Fighting Entanglement with Entanglement

On Decoherence in Quantum Systems and Quantum Error Correction

Søren Stenild Juhl Sune Lehmann

Bach. Sc. in Physics
University of Copenhagen
Supervisor: Benny Lautrup, The Niels Bohr Institute
January – May 2000

Acknowledgements

We would like to thank Klaus Mølmer at Århus Universitet for helpful advice and for spending so much time helping us through times of trouble. We also owe thanks to our supervisor Benny Lautrup for the many stimulating conversations.

Contents

List of Figures

1 Introduction

Right now it is impossible to say if we can scale these technologies ... But if you had asked me five years ago if we could build a 7-qubit quantum computer in five years, I would have said it was impossible ... On my optimistic days I think we will have quantum computers in 20, 30, 40 years maybe ... on my pessimistic days, I think quantum computing is crazy.

Raymond Laflamme in *Wired* [27].

The theory of Quantum Computers has evolved tremendously during the past 15 years. – Envisioned by Feynmann and independently by Benioff in 1982 [18, 2], quantum computers received relatively little attention until the beginning of the 1990's when David Deutsch showed that quantum computers had powers far beyond those of the classical computer [10]. In 1994, when Peter Shor showed that quantum computers could factor large numbers *efficiently* [38], everybody started paying attention to quantum computing and since then it has grown to become one of the most exciting fields of modern physics.

Fairly early on it was pointed out [29, 43, 23] that a quantum computer is a very fragile system which will unavoidably interact with the environment. These interactions disturb the delicate quantum states, destroying the calculations. Therefore it was widely believed that quantum computing would be impossible to carry out experimentally, until 1995 when Peter Shor and Andrew Steane independently developed schemes for reducing the damage done by the environment [39, 40].

1.1 The Present Report

Error correction is of paramount importance to quantum computing and in this report we will describe the physical mechanisms behind the errors, i.e. the interactions between the environment and the quantum system, the *decoherence*. Afterwards we will explore the ways in which physicists have overcome the difficulties in correcting errors in delicate quantum systems. Let us make things a bit more explicit:

After the introductory sections (*Introduction* and *Basics*) where we provide the reader with the tools to understand the quantum computing, the report will fall into two distinct parts. In the first part, *Decoherence* we will discuss common properties of decoherence in all physical systems, and we will also take the time to present a beautiful mathematical formalism for describing decoherence. This part of the report is not intended as an introduction to "decoherence in quantum computers", but as an exploration of the fundamental *physics* of decoherence – the physical mechanisms behind all of the vast numerical calculations.

Having understood what decoherence is, we will take a thorough look at the errors caused by decoherence and the quantum error correcting codes which correct these, in the section *Quantum Error Correction*. We will discuss the first quantum error correcting code, Shor's nine qubit code. Having understood the mechanisms of quantum error correction, we will be ready to approach a more general class of codes, the *Calderbank, Shor, and Steane* (CSS) codes, of which Steane's seven qubit code is a very important example. The final section *Perspectives* will round off the report, with a brief look at experiments concerning quantum error correction.

1.2 Technology

The question any physicist asks himself is: *When can I get my hands on a quantum computer* – have they built one yet? We think that this is an important question to ask and before we get started, we will answer it by supplying a popular introduction to the current technology used to implement quantum computers. After this we will describe the theory of quantum computers more stringently and in depth, before returning to the real subject at hand: Errors and quantum error correction!

The theory of quantum computers has been an area of rapid growth, but as we will see, the technological implementations of quantum computers have not advanced at quite the same pace. The following is by no means a complete comment on the extensive field of quantum computing technology, and should be considered no more than a brief answer to the above question. Addressing the question of technology at this early stage, we are unable to make use of the "appropriate" nomenclature, but we believe that a popular introduction will make the rather theoretical contents of this report more accessible to the general reader.

1.2.1 The Quantum Computer

To build a quantum computer, one basically needs two things

A quantum hard drive. This is usually called a quantum register – physically this is n two-state systems; also known as quantum bits or *qubits*. It is evident that we must be able to initialize these qubits and measure them reliably in order to attain a usable readout of our results.

In order to prevent the interactions that destroy the quantum superpositions, it is also very important that we can effectively isolate the register from the environment. In other words: We need reliable storage facilities.

A quantum processor. A processor for a universal[1] quantum computer should be able to perform any unitary operation on an n-qubit system. As we will discuss in section 2.4.3 this is equivalent to being able to perform any unitary operation on a single qubit and conditional operations on two qubits, i.e. regarding the two qubit operations, the action on the second qubit must depend on the state of first qubit. These unitary operations are referred to as *quantum gates*.

To perform a reliable calculation, gates that can be implemented with a high degree of accuracy are needed. – Only errors of a fraction of a percent are acceptable, otherwise errors will accumulate and ruin the computations [34].

Implementations of single qubit operations are relatively easy, but this is not the case for the conditional two qubit gates. Two qubit gates require that the interaction with the external apparatus (which implements the gate) depends on the fragile quantum correlations between the quantum bits.

1.2.2 Quantum Parallelism

The thing that really separates quantum computers from classical computers is *quantum parallelism*: A qubit is potentially a quantum superposition of $|0\rangle$ and $|1\rangle$, so – in a sense – a qubit can "occupy both states". Potentially then, we can use a superposition state of n qubits to parallel process 2^n bits in one computational step, a feat that would take a classical computer 2^n computations. Only a small class of problems can be solved exponentially faster by a quantum computer, though, for example Shor's algorithm [38] and Deutsch's problem, cf. [10], because when we measure the n qubit register, we project the superposition onto a basis state, thus collapsing the superposition.

1.2.3 The Ion Trap

This contraption was invented by Cirac and Zoller [7], and is basically a string of ions trapped in an electric field in a high vacuum. Transitions between the $|g\rangle$round state $\equiv |0\rangle$ and a long lived $|e\rangle$xcited state $\equiv |1\rangle$ and rotations (superpositions of $|g\rangle$ and $|e\rangle$) are induced via laser pulses. The two qubit operations are realized by way of the mutual ionic Coulomb repulsion, which results in a collective vibration of the whole string of ions with a common frequency as the motion is quantized (Mößbauer effect). The quantum states of motion correspond to the different degrees of excitation of the normal modes of string vibration. The normal modes of vibrations are excited (or absorbed) by the laser photon momentum; this mechanism makes it possible to transfer information between any two ions, permitting the execution of conditional two qubit gates. The actual execution of the conditional two qubit gates is rather complicated, and we will not go into any detail here. The reader is referred to [42] or the original proposal by Cirac and Zoller [7] for an introduction to the subject.

