state, which may or may not depend on the polarization of the original photon, and $|ss\rangle$ is the state of the radiation field where there are two photons, each with polarization $|s\rangle$. Then, assume we can clone a photon, with a vertical polarization $|\updownarrow\rangle$ and with a horizontal polarization $|\longleftrightarrow\rangle$:

$$|A_0\rangle|\updownarrow\rangle \to |A_{vert}\rangle|\updownarrow\updownarrow\rangle$$

$$|A_0\rangle|\longleftrightarrow\rangle \to |A_{hor}\rangle|\Longleftrightarrow\rangle$$

We should be able to represent this with a unitary operator. Therefore, we can say the incoming photon's polarization is the following linear combination: $\alpha|\updownarrow\rangle + \beta|\longleftrightarrow\rangle$. If we assume the photon is linearly polarized 45° such that $\alpha = \beta = 2^{-1/2}$, we get the superposition:

$$|A_0\rangle(\alpha|\updownarrow\rangle + \beta|\longleftrightarrow\rangle) \to \alpha|A_{vert}\rangle|\updownarrow\updownarrow\rangle + \beta|A_{hor}\rangle|\Longleftrightarrow\rangle$$

If the apparatus states, $|A_{vert}\rangle$ and $|A_{hor}\rangle$ are equivalent, then the two photons are in the pure state

$$\alpha|\updownarrow\updownarrow\rangle + \beta|\Longleftrightarrow\rangle$$

But this doesn't match to final state if both photons were to have the same polarization $\alpha|\updownarrow\rangle + \beta|\longleftrightarrow\rangle$, as this would have to be

$$2^{1/2}(\alpha a^{+}_{vert}\beta a^{+}_{hor})^2|0\rangle = \alpha^2|\updownarrow\updownarrow\rangle + 2^{1/2}\alpha\beta|\updownarrow\longleftrightarrow\rangle + \beta^2|\Longleftrightarrow\rangle$$

which is a pure state that differs from that found using the superposition. Therefore, no apparatus can clone a photon perfectly, and no quantum system can use redundancy as is useful in classical error-correction.

Rather than relying on duplication, quantum systems must spread information over many qubits through an encoding to correct errors. If we know how an encoding behaves under evolution by the interaction superoperator, then we can use this information to recover the original state.

Let's look at an example of encoding a single qubit, with general state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then, we map $|\Psi\rangle$ into a higher dimensional Hilbert space:

$$(\alpha|0\rangle + \beta|1\rangle)|000...\rangle \to \alpha|0_L\rangle + \beta|1_L\rangle$$

where $|0_L\rangle$ is the logical zero and $|1_L\rangle$ is the logical one of the qubit. Therefore any errors induced by a computer malfunction maps it into one of a family of two-dimensional subspaces which preserve the relative coherence of the quantum information. Then, you perform a measurement by projecting the state into one of the subspaces and then recover the original state by using a unitary transformation.

Now we want to understand what kinds of error can occur. We take the initial state as Ψ_i, which then endures an interaction with the environment. Then, we get the reduced density matrix

$$\rho_f = \$(|\Psi_i\rangle),$$

where \$ is the superoperator associated with the interaction. If the environment is not initially entangled with the system, we can say

$$\rho_f = \sum_a A_0 \rho_i A_a^{\dagger}.$$

The possible operators A_a can be found from an orthonormal basis $|\mu_a\rangle$ of the environment, the environment's initial state $|e\rangle$ and the evolution operator of the whole system, U:

$$A_a = \langle\mu_a|U|e\rangle$$

And therefore we can see that

$\sum_a A_a^\dagger A_a = I$.
Thus, A_a are linear operators, called *interaction operators*, of the Hilbert space of the system and describe the effect of the environment. A family of operators A_a which satisfy the identity relation above defines the superoperator.

There are two conditions necessary for recovery of state $|\Psi\rangle$:
$\langle 0_L|A_a^\dagger A_b|1_L\rangle = 0$,
$\langle 0_L|A_a^\dagger A_b|0_L\rangle = \langle 1_L|A_a^\dagger A_b|1_L\rangle$.
This first condition requires that logical zero and one must go to orthogonal states under any error. The second condition shows that the length and inner products of the projections of the corrupted logical zero and one should be the same.

Now we will look at *fidelity*, which is the overlap between the final state ρ_f of a system ρ and the original state $|\Psi_i\rangle$. We define the combined superoperator (containing the information regarding the interaction with the environment) and then applying a recovery operation as $A = A_0, \ldots.$ Then the fidelity is
$F(|\Psi_i\rangle, A) = \langle\Psi_i|\rho_f|\Psi_i\rangle = \sum_a \langle\Psi_i|A_a|\Psi_i\rangle\langle\Psi_i|A_a^\dagger|\Psi_i\rangle$.

