Quantum information theory (20110401)

Lecturer: Jens Eisert

Chapter 13: Quantum error correction

Contents

Chapter 13

Quantum error correction

Quantum error correction is one of the most important ideas of the field of quantum information theory. Without it, quantum computers can presumably not be more powerful than classical computers (with exceptions in rather delicate situations where the practical use is not entirely clear). In fact, error correction is already important for classical computers and any kind of classical information transmission. However, here the issue of error correction is much easier to tackle. One can simply make use of *redundancy* to protect encoded information. One can, e.g., encode a bit as

$$0 \mapsto 000, \quad 1 \mapsto 111. \tag{13.1}$$

If these physical bits are subjected to noise, one can make use of a majority rule. If the noise levels are then sufficiently small, one can correct for errors. The same idea will not immediately work in the quantum realm.

- One cannot perform measurements of unknown quantum states in general and learn about the quantum state without altering it.

- Then, one cannot simply copy quantum information. A map of the type

  $$\rho \mapsto \rho \otimes \rho \otimes \rho \tag{13.2}$$

  for unknown quantum states ρ is not linear, not a valid quantum operation or quantum channel, and forbidden by the *no cloning theorem*. Unknown quantum information cannot be copied.

- Also, one is facing a continuous families of errors in the quantum setting.

All this was seen as an obstacle against the possibility of performing quantum computing for quite a while. Only the advent of quantum error correction overcame these obstacles. It is a deep and important theory, and – needless to say – one that overcomes the above obstacles and identifies them as prejudice.

13.1 Peres code

13.1.1 Bit flip errors

We start by discussing the first code in the quantum realm, the so-called *Peres code*. It is not quite a quantum error correcting code in the strict sense yet: It cannot protect against a single general quantum error. But it can correct for single errors in a given basis. And it shows nicely how the above obstacles can be overcome. We discuss the encoding of pure states only, but it should be clear that this does not restrict generality. So let us assume we are given a single qubit. We would like to protect this qubit against *bit flip errors*. These are given by the application of Pauli-X operations as

$$|0\rangle \mapsto X|0\rangle = |1\rangle, \tag{13.3}$$
$$|1\rangle \mapsto X|1\rangle = |0\rangle. \tag{13.4}$$

So let us assume this qubit is initially in a pure state described by a state vector

$$|\psi\rangle_L = \alpha|0\rangle_L + \beta|1\rangle_L, \tag{13.5}$$

for $\alpha, \beta \in \mathbb{C}$. The index L indicates that this is the *logical information* we wish to protect. This qubit can be protected by an encoding of the type

$$|0\rangle_L \mapsto |0,0,0\rangle, |1\rangle_L \mapsto |1,1,1\rangle \tag{13.6}$$

so that the encoded state vector becomes

$$|\psi\rangle_L \mapsto \alpha|0,0,0\rangle + \beta|1,1,1\rangle. \tag{13.7}$$

The latter three qubits are referred to as *physical qubits*. But have we not violated the no-cloning theorem here? We have not, as this is a perfectly linear operation. In fact, a moment of thought reveals that this can be easily encoded making use of two CNOT quantum gates. Also, a single measurement in the Z basis would collapse the state, so that a further measurement does not reveal information about the superposition. So how can we find out whether an error has occurred? In case of either no error or a single bit flip error, we will obtain one of the four state vectors,

$$\alpha|0,0,0\rangle + \beta|1,1,1\rangle, \tag{13.8}$$
$$\alpha|1,0,0\rangle + \beta|0,1,1\rangle, \tag{13.9}$$
$$\alpha|0,1,0\rangle + \beta|1,0,1\rangle, \tag{13.10}$$
$$\alpha|0,0,1\rangle + \beta|1,1,0\rangle. \tag{13.11}$$

These are precisely the state vectors we obtain in case of no error, and applying the bit flip to the first, the second, or the third physical qubit. There is one key property these state vectors have: They are all mutually orthogonal! This is true regardless of the values of α, β. In fact, the entire respective two-dimensional complex subspaces are orthogonal.