The ion trap is initialized by laser cooling, whilst the final state is "read" through laser fluorescence. Control of the noise, requires temperatures lower than 1μK and shielding from noise voltage. Noise is the main limitation of increasing the computational capacity. Furthermore, it has been pointed out that the uncertainty relation between time and energy severely limits the speed of the ion trap, cf. [35]. The uncertainty in the energy of the laser photons should be small compared to the differences of the characteristic vibrational frequencies ν, so each laser pulse should last a long time compared to ν^{-1}. In the experiments ν is of the order 100 kHz; this fact makes the ion trap intrinsically slow.

[1] Cf. section 2.4.3

A thorough review of the ion trap can be found in [42] by Andrew Steane and shorter ones can be found in [41, 34] and [22]. So far the best experimental result is that an Innsbruck group has managed to cool ten ions to the ground state [1], but conditional gates have yet to be executed. A group in Boulder has recently created a maximally entangled state of four atoms [13]. The predictions for the register size of the ion trap varies from being able to process 10 to 50 qubits [22].

1.2.4 NMR

Nuclear **M**agnetic **R**esonance was first considered as a means for quantum computation by Gershenfeld and Chuang in 1996 [19] and simultaneously by Cory *et al.* [8][2]. A qubit is represented by the two spin states of a spin-$\frac{1}{2}$ atomic nucleus in a magnetic field: $|\uparrow_z\rangle \equiv |0\rangle$ and $|\downarrow_z\rangle \equiv |1\rangle$. The nuclei are parts of a molecule situated in large magnetic field. The spin states of the nuclei are manipulated by applying oscillating magnetic fields in pulses of controlled duration. Because of magnetic dipole-dipole interactions, the resonance frequencies depend on the orientation of the neighboring spins. This coupling makes it possible to perform the necessary conditional two qubit operation.

Since the signal of one nucleus is too weak to be detected, NMR experiments are performed on liquid compounds with $\mathcal{O}(10^{23})$ molecules at room temperature. The collective spin state is then measured, but since each of the molecules in the liquid feels a slightly differing local field because of the other molecules, the state of every molecule evolves differently. We do not have the time to go into any detail of how this problem is circumvented, but only state that a standard tool in NMR, the spin echo technique, is used.

Since NMR is carried out at room temperature, the different spin states are initially Boltzmann distributed, and to initialize the quantum computer, it is required to bring these from a thermal equilibrium to a highly organized state. To do so, the signal has to be cleverly extracted.

The coherent quantum signal appears only as a small deviation from the incoherent thermal background, but because the spins are close in energy, the density matrix $\boldsymbol{\rho}$ is nearly the identity matrix, $\mathbf{1}_{10^{23}}$. The difference $\boldsymbol{\Delta} = \boldsymbol{\rho} - \mathbf{1}$ then picks out the signal. By means of well-chosen field pulses, the traceless part of the density matrix, $\boldsymbol{\Delta}$ can be initialized, manipulated and measured just like a quantum state, and hence it can be considered to represent an effective quantum computer [34].

NMR has been very successful performing manipulations equivalent in complexity to those required for quantum computing with a few qubits. The problem is that NMR does not scale very well as the number of qubits is increased: With n qubits, the measured signal scales as 2^{-n}. Another problem is that the possibility of presicion measurement is impaired, since only the ensemble average is available. This makes applications of error correction more toilsome and also demands more of the quantum algorithms, since a probabilistic outcome must be allowed for.

Experimentally NMR works far better than the ion trap. Recently a seven-qubit NMR quantum computer has been constructed [27] and Grover's database search algorithm [21] has been implemented on three qubits [16], as well as Deutsh's problem [6]. One should note, though, that because NMR does not scale up very well, the limit on the number of qubits is expected to be about 15 [27].

1.2.5 Other Approaches

The ion trap and NMR are the most promising experimental implementations of quantum computers, but other systems suitable for quantum computation have been proposed, cf. Gruska [22] for further discussion. We will list them below for completeness, but not discuss them further, since these experiments have not been at all as successful as the ion trap and NMR.

- Cavity QED
- Quantum Dots
- Super-Conducting Quantum Interference Devices (SQUIDs)
- A Combination of NMR technology with semiconductor physics

This concludes the experimental review, and we will now move on to take a look at the fundamental *theory* behind quantum computers.

[2]To both of whom the reader is referred for an exhaustive analysis. Our review is based primarily on [42, 22, 34]

2 Basics

In this section we will introduce the quantum mechanical concepts necessary to understand quantum computing, decoherence, and quantum error correction. Some concepts have been mentioned in the previous sections, but here we will provide a stringent presentation of the theory.

2.1 The Qubit

The fundamental unit of classical information theory is the bit. A bit can assume only the values 0 and 1. In quantum information theory, the building block is the *qubit* which is represented by a state in a two-dimensional Hilbert space with orthonormal basis $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1, \quad a, b \in \mathbb{C} \tag{2.1}$$

As opposed to the classical bit, the qubit can exist as any superposition of $|0\rangle$ and $|1\rangle$, and a measurement in the standard basis, $\{|0\rangle, |1\rangle\}$, will have the outcome $|0\rangle$, $|1\rangle$ with respective probabilities $|a|^2$ and $|b|^2$. It is evident that we can make the qubit behave as a classical bit; we can prepare the states $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$ which can be distinguished perfectly, since they are orthogonal. Turning things around, the possibility of superposition states makes the qubit superior to the classical bit – this point is essential to quantum computing, and we will return to this repeatedly in the following.

Generalizing to an N qubit system, a state can be represented as a state vector in a 2^N dimensional Hilbert space. The standard basis of this 2^N dimensional Hilbert space is the 2^N strings chosen from the set:

$$\underbrace{\{|0\rangle_A, |1\rangle_A\} \otimes \{|0\rangle_B, |1\rangle_B\} \otimes \ldots}_{N} \equiv \{|0\rangle, |1\rangle\}^{\otimes N} \tag{2.2}$$

We can expand any N qubit state in this basis as:

$$|\psi_N\rangle = \sum_{x \in \{|0\rangle, |1\rangle\}^{\otimes N}} a_x |x\rangle, \qquad \sum_x |a_x|^2 = 1 \tag{2.3}$$

So if we measure $|\psi_N\rangle$ in the standard basis we will obtain the outcome $|\psi_N\rangle = |x\rangle$ with the probability $|a_x|^2$. In principle it is of course possible to measure the N qubits in any conceivable basis of this 2^N dimensional Hilbert space, the standard basis is simply the most natural basis to choose, when measuring two state systems.

2.2 Unitary Transformations of Qubits seen as Rotations of Spin-$\frac{1}{2}$ Systems

When thinking of a qubit, most physicists tend to think about a spin-$\frac{1}{2}$ object, identifying $|0\rangle \equiv \binom{1}{0}$ with $|\uparrow_z\rangle$ and $|1\rangle \equiv \binom{0}{1}$ with $|\downarrow_z\rangle$, thus identifying the qubit with the spinor $\binom{a}{b}$. In the following we will illustrate that this is well motivated; we assume that the reader is familiar with representations of rotations, and we will only supply a brief recapitulation of the most important results, as explained by [31, 35].