The minimum, or worst case, fidelity is defined as
$F_{min} = \min_{|\Psi\rangle}\langle\Psi|\rho_f|\Psi\rangle$.

Let's look at an example of decoherence. For one qubit, the decoherence takes the form
$|\Psi_i\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \rho\begin{pmatrix}\alpha\alpha^* & \alpha\beta^* e^{-\gamma}\\ \alpha^*\beta e^{-\gamma} & \beta\beta^*\end{pmatrix}$,
where $e^{-\gamma}$ parameterizes the amount of decoherence. The decoherence can be understood as the following interaction with the environment
$|e\rangle|0\rangle \rightarrow |e_0\rangle|0\rangle \; |e\rangle|1\rangle \rightarrow |e_1\rangle|1\rangle$,
where $\langle e_0|e_1\rangle = e^{-\gamma}$. Then, using the environment bases $|\mu_0\rangle = |e_0\rangle and |\mu_1\rangle = (|e_1\rangle - e^{-\gamma}|e_0\rangle)/\sqrt{1-e^{-2\gamma}}$, we find the following interaction operators:
$A_0 = \begin{pmatrix}1 & 0\\ 0 & e^{-\gamma}\end{pmatrix}$; $A_1 = \begin{pmatrix}0 & 0\\ 0 & \sqrt{1-e^{-2\gamma}}\end{pmatrix}$.

Therefore, the minimum fidelity of a corrupted single qubit is given by
$F = \frac{1+e^{-\gamma}}{2} \approx 1 - \frac{\gamma}{2} + \ldots$, where the approximation is valid for small γ.

We can extend this for different qubits with all independent environments. We will now look at a one-qubit code that can correct for this error using three qubits. Now, using the basis state of the environment as $|\mu_+\rangle = (|e_0\rangle + |e_1\rangle)/\sqrt{2(1+e^{-\gamma}}$ and $|\mu_-\rangle = (|e_0\rangle - |e_1\rangle)/\sqrt{2(1-e^{-\gamma}}$ yields the one qubit interaction operators:
$A_+ = a_+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$; $A_- = a_-\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$,
where $a_+ = \sqrt{(1+e^{-\gamma})/2}$ and $a_- = \sqrt{(1-e^{-\gamma})/2}$. Therefore, in this basis, the environment either leaves the system alone or flips the sign if the qubit is in state $|1\rangle$. Thus, the encoding takes the form:
$|0_L\rangle = (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$
$|1_L\rangle = (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$.
So if one qubit is corrupted, it is possible to detect this by majority rule.

If there is at most one incorrect qubit, the result is one of the following:

$A_+|0_l\rangle = a_+^{3/2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$
$A_-^1|0_l\rangle = a_+^2 a_-^{1/2}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$
$A_-^2|0_l\rangle = a_+^2 a_-^{1/2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)$
$A_-^3|0_l\rangle = a_+^2 a_-^{1/2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$,
where the superscripts indicate which qubit is interacting with the environment. A similar computation for $|1_L\rangle$ holds as well.

Then, the recovery operator is the superoperator determined by the interactions
$R_+ = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)$
$R_1^1 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^1$
$R_1^2 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^2$
$R_1^3 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^3$,
where σ_z^r is the z Pauli matrix for the rth qubit.

3 Quantum error-correcting codes

3.1 Fundamentals of quantum error-correcting codes

The goal is to preserve a k-dimensional subspace against some known errors by mapping the states into a larger, n-dimensional Hilbert space.

First let's define a few key terms. $(n, k) - quantumcode$ is a k-dimensional subspace of an n-dimensional Hilbert space. This Hilbert space is also called a *coding space* and is denoted by H. The *encoding operator* for a code, C, is a unitary operator E from a k-dimensional Hilbert space Q onto C. To decode, take the right inverse of the encoding operator.

A *recovery (super)operator* R is a superoperator on the coding space. This recovery operator restores a state to the code after it's been affected by an interaction with the environment.

A *quantum error-correcting code* is a pair (C, R) consisting of a quantum code and a recovery operator. We let A be a family of linear operators. Then, the fidelity of the code is defined as
$F(C, R, A) = \min_{|\Psi\rangle \epsilon C} F(|\Psi\rangle, R, A) = \min_{|\Psi\rangle \epsilon C} \sum_{r,a} |\langle\Psi|R_r A_a|\Psi\rangle|^2$,
where R_r are the interaction operators for the superoperator R.