13.1.2 Encoding and correction

In the following measurement, one obtains in fact no information whatsoever about the logical information encoded: That would indeed be detrimental and alter the logical information. This measurement identifies the kind of error, without learning about the encoded state, which is hence unaltered by means of this measurement. One performs a projective measurement involving the four projections

$$P := P_0 := |0,0,0\rangle\langle 0,0,0| + |1,1,1\rangle\langle 1,1,1|, \tag{13.12}$$
$$P_1 := |1,0,0\rangle\langle 1,0,0| + |0,1,1\rangle\langle 0,1,1|, \tag{13.13}$$
$$P_2 := |0,1,0\rangle\langle 0,1,0| + |1,0,1\rangle\langle 1,0,1|, \tag{13.14}$$
$$P_3 := |0,0,1\rangle\langle 0,0,1| + |1,1,0\rangle\langle 1,1,0|. \tag{13.15}$$

The first projection P is the projection onto the code space. Has no error occurred, we will receive $P = P_0$, otherwise, we get one of the outcomes associated with P_1, P_2, or P_3. This will identify the error which can subsequently be corrected.

There is another picture of the problem that we will later make use of when considering stabilizer codes. Let us assume that instead of measuring $P_0, \ldots, P_3$, we measure the observabkes

$$Z_1 Z_2 = Z_1 \otimes Z_2 \otimes \mathbb{I} \tag{13.16}$$

and

$$Z_2 Z_3 = \mathbb{I} \otimes Z_2 \otimes Z_3. \tag{13.17}$$

Each of these observables has eigenvalues ± 1, so that the two measurements provide two bits of information. This is enough diagnostic information to detect the errors. What is more, one can interpret the measurement of the first two qubits as comparing whether the two qubits are the same. To see why this is the case, let us consider the spectral decomposition of $Z_1 Z_2$. This is

$$Z_1 Z_2 = (+1)(|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1|) + (-1)(|0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0|). \tag{13.18}$$

That is to say, the eigenvalue indeed allows to compare the states. In the same fashion, one can interpret the measurement outcomes of the latter two qubits. Again, this measurement provide precisely provide the information required to detect the error, but not more. To reiterate, one gets information about the error, but not the logical information encoded. In the light of all this, it is obvious how a correction works:

$$P_0 : \text{Apply } \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I}, \tag{13.19}$$
$$P_1 : \text{Apply } X \otimes \mathbb{I} \otimes \mathbb{I}, \tag{13.20}$$
$$P_2 : \text{Apply } \mathbb{I} \otimes X \otimes \mathbb{I}, \tag{13.21}$$
$$P_3 : \text{Apply } \mathbb{I} \otimes \mathbb{I} \otimes X. \tag{13.22}$$

A moment of thought reveals that the state after the correction is again the original one. Of course, this only works if at most a single error occurs. If an error occurs with probability p, this procedure reduces the error rate to p^2.

13.2 Shor's 9-qubit code

13.2.1 Phase flip errors

The Peres code is no actual quantum error correction code. It fails for *phase flip errors*. A phase flip is an error of the kind

$$|0\rangle \mapsto Z|0\rangle = |0\rangle, \tag{13.23}$$
$$|1\rangle \mapsto Z|1\rangle = -|1\rangle. \tag{13.24}$$

This error has no classical analogon. Instead of applying a Pauli X gate, one here applies the Pauli Z quantum gate. How can we correct against such errors? This seems very simple: A phase error is a bit flip error in a different basis. We can simply work in the basis $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, so that the phase flip takes the action $|+\rangle \mapsto |-\rangle$ and $|-\rangle \mapsto |+\rangle$ and hence is nothing but a bit flip error in a different basis. Therefore, an obvious choice of encoding involves code words spanned by $|+,+,+\rangle$ and $|-,-,-\rangle$. This, in turn, can be achieved by a row of Hadamard gates. After the error correction, one can per Hadamard transformation $H^{-1} = H$, go back to the original basis.