The generator of rotations in spin-$\frac{1}{2}$ systems is: $\mathbf{J} = \frac{\hbar}{2}\vec{\boldsymbol{\sigma}}$, consisting of the Pauli matrices:

$$\boldsymbol{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \boldsymbol{\sigma}_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \qquad \boldsymbol{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.4}$$

It is easily seen that the different Pauli matrices anti-commutate and $\sigma_i^2 = \mathbf{1}$. For a spin-$\frac{1}{2}$ system, the unitary rotations around the axis given by the unit vector $\hat{n}$ by the angle θ are:

$$\mathbf{U}_R = \exp\left(-\frac{i\theta}{2}\hat{n} \cdot \vec{\boldsymbol{\sigma}}\right) = \mathbf{1}\cos\frac{\theta}{2} - i\hat{n} \cdot \vec{\boldsymbol{\sigma}} \sin\frac{\theta}{2} \tag{2.5}$$

The last equation is obtained by expanding the exponential in powers of $(\frac{i\theta}{2}\hat{n} \cdot \vec{\boldsymbol{\sigma}})$ and using that $(\hat{n} \cdot \vec{\boldsymbol{\sigma}})^2 = \sum_{ij} n_i n_j \sigma_i \sigma_j = \sum_i n_i n_i \mathbf{1} = \mathbf{1}$. Thus the even terms of the expansion sum to cosine

multiplied by the identity, and the odd terms form the sine function multiplied by the one remaining $(\hat{n}\cdot\vec{\boldsymbol{\sigma}})$ that is left after the even powers square to the identity.

The last expression in equation (2.5) is the form of the most general $\mathbf{U}\in SU(2)$ – i.e. the most general unitary 2×2 matrix with determinant 1. This means that any transformation $\mathbf{U}\in SU(2)$ on a qubit can be interpreted as a rotation of a spin-$\frac{1}{2}$ system. Since any element in $U(2)$ can be expressed $\mathbf{U}'=e^{i\gamma}\mathbf{U}$, $\mathbf{U}\in SU(2)$, it is permissible to consider the qubit as a spin-$\frac{1}{2}$ object, letting unitary transformations of the qubit correspond to rotations of the spin, aside from a possible total phase $e^{i\gamma}$.

We can thus interchange $|0\rangle$, $|1\rangle$ and $|\uparrow_z\rangle$, $|\downarrow_z\rangle$ as we please, but we will generally use the notation $a|0\rangle+b|1\rangle$ to emphasize the kinship to the classical bit, emphazising that both the qubit and the bit are measures of information and independent of their particular physical manifestations. However, when we *do* use spin notation for certain problems, this has historical or practical reasons.

2.3 Entanglement

The key element in understanding decoherence and quantum error correction is entanglement[3]. In order to understand entanglement, we will have to introduce the notion of a bipartite system: A bipartite system is a system divided into two parts, A and B. The Hilbert space of the bipartite system is the direct product $\mathcal{H}_A\otimes\mathcal{H}_B$ where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the Hilbert spaces of systems A and B. A pure state $|\psi\rangle_{AB}$ in such a bipartite system is called *entangled*, if we cannot express it as a direct product of pure states of A and B, i.e. the states of systems A and B are mixed. The simplest example of entangled states is the four Bell basis states of a two-qubit system:

$$\begin{array}{lcl} |\phi^{\pm}\rangle_{AB} &=& \frac{1}{\sqrt{2}}(|00\rangle_{AB}\pm|11\rangle_{AB}) \\ |\psi^{\pm}\rangle_{AB} &=& \frac{1}{\sqrt{2}}(|01\rangle_{AB}\pm|10\rangle_{AB}) \end{array} \tag{2.6}$$

Let us take a look at the implications of entanglement. Assume that we have prepared the state $|\phi^+\rangle$, and that we have two observers Andy and Benny, each with access to only one of the qubits A and B.

The states of system A and B seen from system A and B respectively are given by the reduced density operators[4]:

$$\begin{array}{lcl} \boldsymbol{\rho}_A &=& tr_B(|\phi^+\rangle_{AB\,AB}\langle\phi^+|) \;=\; \frac{1}{2}(|0\rangle_{AA}\langle 0|+|1\rangle_{AA}\langle 1|) \\ \boldsymbol{\rho}_B &=& tr_A(|\phi^+\rangle_{AB\,AB}\langle\phi^+|) \;=\; \frac{1}{2}(|0\rangle_{BB}\langle 0|+|1\rangle_{BB}\langle 1|) \end{array} \tag{2.7}$$

This calculation shows that $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ are multiples of the identity; $|\phi^+\rangle$ has a totally random density matrix[5]. So if Andy measures qubit A in the standard basis, he will obtain the result $|0\rangle_A$ with probability $\frac{1}{2}$ and $|1\rangle_A$ with probability $\frac{1}{2}$. If Andy's result is $|0\rangle_A$, he instantaneously projects the bipartite state $|\phi^+\rangle$ onto the state $|00\rangle_{AB}$ – in effect causing qubit B to change from the mixed state (2.7) to the pure state $|0\rangle_B$[6]. In principle qubit A could be in Timbuktu and qubit B somewhere in the Hubble Deep Field; measuring qubit A instantaneously changes the state of qubit B. Thus entanglement establishes *non-local* correlations between the two entangled systems. Furthermore, these nonlocal correlations can only be created locally, that is, the two systems have to interact in order to become entangled. For a further discussion of all these subjects, see [35].

Defining entanglement for more than two subsystems is highly nontrivial, cf. [22], so in the following we simply will call a state of a system consisting of more than two subsystems entangled if it displays the same sort of non-local correlations as the ones discussed above.

2.3.1 Interpretation of the Ensemble

We will now leave the subject of entanglement for a short while and introduce a few concepts necessary to understand some subtleties regarding entangled states. We will discuss the interpretation of a state represented by a mixed state density operator.