The *error* of the code is defined as
$E(C, RA) = \max_{|\Psi\rangle \epsilon C} \sum_{r,a} |(R_r A_a - \langle\Psi|R_r A_a|\Psi\rangle)|\Psi\rangle|^2$

In the ideal case, the code corrects all errors, or when we recover the initial state for all operators in A. This means that $E(C, RA) = 0$, and the pair (C, R) is called an *A-correcting code.*

Theorem 1. *The operator A_a is in $A(C, R)$ iff when restricted to $C, R_r A_a = \lambda_{ra}$ for each $R_r \epsilon R$. The family $A(C, R)$ is linearly closed and (C, R) is $A(C, R)$ correcting.*

Proof. To be A_a-correcting requires that for $|\psi\rangle \epsilon C$,
$|(R_r A_a - (\langle\Psi|R_r A_a|\Psi\rangle))|\Psi\rangle| = 0.$

Therefore we can see that $R_r A_a |\Psi\rangle = \lambda_{ra}(|\Psi\rangle)|\Psi\rangle$. And by the linearity of $R_r A_a$, $\lambda_{ra}(|\Psi\rangle)$ cannot depend on $|\Psi\rangle$.

3.2 Characterizations of A-correcting Codes

Let $|i_L\rangle$ represent the elements of an orthonormal basis of C. Then, the following theorem applies:

Theorem 2. *The code* C *can be extended to an* A*-correcting code iff for all basis elements $|i_L\rangle$, $|j_L\rangle$, $i \neq j$ and operators A_a, A_b in* A

$\langle i_L|A_a^\dagger A_b|i_L\rangle = \langle j_L|A_a^\dagger A_b|j_L\rangle$

and

$\langle i_L|A_a^\dagger A_b|j_L\rangle = 0.$

Proof. Assume that (C, R) is an A-correcting code. Then

$$\begin{aligned}\langle i_L|A_a^\dagger A_b|j_L\rangle = \langle i_L|A_a^\dagger I A_b|j_L\rangle &= \langle i_L|A_a^\dagger \sum_r R_r^\dagger R_r A_b|j_L\rangle \\ &= \sum_r \langle i_L|A_a^\dagger R_r^\dagger R_r A_b|j_L\rangle \\ &= \sum_r \langle i_L|\overline{\lambda_{ar}}\lambda_{br} R_r^\dagger R_r A_b|j_L\rangle \\ &= \alpha_{ab}\delta_{ij},\end{aligned}$$

where we have used Theorem 1.

Now, we are going to construct a recovery operator given that $\langle i_L|A_a^\dagger A_b|i_L\rangle = \langle j_L|A_a^\dagger A_b|j_L\rangle$ and $\langle i_L|A_a^\dagger A_b|j_L\rangle = 0$ hold. Let V^i denote the subspace spanned by $A_a|i_L\rangle$ for all a. Let $|\nu_r^i\rangle$ be an orthonormal basis for V^i. Therefore, there exist unitary V_r which return $|\nu_r^i\rangle$ to the corresponding state $|i_L\rangle$:

$V_r|\nu_r^i\rangle = |i_L\rangle$.

The recovery operator is given by the interaction operators: $R = \{O,\ R_1,\ ...,\ R_r,\ ...\}$, where O is the projection onto the orthogonal complement of $\oplus_i V^i$, which is also the part of the Hilbert space that isn't reached by acting on the code with A_a, and

$R_r = V_r \sum_i |\nu_r^i\rangle\langle v_r^i|$.

To make sure that R recovers the state, we must find unitary operations U_i such that $U_i|\nu_r^0\rangle = |nu_r^i\rangle$ and for all A_a, $U_i A_a|0_L\rangle = A_a|i_L\rangle$. Now, we choose the basis $|\nu_r^0\rangle$ of V^0 and defining $|\nu_r^i\rangle = U_i|v_r^0\rangle$.

Now, we show that R does recover the state, as we can write:

$$\begin{aligned} A_a|\Psi\rangle = A_a \sum_i \alpha_i |i_L\rangle &= \sum_i \alpha_{ia}|i_L\rangle \\ &= \sum_i \alpha_i U_i A_a |0_L\rangle \\ &= \sum_{i,r} \alpha_i U_i \beta^0_{ar} |\nu^0_r\rangle \\ &= \alpha_i \beta^0_{ar} |\nu^i_r\rangle, \end{aligned}$$

where the identities define α_i and β^0_{ar} by expansion in terms of the corresponding basis elements. Then, we can find that

$$\begin{aligned} R_r A_a |\Psi\rangle = \sum_i V_r |\nu^i_r\rangle\langle v^i_r| \sum_{j,s} \alpha_j \beta^0_{as} |\nu^j_s\rangle &= \sum_i \alpha_i \beta^0_{ar} V_r |\nu^i_r\rangle \\ &= \sum_i \beta^0_{ar} \alpha_i |i_L\rangle \\ &= \beta^0_{ar} |\Psi\rangle. \end{aligned}$$

This therefore shows that $R_r A_a$ is a multiple of the identity applied to C.