13.2.2 General single qubit errors

This is great, but of course, this new strategy works for phase flip errors alone. If we additionally have bit flip errors as before, one cannot determine the error by means of measurement. There is an even more severe problem: This occurs if the error appears due to an interaction with the environment. If the error occurs due to an interaction

$$|0\rangle \otimes |\psi_0\rangle \mapsto |0\rangle \otimes |\psi_0\rangle, \tag{13.25}$$
$$|1\rangle \otimes |\psi_0\rangle \mapsto |1\rangle \otimes |\psi_1\rangle, \tag{13.26}$$

generating entanglement between the system and its environment that is hard to get rid of. The *Shor code* tackles these problems at once and is indeed a full *quantum error correcting code*. It allows to correct an arbitrary single error of any qubit. The most general error leads to

$$\begin{aligned}(\alpha|0\rangle + \beta|1\rangle) \otimes |\psi_0\rangle \mapsto\ & (\alpha|0\rangle + \beta|1\rangle) \otimes |\psi_0\rangle \\ +\ & (\alpha|1\rangle + \beta|0\rangle) \otimes |\psi_1\rangle \\ +\ & (\alpha|0\rangle - \beta|1\rangle) \otimes |\psi_2\rangle \\ +\ & (\alpha|1\rangle - \beta|0\rangle) \otimes |\psi_3\rangle.\end{aligned} \tag{13.27}$$

In a Pauli language, and restricting to the physical systems at hand, these are X_i, Pauli X errors on the i-th physical qubit, Z_i, Pauli Z errors on the i-th physical qubit, and X_iZ_i, basically Pauli Y errors on the i-th physical qubit. So once we have understood Pauli X and Z errors, we are in business.

13.2.3 Shor code

The *Shor code* encodes a logical qubit in the following fashion

$$|0\rangle_L \mapsto (|0,0,0\rangle - |1,1,1\rangle) \otimes (|0,0,0\rangle - |1,1,1\rangle) \otimes (|0,0,0\rangle - |1,1,1\rangle)/\sqrt{8},$$
$$|1\rangle_L \mapsto (|0,0,0\rangle + |1,1,1\rangle) \otimes (|0,0,0\rangle + |1,1,1\rangle) \otimes (|0,0,0\rangle + |1,1,1\rangle)/\sqrt{8}. \tag{13.28}$$

That is to say, a single logical qubit is being encoded in nine physical qubits, hence a nine qubit code. A moment of thought reveals what is happening here. One first encodes

$$|0\rangle_L \mapsto |-,-,-\rangle, \tag{13.29}$$
$$|1\rangle_L \mapsto |+,+,+\rangle \tag{13.30}$$

in a phase flip code, one rotates the basis and then implements a bit flip Peres code. So the Shor code is nothing but a concatenated code that protects against phase and bit flip errors separately. It takes a moment of thought to understand that this is indeed good enough to protect against arbitrary errors on a single qubit.

13.2.4 Kraus decomposition of single qubit errors

Indeed, the above code is able to correct for all (continuous) single qubit errors. Such errors can be corrected with a discrete set of quantum error correcting codes. A general error is described by a quantum channel T. This is a completely positive, trace-preserving map as we have encountered it earlier in this course. In its Kraus decomposition, one finds

$$\rho \mapsto T(\rho) \sum_{k=1}^{K} E_k \rho E_k^\dagger, \tag{13.31}$$

with

$$\sum_{k=1}^{K} E_k^\dagger E_k = \mathbb{I}. \tag{13.32}$$

What happens for each summand $E_k \rho E_k^\dagger$? If these Kraus operators act on a single qubit only, we can decompose them as

$$E_k = e_{k,0}\mathbb{I} + e_{k,1}X + e_{k,2}XZ + e_{k,3}Z. \tag{13.33}$$

Obviously, from the Pauli algebra, we also know that

$$Y = iXZ \tag{13.34}$$

Therefore, for this decomposition, the above Shor code as a quantum error correcting code can correct against arbitrary single errors.