The interpretation of a mixed state density operator as representing an ensemble of pure quantum states is in some ways misleading. If a system is known to be in a mixed state with density matrix $\boldsymbol{\rho}$,

[3] Entanglement was first named *Verschränkung*, which means foldedness, by Erwin Schrödinger.
[4] Cf. appendix A for a discussion of the concept of a reduced density matrix.
[5] To be defined in section 2.3.1
[6] From this point on, we will leave out the subscripts A, B, etc., when there is no danger of confusion.

one cannot tell which ensemble of the system that has been prepared; the same mixed state density operator can be realized by many ensemble preparations. The simplest example of this ambiguity of the ensemble interpretation, is the totally random density matrix of a spin-$\frac{1}{2}$ object (for this example, we will use $|\updownarrow\rangle$ notation):

$$\boldsymbol{\rho} = \frac{1}{2}\mathbf{1}. \tag{2.8}$$

This mixed state can be prepared as an ensemble of pure states in infinitely many ways. One could for example prepare the ensemble where $|\uparrow_z\rangle$ and $|\downarrow_z\rangle$ each occurs with probability $\frac{1}{2}$, that is, the ensemble:

$$\boldsymbol{\rho} = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle\langle\downarrow_z|. \tag{2.9}$$

But using the identities $|\uparrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle + |\downarrow_z\rangle)$ and $|\downarrow_x\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\rangle - |\downarrow_z\rangle)$, we easily see that $\boldsymbol{\rho}$ also can be expressed as:

$$\boldsymbol{\rho} = \frac{1}{2}|\uparrow_x\rangle\langle\uparrow_x| + \frac{1}{2}|\downarrow_x\rangle\langle\downarrow_x|, \tag{2.10}$$

so if we had prepared the ensemble in which $|\uparrow_x\rangle$ and $|\downarrow_x\rangle$ each occurred with probability $\frac{1}{2}$ instead, we would have obtained the same density matrix. This means that the two different ensemble preparations lead to the same density operator, and therefore the expectation value of any observable is the same for the two ensemble preparations, so one cannot tell which ensemble has been prepared by observing of the system.

Indeed it turns out for any axis $\hat{n}$ that if we prepared the ensemble in which spin up and down along the $\hat{n}$-axis, $|\uparrow_{\hat{n}}\rangle$ and $|\downarrow_{\hat{n}}\rangle$, each occur with probability $\frac{1}{2}$, we would generate the density matrix (2.8). This is why the density matrix (2.8) is denoted *the totally random density matrix*; if the system is prepared in this state, measurement of the spin along any axis, will have a completely random outcome, i.e. the outcomes *spin up* and *spin down* both will have the probability $\frac{1}{2}$. This ambiguity of the ensemble interpretation, has the consequence that if one measures the observable $\boldsymbol{\sigma}_z$ on a qubit in the mixed state (2.8), and obtains the outcome $|\uparrow_z\rangle$, one cannot, unlike what is the case in classical statistics, conclude that the system also was in the state $|\uparrow_z\rangle$ before the measurement (the preparer could have prepared the ensemble $|\updownarrow_x\rangle$ instead of $|\updownarrow_z\rangle$). Therefore, a mixed state $\boldsymbol{\rho}$, is often referred to as an *improper mixture* and a mixed state representing a classical statistical ensemble is often referred to as a *proper mixture*.

2.3.2 Non-local correlations

Let us pause for a moment and contemplate the Andy-Benny example again; it is imperative to realize that it is *not* just our knowledge of the state of qubit B that increases when we measure $\boldsymbol{\sigma}_z^{(A)}$; the state of qubit B actually *changes*. Before the measurement, qubit B does not have a state of its own – or as Zurek says it, *the alternatives are undefined*, [46], cf. the previous section. After the measurement, the state of qubit B has changed to a pure state. The measurement of qubit A forces the state of qubit B to change.

These nonlocal correlations between separated quantum systems are fundamentally different from classical correlations. In order to understand this, we can think of a classical experiment in which two systems separated in space are correlated. Imagine that we have two footballs, one is red and the other one is blue, and that we place the footballs in boxes without seeing which ball we put in which box. We could send one box to Canada and the other one to the Dominican Republic. If an observer, Denny, opens the Dominican Republic-box and see that his football is blue, he instantaneously knows that Candy's ball in Canada is red. He has not changed the state (color) of the Canada-ball, only his knowledge of the color of the ball, has increased. But in quantum entanglement things are different: If Andy and Benny share two qubits A and B (in this example we will again use the $|\updownarrow\rangle$ notation) in the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow_z\uparrow_z\rangle + |\downarrow_z\downarrow_z\rangle)$ then, as explained before; if Andy measures the spin of qubit A in the z-direction, i.e. if he measures the observable $\boldsymbol{\sigma}_z^{(A)}$, and obtains the outcome $|\uparrow_z\rangle_A$ he instantaneously prepares qubit B in the state $|\uparrow_z\rangle_B$. But since the state $|\phi^+\rangle$ also can be expressed

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow_x\uparrow_x\rangle + |\downarrow_x\downarrow_x\rangle)$, by measuring $\boldsymbol{\sigma}_x^{(A)}$, Andy could thus prepare qubit B in one of the states $|\uparrow_x\rangle$ or $|\downarrow_x\rangle$. We see that the essential difference between the Andy-Benny *gedanken* experiment and the Candy-Denny experiment is that the color of the Canada-ball is determined before the Dominican Republic-measurement (it is unknown but the alternatives are defined), but in the Andy-Benny example the ensemble interpretation, i.e. the possible states of qubit B after the measurement, depends on which measurement Andy performs on qubit A.

2.4 Quantum Gates and Circuits

The material in this section is based primarily on an article by David DiVincenzo [11] and [35].

2.4.1 One Qubit Gates

In quantum computing it is customary to refer to unitary operations on qubits as *quantum gates*. Quantum gates are not as simple as classical gates as they are able to act not only on 0's and 1's but also on superpositions of the two. Before we can get started we need to introduce some notation. Qubits are represented by horizontal lines and operations on the qubits (gates) will be introduced when needed. For instance, figure 1 is the diagram representing the NOT operation, $\bigoplus$. The NOT operation

Figure 1: The NOT gate.

takes $|a\rangle \to \neg|a\rangle$, flipping the basis states, $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$. Acting on a arbitrary superposition it takes $a|0\rangle + b|1\rangle$ to $a|1\rangle + b|0\rangle$ thus the matrix representation of NOT is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \boldsymbol{\sigma}_x$. Another important unitary transformation is the *Hadamard gate*, $\boxed{\text{H}}$, that is represented by the matrix:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\boldsymbol{\sigma}_x + \boldsymbol{\sigma}_z) \tag{2.11}$$

To utilize the results of section 2.2, we can think of the Hadamard gate as a $\theta = \pi$ rotation around the axis given by $\hat{n} = \frac{1}{\sqrt{2}}(\hat{n}_x + \hat{n}_z)$, up to the total phase. So acting on the basis states, the Hadamard gate has the following effect:

$$\begin{array}{lcccl} \mathbf{H} : |0\rangle & \to & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \equiv & |+\rangle \\ \mathbf{H} : |1\rangle & \to & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \equiv & |-\rangle \end{array} \quad \text{or} \quad \mathbf{H} : |a\rangle = \frac{1}{\sqrt{2}} \sum_{b=0}^{1} (-1)^{ab} |b\rangle \tag{2.12}$$

Later on, we will also need to use the more general Hadamard gate $\mathbf{H}^{(n)} = \overbrace{\mathbf{H} \otimes \ldots \otimes \mathbf{H}}^{n}$ which acts bitwise on n qubits. Utilizing (2.12) we can find an expression for the effect of $\mathbf{H}^{(n)}$ on an n qubit standard basis state, that is, a n qubit bit string, $|u\rangle$:

$$\mathbf{H}^{(n)} : |u\rangle \to \bigotimes_{i=1}^{n} \left(\frac{1}{\sqrt{2}} \sum_{v_i \in \{0,1\}} (-1)^{u_i v_i} |v_i\rangle \right) = \frac{1}{2^{\frac{n}{2}}} \sum_{v \in \{0,1\}^{\otimes n}} (-1)^{u \cdot v} |v\rangle \tag{2.13}$$

where u, v represent n-bit strings and $u \cdot v$ is the modulo 2 scalar product. The Hadamard gate is an important example, but in principle, we can of course construct a gate that induces any rotation $\mathbf{U} = \mathbf{R}(\hat{n}, \theta)$, or equivalently any superposition, of the qubit, cf. the last expression in (2.5).