Now, let's look at an example. Consider the code $|0_L\rangle = |00\rangle, |1_L\rangle = |11\rangle$ subject to the interaction operators $A_0 = \begin{pmatrix} \sqrt{1-2q} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \sqrt{1-2q} \end{pmatrix}$, $A_1 = \begin{pmatrix} \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \\ \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \end{pmatrix}$, $A_2 = \begin{pmatrix} \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \\ -\sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\sqrt{q/2} \end{pmatrix}$, for some fixed $0 < q < 1$. These operators form a superoperator, as they're linearly independent and cannot be reduced to smaller, equivalent interactions. The A_i map the logical states as follows:

$|0_L\rangle \to \sqrt{1-2q}|00\rangle, \sqrt{q/2}(|00\rangle + |10\rangle), \sqrt{q/2}(|00\rangle - |10\rangle)$
$|1_L\rangle \to \sqrt{1-2q}|11\rangle, \sqrt{q/2}(|01\rangle + |11\rangle), \sqrt{q/2}(|01\rangle - |11\rangle)$.

Interestingly, one of the states is linearly dependent on the other two states in each case, so we only need two recovery operators to retrieve the initial state:

$R_0 = |00\rangle\langle 00| + |11\rangle\langle 11|; R_1 = |00\rangle\langle 01| + |11\rangle\langle 01|$

Next, the text lays out numerous theorems and their respective proofs.

Theorem 3. *Let A be a superoperator. C is an A-correcting code iff the restriction of A to C has a left superoperator inverse.*

Proof. By Theorem 1, C is an A-correcting code iff there exists a superoperator R such that on $C, R_r A_a = \lambda_{ra} I$ for all r and a. This means that RA is a superoperator equivalent to the identity.

Theorem 4. *B has error 0 on C iff $I \otimes B \sum_i |i_L\rangle|i_L\rangle = \lambda \sum_i |i_L\rangle|i_L\rangle$.*

Proof. Let B_r be a member of B. Then, $I \otimes B_r$ is a member of $I \otimes B$. If B has error 0 on C, then
$I \otimes B_r \sum_i |i_L\rangle|i_L\rangle = \sum_i |i_L\rangle B_r|i_L\rangle = \sum_i |i_L\rangle\lambda_r|i_L\rangle = \lambda_r \sum_i |i_L\rangle|i_L\rangle$.

This shows that the ensemble $I \otimes B_r \sum_i |i_L\rangle|i_L\rangle$ is the same as a scalar multiple of $\sum_i |i_L\rangle|i_L\rangle$.

Theorem 5. *C is an A-correcting code iff there is an isomorphism σ: $H \simeq C \otimes E \otimes D$ such that for all $A_a\epsilon$ and $|\Psi\rangle\epsilon C$, $A_a|\Psi\rangle = \sigma(|\Psi\rangle \otimes |E(a)\rangle$*

Proof. Let C be an A-correcting code in H. We use the notation from Theorem 2. Let D denote the orthogonal complement of the subspace spanned by the $|\nu_r^i\rangle$. Let E be the Hilbert space spanned by $|\nu_r^i\rangle_r$. The isomorphism between H and $C \otimes E \otimes D$ is established by letting $\sigma(|i_L\rangle|\nu_r^0\rangle = |\nu_r^i\rangle$ and defining σ to be the identity map on D. Let $A_a\epsilon A$ and $|\Psi\rangle = \sum_j \alpha_j|j_L\rangle\epsilon C$. Write $A_a|0_L\rangle = \sum_r \beta_{ra}^0|\nu_r^0\rangle$. Applying properties discussed in Theorem 2 yields
$A_a|\Psi\rangle = \sum_{jr} \alpha_j\beta_{ra}^0|\nu_r^j\rangle$
$= \sigma(\sum_j \alpha_j|j_L\rangle \otimes \sum_r \beta_{ra}^0|\nu_r^0\rangle)$
$= \sigma(|\Psi\rangle \otimes \sum_r \beta_{ra}^0|\nu_r^0\rangle)$.

Theorem 6. *Let A be a superoperator. Then C is an A-correcting code iff $S(\overline{\rho}) - S(\rho) = \log k$.*