13.3 Elements of quantum error correction

13.3.1 Encoding logical information

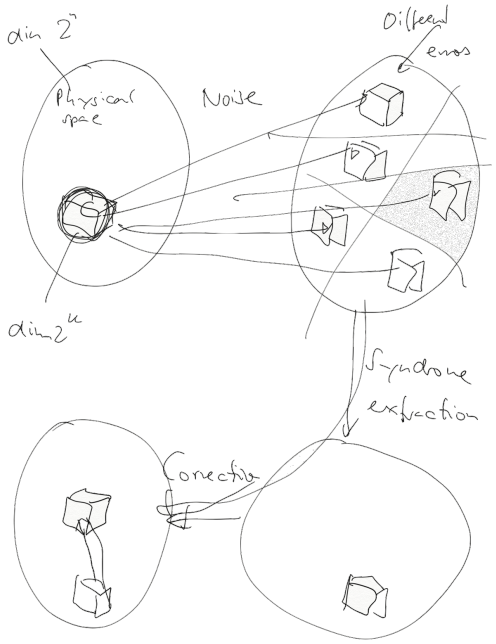
The above ideas provide the building ground for a general theory of quantum error correction. A quantum error correcting code $\mathcal{C}$ is a subspace $\mathcal{C} \subset (\mathbb{C}^2)^{\otimes n}$ of an n qubit system. An encoding can be seen as a unitary

$$|\psi\rangle_L \mapsto U(|\psi\rangle_L \otimes |0\rangle \dots |0\rangle) \subset \mathcal{C}. \tag{13.35}$$

We can as before denote with P the projection onto the subspace $\mathcal{C}$. If the logical information involves k qubits, so if

$$|\psi\rangle_L \in (\mathbb{C}^2)^{\otimes k} =: \mathcal{L}, \tag{13.36}$$

then we aim at encoding k logical qubits in n physical qubits, giving rise to the physical space $\mathcal{P}$. $\mathcal{L}$ we call the logical subspace. After the encoding, the physical qubits are being subjected to quantum noise, so to quantum channels. These errors will transform the states, but in fact, will map the logical subspace $\mathcal{L}$ into separate subspaces of $\mathcal{P}$ which are mutually orthogonal. This is why one can perform measurements and can identify the type of error has occurred without altering the logical quantum information encoded. This step is called the *syndrome extraction*. It is the entire subspace that is transformed. Once the error has been identified, one can shift the subspace back to $\mathcal{C}$, and the error has been corrected for.



Again, it is important that different error syndromes correspond to orthogonal subspaces. Otherwise, we cannot discriminate them in a lossless fashion, would learn

about the encoded information and would hence alter the quantum state at hand. What is more, the error must not deform the subspaces, and hence must within those subspaces map orthogonal state vectors onto orthogonal state vectors. Otherwise, no perfect quantum error correction is possible.

13.3.2 Knill-Laflamme conditions

The general theory of quantum error correction make a few assumptions (which are way more realistic than they may at first look like). In this general framework, one assumes that

- the errors are described by quantum channels T, and
- the correction is described by quantum operations R.
- For every state supported on $\mathcal{C}$, one has

$$(R \circ T)(\rho) = \rho. \tag{13.37}$$

These conditions can be satisfied if the so-called *Knill-Laflamme conditions* are met. This is a pretty deep insight in the theory of quantum error correction. Note that as it is formulated, it rather guarantees the existance of a recovery, but does not quite deliver this recovery explicitly.

Knill-Laflamme conditions: Let $\mathcal{C}$ be a quantum error correcting code and P the projection onto $\mathcal{C}$. Let T be a quantum operation (trace-preserving, completely positive) with Kraus operators $\{E_k\}$. Then there exists a recovery operation R that corrects for T on $\mathcal{C}$ exactly if

$$PE_i^\dagger E_j P = A_{i,j} P \tag{13.38}$$

with an arbitrary Hermitian matrix $A = A^\dagger$. The elements $\{E_k\}$ are called errors, and if such an R exists, $\{E_k\}$ is called a correctable set of errors.

If A in the Knill-Laflamme conditions has full rank, the code is called a *non-generate code*. Otherwise, it is called *degenerate*. Interestingly, the Shor code falls into the latter category.

13.3.3 Quantum Hamming bound

Can arbitrary errors be corrected for in an arbitrarily economical fashion? Surely not, we have to deal with some sort of redundancy and overhead. k logical qubits are encoded in n physical qubits, and n is usually much larger than k. In case of the Shor code, we have encoded one $k = 1$ logical qubit into $n = 9$ physical qubits. How many do we actually need? This is a question that is easy to answer for non-degenerate codes (which we look at here) and not so easy for non-degenerate codes (that we do

not consider here). For the former, if one wants to encode k qubits in a non-degenerate fashion, each error must correspond to a 2^k-dimensional subspace. All these subspaces have to "fit into" the physical space $\mathcal{P} = (\mathbb{C}^2)^{\otimes n}$. This leads to the following condition, arising from purely combinatorical considerations.