2.4.2 Two Qubit Gates

The NOT gate can be extended to a conditional two qubit gate, the controlled not (CNOT) or XOR gate. Figure 2 shows the diagrammic representation of the CNOT gate. This gate operates on the the basis state as $(a, b) \to (a, a \oplus b)$, where $a, b \in 0, 1$ and $\oplus$ signifies addition modulo 2, i.e. it flips the

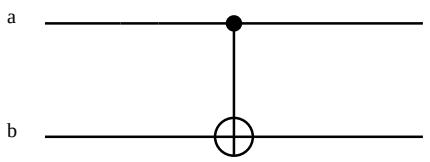

Figure 2: The CNOT gate.

second qubit, if the first qubit is in the state $|1\rangle$ and does nothing if the first state is $|0\rangle$. The matrix representation of the CNOT is:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \text{CNOT}^2 = \mathbf{1} \tag{2.14}$$

Now, combining CNOT and the Hadamard, we can design a quantum circuit that entangles two qubits, it is displayed in figure 3. Equation (2.15) demonstrates how this circuit works on the state $|00\rangle$.

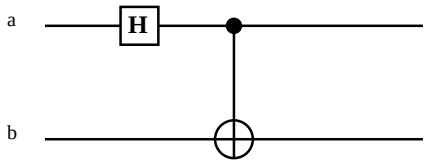

Figure 3: The entangling circuit.

$$|00\rangle \overset{\mathbf{H}}{\to} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\text{CNOT}}{\to} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle \tag{2.15}$$

The effect on the remaining elements of the standard basis is:

$$|01\rangle \to |\psi^+\rangle, \quad |10\rangle \to |\phi^-\rangle, \quad |11\rangle \to |\psi^-\rangle. \tag{2.16}$$

So the circuit in figure 3 takes the standard basis to the Bell basis. The only connection between a and b in the diagram is the CNOT, so the CNOT is the operation that establishes entanglement: It *is* the non-local element of the discussion in section 2.3. The CNOT can also remove entanglement, because seeing that CNOT and **H** are their own inverses, it is clear that we can run the circuit backwards and *un*entangle the two qubits; rotating the Bell states back to the standard basis.

2.4.3 Universality

When we say that a set of classical gates[7] is *universal*, we mean that using only compositions of these gates, we can compute any function $f\{0,1\}^N \to \{0,1\}^N$, reversibly. For a quantum computer universality of a set of gates indicates that we can get as close as we wish to any unitary operation $\mathbf{U} \in U(2^N)$, acting on arbitrarily many (N) qubits, by means of compositions of the members of the set.

The most important result concerning quantum gates and universality was published by Barenco *et al.* (including Shor and DiVincenzo) [12]. Their article states that a set of gates which consists of all one qubit quantum gates ($U(2)$) and the two qubit controlled not gate (CNOT) is a universal set. This result is significant because of its practical applicability – it means that if we wish to build a universal quantum computer, it is sufficient that we can perform the CNOT and all unitary operations on a single qubit, cf. §1.2.1.

[7] Classical gates operate on classical bits.

3 Decoherence

We have completed the introductory sections and are now ready to move up one level and get started with the the subject this report is basically about: quantum error correction. The most serious threat to successful quantum computing is decoherence, and initially quantum error correction was designed to battle exactly this sort of disturbances. Therefore, we will start out by explaining just what decoherence is and how it manifests itself in physical systems (including a quantum computer memory). We will then look at how decoherence can be described mathematically and finally make room for a few remarks of a more "philosophical" nature, discussing whether decoherence *may* be the reason for the classical appearance of everyday objects.

The evolution of a closed quantum system is unitary and governed by the time dependent Schrödinger equation:

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = \mathsf{H}|\psi\rangle \tag{3.1}$$

Unitary evolution is deterministic and accordingly it takes pure states to pure states, or, in the words of W. Zurek: *Unitary evolution condemns every closed system to "purity"* [46]. Unfortunately the notion of a closed system is only an idealization, and when dealing with an open system that interacts with an *environment*, complications arise.

If the bipartite system consisting of subsystems A and B in the familiar Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, is subjected to unitary evolution, the evolution of subsystem A (and B) alone is not necessarily unitary. During their evolution, systems A and B may interact and become entangled; as a consequence the state of system A (and B) alone, can evolve from an initially pure state into a mixture. As announced in the introduction decoherence is the key process by which errors in quantum computer memory arise.

3.1 Superoperators

As a first approach to decoherence, we will take a look at a mathematical formalism for describing decoherence, the *superoperators*. Superoperators are the "correct" formalism for describing the dynamics of an open system, and they give us a clear picture of how decoherence works. Our discussion will follow Preskill [35].

Let us again consider the bipartite system comprised of the subsystem A and B, and let us assume that the state of the two systems is of the form:

$$\boldsymbol{\rho}_A \otimes |\ell\rangle_{BB}\langle\ell|, \tag{3.2}$$

where the state of system A is described by $\boldsymbol{\rho}_A$ and system B is in an initially pure state, $|\ell\rangle_B$. Our aim is to describe the evolution of system A alone, as the bipartite state (3.2) undergoes unitary evolution. The time evolution of the bipartite state is determined by the unitary operator $\mathbf{U}_{AB}$ whose effect on (3.2) is: $\mathbf{U}_{AB}(\boldsymbol{\rho}_A \otimes |\ell\rangle_{BB}\langle\ell|)\mathbf{U}_{AB}^\dagger$. We trace over B to find the final reduced density matrix of system A:

$$\boldsymbol{\rho'}_A = tr_B(\mathbf{U}_{AB}(\boldsymbol{\rho}_A \otimes |\ell\rangle_{BB}\langle\ell|)\mathbf{U}_{AB}^\dagger) = \sum_m {}_B\langle m|\mathbf{U}_{AB}|\ell\rangle_B \boldsymbol{\rho}_A\, {}_B\langle\ell|\mathbf{U}_{AB}^\dagger|m\rangle_B, \tag{3.3}$$

where $\{|m\rangle_B\}$ is an orthonormal basis for $\mathcal{H}_B$. Since $\boldsymbol{\rho}_A$ is not part of the inner product in $\mathcal{H}_B$, it can be placed outside the $\langle$bra|c|kets$\rangle$. The partial inner product ${}_B\langle m|\mathbf{U}_{AB}|\ell\rangle_B$ constitutes an operator acting on $\mathcal{H}_A$. We easily see that (3.3) can be written:

$$\$(\boldsymbol{\rho}_A) \equiv \boldsymbol{\rho}'_A = \sum_m K_m \boldsymbol{\rho}_A K_m^\dagger, \quad K_m \equiv \langle m|\mathbf{U}_{AB}|\ell\rangle_B. \tag{3.4}$$

Since $\mathbf{U}_{AB}$ is unitary, the K_m's satisfy the following condition.

$$\begin{aligned} \sum_m K_m^\dagger K_m &= \sum_m {}_B\langle\ell|\mathbf{U}_{AB}^\dagger|m\rangle_{BB}\langle m|\mathbf{U}_{AB}|\ell\rangle_B \\ &= {}_B\langle\ell|\mathbf{U}_{AB}^\dagger\mathbf{U}_{AB}|\ell\rangle_B = {}_B\langle\ell|\mathbf{1}_{AB}|\ell\rangle_B = \mathbf{1}_A. \end{aligned} \tag{3.5}$$

Equations (3.4) and the normalization condition (3.5) imply that $\boldsymbol{\rho}'_A$ satisfies the three density matrix conditions if $\boldsymbol{\rho}_A$ does, cf. appendix A:

1. Hermiticity: $\boldsymbol{\rho}_A'^{\dagger} = \left(\sum_m K_m \boldsymbol{\rho}_A K_m^{\dagger}\right)^{\dagger} = \sum_m K_m \boldsymbol{\rho}_A^{\dagger} K_m^{\dagger} = \sum_m K_m \boldsymbol{\rho}_A K_m^{\dagger} = \boldsymbol{\rho}_A'$
2. Unit Trace: $\mathrm{tr}\boldsymbol{\rho}_A' = \mathrm{tr}(\sum_m K_m^{\dagger}\boldsymbol{\rho}_A K_m) = \sum_m \mathrm{tr}(K_m^{\dagger}\boldsymbol{\rho}_A K_m) = \sum_m \mathrm{tr}(\boldsymbol{\rho}_A K_m^{\dagger} K_m) = \mathrm{tr}\boldsymbol{\rho}_{\mathrm{A}} = 1$
3. Non-negativity: ${}_A\langle\psi|\boldsymbol{\rho}_A'|\psi\rangle_A = {}_A\langle\psi|\left(\sum_m K_m^{\dagger}\boldsymbol{\rho}_A K_m\right)|\psi\rangle_A = \sum_m ({}_A\langle\psi|K_m)\boldsymbol{\rho}_A(K_m^{\dagger}|\psi\rangle_A) \geq 0$

Equation (3.4) defines a linear mapping which takes linear operators to linear operators. If the map also satisfies equation (3.5), it is referred to as a *superoperator*, \$; the decomposition into K_m's is called *the operator-sum representation* of the superoperator, and the K_m's are called *Krauss operators*. Since $\boldsymbol{\rho}_A'$ fulfills the conditions (1) – (3), a superoperator takes density operators to density operators.

To summarize the above: We have shown that when a bipartite system, initially in the state $\boldsymbol{\rho}_A \otimes |\ell\rangle_{B\,B}\langle\ell|$, undergoes unitary evolution, the state of system A alone is given by the superoperator (3.4). Now, we can also turn things around: given an operator-sum representation of a superoperator, we can construct a unitary representation by choosing the Hilbert space of system B to be of at least the dimension of the number of terms in the operator-sum representation. Let us denote an orthonormal system in $\mathcal{H}_B$, $\{|m\rangle_B\}$, and let $|\varphi\rangle_A$ be an arbitrary state in $\mathcal{H}_A$, and let us define the action of $\mathbf{U}_{AB}$ by:

$$\mathbf{U}_{AB}(|\varphi\rangle_A \otimes |\ell\rangle_B) = \sum_m K_m|\varphi\rangle_A \otimes |m\rangle_B. \tag{3.6}$$

This action preserves the inner product:

$$\begin{aligned}({}_A\langle\varphi_2| \otimes {}_B\langle\ell|\mathbf{U}_{AB}^{\dagger})(\mathbf{U}_{AB}|\varphi_1\rangle_A \otimes |\ell\rangle_B) &= \left(\sum_n {}_A\langle\varphi_2|K_n^{\dagger} \otimes {}_B\langle n|\right)\left(\sum_m K_m|\varphi_1\rangle_A \otimes |m\rangle_B\right) \\ &= {}_A\langle\varphi_2|\sum_m K_n^{\dagger}K_m|\varphi_1\rangle_A = {}_A\langle\varphi_2|\varphi_1\rangle_A \quad \Big(= ({}_A\langle\varphi_2| \otimes {}_B\langle\ell|)\,(|\psi_1\rangle_A \otimes |\ell\rangle_B)\Big)\end{aligned} \tag{3.7}$$

so we can conclude that $\mathbf{U}_{AB}$ can be extended to an unitary operator acting on the total $\mathcal{H}_A \otimes \mathcal{H}_B$. We perform the partial trace over system B to find the reduced density matrix of system A.

$$\mathrm{tr}\left(\mathbf{U}_{AB}(|\varphi\rangle_A \otimes |\ell\rangle_B)(\langle\varphi|_A \otimes \langle\ell|_B)\mathbf{U}_{AB}^{\dagger}\right) = \sum_m K_m(|\varphi\rangle_{A\,A}\langle\varphi|)K_m^{\dagger}. \tag{3.8}$$

Thus we have shown that we recover the operator-sum representation acting on a pure state; since any density operator $\boldsymbol{\rho}_A$ can be expressed as an ensemble of pure states, we recover the operator-sum representation acting on an arbitrary $\boldsymbol{\rho}_A$.

If we regard system A as our local quantum system and system B as an environment, we can understand why the superoperator formalism is ideal for describing decoherence. When a quantum system decoheres it becomes entangled with the environment, and since we generally cannot keep track of all of the environment's degrees of freedom, we need a formalism that keeps track of system A while disregarding system B. The mathematical tool is the superoperator.

More specifically we can see unitary evolution of system A as the special case in which the operator-sum representation contains only one term, $\boldsymbol{\rho}_A' = K_1\boldsymbol{\rho}_A K_1^{\dagger}$ ($K_1^{\dagger} = K_1^{-1}$). If there is more than one term in the representation, there are initially pure states of system A that become entangled with system B during the unitary evolution $\mathbf{U}_{AB}$. For example, suppose there are two terms in the operator-sum representation: $\boldsymbol{\rho}_A' = K_1\boldsymbol{\rho}_A K_1^{\dagger} + K_2\boldsymbol{\rho}_A K_2^{\dagger}$, and that K_1 and K_2 are linearly independent. Then there exists a vector $|\varphi\rangle_A$, satisfying that $K_1|\varphi\rangle_A = |\varphi_1\rangle_A$ and $K_2|\varphi\rangle_A = |\varphi_2\rangle_A$ are linearly independent, and therefore the state of the bipartite system evolves to a state $|\varphi_1\rangle_A|1\rangle_B + |\varphi_2\rangle_A|2\rangle_B$, that can not be written as a product of pure states of the subsystems A and B.