Quantum Hamming bound: Non-degenerate quantum codes encoding k logical qubits into n physical qubits correcting for t errors must satisfy

$$\sum_{j=0}^{t} 3^j 2^k \binom{n}{j} \leq 2^n. \tag{13.39}$$

Another bound that is similarly important is the *Singleton bound*.

13.3.4 Distance of a code

Indeed, the smallest quantum error correcting code that can correct for arbitrary single qubit errors for $k = 1$ and $t = 1$ involves $n = 5$ qubits (which is already an improvement over the Shor code). There cannot be a quantum error correcting code involving a smaller number of physical qubits. t is also called the *weight* of the error. A code that corrects t errors is said to have *distance* $2t + 1$, because it takes $2t + 1$ single-qubit changes to get from one code word to another. The general notation is

$$[[n, k, d]] \tag{13.40}$$

for a quantum error correcting code for k logical qubits, involving n physical qubits, of distance d. The optimal five qubit code is a $[[5, 1, 3]]$ quantum error correcting code.

13.4 Stabilizer codes

13.4.1 General theory of stabilizer quantum error correcting codes

A particularly important class of quantum error correcting codes is given by so-called *stabilizer codes*. In fact, we have to an extent already anticipated them above. We have seen in the Peres code where it is sufficient to measure $Z_1 Z_2$ and $Z_2 Z_3$. But the same strategy works also for the more elaborate Shor code. We can then measure the same for the second and the third group of qubits, so $Z_4 Z_5$ and $Z_5 Z_6$ as well as $Z_7 Z_8$ and $Z_8 Z_9$. Subsequently, we must figure out if the three signs are the same or different. We do this by measuring

$$X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes \mathbb{I} \otimes \mathbb{I} \otimes \mathbb{I} \tag{13.41}$$

and

$$\mathbb{I} \otimes \mathbb{I} \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes \mathbb{I}. \tag{13.42}$$

All the Pauli operators we need to measure can hence be collected in a table. We are in

Z	Z	I	I	I	I	I	I	I
I	Z	Z	I	I	I	I	I	I
I	I	I	Z	Z	I	I	I	I
I	I	I	I	Z	Z	I	I	I
I	I	I	I	I	I	Z	Z	I
I	I	I	I	I	I	I	Z	Z
X	X	X	X	X	X	I	I	I
I	I	I	X	X	X	X	X	X

each case measuring an operator M that has a spectrum $\{-1, 1\}$. It should have have eigenvalue +1 for any codeword

$$M|\psi\rangle = |\psi\rangle \tag{13.43}$$

If an error E which anti-commutes with M has occurred, then the true state vector is $E|\psi\rangle$,

$$M(E|\psi\rangle) = -EM|\psi\rangle = -E|\psi\rangle. \tag{13.44}$$

That is, the new state vector has eigenvalue -1 instead of $+1$. We can use this fact to correct errors. Each single-qubit error E anti- commutes with a particular set of operators M, which set, exactly, tells us what E is.

Stabilizer codes: The Pauli operators characterizing a stabilizer quantum error correcting code generate an Abelian sub-group of the Pauli group called the stabilizer of the code. The stabilizer contains all operators M in the Pauli group for which

$$M|\psi\rangle = |\psi\rangle \tag{13.45}$$

in the code $\mathcal{C}$.

Most known and practically relevant quantum error correcting codes are stabilized codes.

13.4.2 Toric and surface codes

The toric code is a stabilizer code, and in addition a topological quantum error correcting code. It is the practically most important code considered to date. It is topological in that the number k of logical qubits to be encoded depends on the topology on the manifold on which the code is considered. It is a stabilized codes involving two types of stabilizers involving four Pauli X and Z operators at the time. What is more, the distance d of the code grows with the size of the qubit lattice on which the code is defined. The *toric code* constitutes the basic code, while the *surface code* is the practically more important planar instance. A later version of the script will be much more elaborate in this respect.