3.1.1 The Kraus Representation Theorem

Consider a linear mapping \$: $\boldsymbol{\rho} \to \boldsymbol{\rho}'$, taking density operators to density operators satisfying the conditions[8].

[8] A superoperator \$ is called completely positive if $\$_A \otimes \mathbf{1}_B$ is positive, i.e. preserves non-negativity of density operators (cf. appendix A) for any extension of the systems Hilbert space $\mathcal{H}_A$ to a tensor product $\mathcal{H} \otimes \mathcal{H}_B$.

1. $ preserves Hermiticity, that means $\boldsymbol{\rho}'$ is hermitian if $\boldsymbol{\rho}$ is.
2. $ preserves trace: $\mathrm{tr}\boldsymbol{\rho}' = 1$ if $\mathrm{tr}\boldsymbol{\rho} = 1$.
3. $ is completely positive.

Kraus' representation theorem says that any linear mapping $\$: \boldsymbol{\rho} \to \boldsymbol{\rho}'$ satisfying the conditions (1)-(3) has an operator sum representation, that is, any $ satisfying these conditions can be realized by unitary evolution of a suitable bipartite system. We will not prove this result here, we have just mentioned the result to complete the superoperator theory. A proof can be found in [28] or in [35].

3.1.2 A Quantum Channel

To pay homage to classical information theory, it is customary to refer to superoperators on qubits as *quantum channels*. Since superoperators may seem rather abstract at first sight, we will present a simple example of their use to investigate their properties.

The following quantum channel which we have adapted from Preskill [35] is perfect for illustrating the basic mechanisms of decoherence: As we will come to realize in the following, this simple channel brings out the characteristics of decoherence in an UN-complicated and easily understandable way.

The easiest way to explain the properties of this *phase dampening channel* channel is by explaining how it affects a qubit in a pure state, system A, which is entangled with another system. System B may be interpreted as an environment[9]. The unitary representation of the channel is:

$$\mathbf{U}_{AB}: \begin{array}{lcl} |0\rangle_A|e_0\rangle_B & \to & \sqrt{p-1}|0\rangle_A|e_0\rangle_B + \sqrt{p}|0\rangle_A|e_1\rangle_B \\ |1\rangle_A|e_0\rangle_B & \to & \sqrt{p-1}|1\rangle_A|e_0\rangle_B + \sqrt{p}|1\rangle_A|e_2\rangle_B \end{array} . \tag{3.9}$$

If the system A is in the state $|0\rangle_A$, system B is scattered into the state $|e_1\rangle_B$ with probability p, and into $|e_2\rangle_B$ if A is in $|1\rangle_A$.

We find the Kraus operators by evaluating the partial trace over B, to find the operators $K_m = {}_B\langle e_m|\mathbf{U}_{AB}|e_0\rangle_B$ in the $\{|e_i\rangle_B\}$ basis:

$$K_0 = \sqrt{p-1}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad K_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad K_2 = \sqrt{p}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.10}$$

The K_i's clearly satisfy the condition (3.5). Now, we are in a position to work out how a general density matrix $\boldsymbol{\rho}$ evolves, we write down the superoperator on $\boldsymbol{\rho} = \left(\begin{smallmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{smallmatrix}\right)$, cf. equation (3.4).

$$\begin{gathered} \$(\boldsymbol{\rho}) = K_0\boldsymbol{\rho}K_0 + K_1\boldsymbol{\rho}K_1 + K_2\boldsymbol{\rho}K_2 = \\ (1-p)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + p\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + p\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \\ = \begin{pmatrix} \rho_{11} & (1-p)\rho_{12} \\ (1-p)\rho_{21} & \rho_{22} \end{pmatrix}, \end{gathered} \tag{3.11}$$

or for n runs through the channel:

$$\$^n(\boldsymbol{\rho}) = \begin{pmatrix} \rho_{11} & (1-p)^n\rho_{12} \\ (1-p)^n\rho_{21} & \rho_{22} \end{pmatrix} \tag{3.12}$$

This is probably a good time to discuss some of the physics behind all of this. We can imagine that one run through this channel describes a small time step, Δt, so the time evolution over $t = n\Delta t$ is governed by $\$^n$. Furthermore we can assume, that the probability of a change in the environment per unit time is ξ, so that $p = \xi\Delta t$ when Δt elapses. Equation (3.12) and the above considerations show that the numerical size of the off-diagonal terms decreases as $(1-p)^n = (1-\xi\Delta t)^{\frac{t}{\Delta t}} \to e^{-\xi t}$ as $\Delta t \to 0$. Decoherence happens *fast*.

Another interesting aspect of this channel is that it picks out what is called a *preferred basis* for decoherence. After a time $t \ll \xi^{-1}$ a general state $a|0\rangle_A + b|1\rangle_A$ evolves into an incoherent mixture $\boldsymbol{\rho}' = |a|^2|0\rangle_{AA}\langle 0| + |b|^2|1\rangle_{AA}\langle 1|$. The preferred basis is: $\{|0\rangle_A, |1\rangle_A\}$. If we imagine that the qubit $a|0\rangle_A + b|1\rangle_A$ represents a particle in a superposition of position eigenstates, and that the environment

[9] We will use the notation $|e_i\rangle_B$, to emphasize that system B can be regarded as an environment.

is photons scattering of the particle, the preferred basis for decoherence would be position eigenstates. Physically this is because the interactions between the photons and the particle are localized in space. Particles *in distinguishable positions tend to scatter the photons into mutually orthogonal states*, as Preskill [35] says. Some physicists believe that this phenomenon can explain how the classical world emerges from quantum theory. The concepts described in this example are very interesting, and we will discuss these notions further in the following cf. section 3.2.2.

3.2 Decoherence and the Process of Measurement

Quantum theory is the best physical theory available to mankind. Unfortunately, there is an huge discrepancy between the world that human beings experience every day and the nebulous world of quantum mechanics. The border between classical and quantum is not an easily definable one – if we need a distinction, cf. [46], and the question of how this distinction arises is part of what will be discussed in this section. It is important to emphasize that the identification of macroscopic with classical is *not* always valid; there are several examples of macroscopic objects that need a quantum mechanical description, for instance the *Weber bar* or super-conductivity [46].

It has been attempted to explain the appearance of a classical world in quantum theory via decoherence, i.e. that the classical appearance is caused by interactions with an environment with too many degrees of freedom to keep track of. Decoherence is also the main reason that errors in quantum computer memory occur, so in the following sections, we will try to explain what actually takes place. We will rely on articles by one of the pioneers of this field, W. Zurek [45, 46] and on a text by Joos [26].

3.2.1 Von Neumann Measurement

The idea of the Von Neumann process of measurement [33] is to correlate the value of the observable we want to measure with the pointer of an apparatus which we take for granted that we are able to measure. The formalism is simpler if we proceed in the *interaction picture* or Dirac picture, cf. [31], so we will do just that.

First we will show how we can couple system A which is our local system, with another system, B, which may be interpreted as an apparatus. We choose an interaction Hamiltonian to be of the form:

$$\mathsf{H}_{int} = \sum_n |n\rangle_{AA}\langle n| \otimes \mathbf{O}_n^{(B)}, \tag{3.13}$$

where $\mathbf{O}_n^{(B)}$ is an arbitrary but n-dependent observable acting on $\mathcal{H}_B$ only, and the $|n\rangle_A$'s are the eigenstates of the observable of system A that is being measured by the interaction. The time development of the state $|n\rangle_A|\varphi_0\rangle_B$, where $|\varphi_0\rangle_B$ is the initial state of system B, is given by:

$$|n\rangle_A|\varphi_0\rangle_B \xrightarrow{t} \mathrm{e}^{(-i\mathsf{H}_{int}t)}|n\rangle_A|\varphi_0\rangle_B = |n\rangle_A \exp\left(-i\mathbf{O}_n^{(B)}t\right)|\varphi_0\rangle_B \equiv |n\rangle_A|\varphi_n\rangle_B \tag{3.14}$$

The time evolution of the bipartite state, with system A in a general arbitrary state, $|\psi\rangle_A = \sum_n c_n|n\rangle_A$, and the apparatus in the state $|\varphi_0\rangle_B$, is:

$$|\psi\rangle_A|\varphi_0\rangle_B = \left(\sum_n c_n|n\rangle_A\right)|\varphi_0\rangle_B \xrightarrow{t} \sum_n c_n|n\rangle_A|\varphi_n\rangle_B. \tag{3.15}$$

By way of entanglement, the eigenstates of the measured observable, $|n\rangle_A$ have become correlated with the $|\varphi_n\rangle_B$'s. These are called *pointer states*. If these pointer states discriminate the $|n\rangle_A$ states, i.e. $\langle\varphi_m|\varphi_n\rangle_B = \delta_{n,m}$ – the purpose of an apparatus is precisely to distinguish between these states – we can interpret (3.15) as a superposition of measurement outcomes; by measuring system B in the $|\varphi_n\rangle_B$ basis and for example obtaining the outcome $|\varphi_\ell\rangle_B$, we have prepared system A in the state $|\ell\rangle_A$.

After the time evolution, the reduced density matrix of system A has changed according to:

$$\boldsymbol{\rho}_A = \sum_{m,n} c_m^* c_n |m\rangle_{AA}\langle n| \xrightarrow{t} \sum_{m,n} c_m^* c_n {}_B\langle\varphi_m|\varphi_n\rangle_B |m\rangle_{AA}\langle n| = \sum_n |c_n|^2 |n\rangle_{AA}\langle n|, \tag{3.16}$$

the last equality follows if the the states of system B are orthonormal as discussed above. Hence we see that the state of system A has changed from a pure state to an improper mixture, *diagonal* in the $\{|n\rangle_A\}$-basis. If we think of system B as an environment that we cannot keep track of, the density matrix of system A alone is precisely what we are looking for: The quantum mechanical correlations (the phase relations characterizing the superposition) are *delocalized.*

We use the word *delocalized*, because the phase relations are not destroyed; they still exist in the state of system $A + B$. If the observer also has access to system B, he could reveal the existence of phase relations and thus expose the quantum nature of the joint system with respect to the observable characterized by the quantum number n. But the correlations are inaccessible to an observer in system A, if the above process is assumed to be irreversible: *The system now* appears *classical with respect to the property given by the quantum number n ... Then the classical assumption that the system* is *in one of the states* $|n\rangle_A$ *cannot be proven wrong by observations at this system (although no collapse was assumed so far) ...* [26]. The mixed state (3.16) *behaves* as a classical ensemble relative to system A.

Historically, though, Von Neumann never made any of the considerations beyond equation (3.15), the name *Von Neumann measurement* stem from the fact that Von Neumann was the first to consider this type of measurement [33].

3.2.2 Introducing the Environment

Tracing over the apparatus states, we obtain a diagonal density matrix for system A, but this is not exactly what we are looking for. We need the apparatus to measure the state of A, but tracing over system B makes it impossible for us to have any knowledge of that system. To achieve the description we want we have to extend the picture and realize that of course the apparatus itself is coupled to an environment E that has degrees of freedom which we cannot keep track of. The Hilbert space of the environment is $\mathcal{H}_E$, so the total system is now: $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. Time evolution will now correlate the state of the environment with the apparatus:

$$\left(\sum_n |n\rangle_A |\varphi_n\rangle_B\right) |e\rangle_E \xrightarrow{t} \sum_n |n\rangle_A |\varphi_n\rangle_B |e_n\rangle_E. \tag{3.17}$$

Now if

$${}_E\langle e_m | e_n\rangle_E \approx \delta_{m,n}, \tag{3.18}$$

we get:

$$\boldsymbol{\rho}_{AB} = \sum_n |c_n|^2 |n\rangle_{AA}\langle n| \otimes |\varphi_n\rangle_{BB}\langle \varphi_n|, \tag{3.19}$$

Again, the quantum correlations are suppressed and without any collapse we are left with a classically looking improper mixture for the combined AB-subsystem. The interaction coupling is again assumed to have the form (3.13), in a sense defining the pointer states $|\varphi_n\rangle_B$. It is important to realize that *this does not solve the measurement problem*; (3.19) is an *im*proper mixture, and a subsequent measurement of an observable would will still cause the enigmatic collapse of (3.17).

A serious problem is the rôle of the pointer states. Zurek has proposed an interpretation of (3.19) as representing a probability distribution of the pointer states, that is, representing a classical statistical ensemble. Zurek's interpretation is condensed in the following quotation [46]:

> A preferred basis of the detector, sometimes called a "pointer basis", has been singled out. An effective superselection rule has emerged – decoherence prevents superpositions of the preferred basis states from persisting. Moreover, we have obtained all this – or so it appears – without having to appeal to anything beyond the ordinary, unitary Schrödinger evolution.
>
> The preferred basis of a detector – or for that matter, any open quantum system – is selected by the dynamics ...

This interpretation is problematic; Zurek appears to disregard the fact that the state of $A + B$ is an *improper* mixture, not a classical statistical ensemble, and we know from section 2.3.1 that a mixed

state density matrix can represent many pure states ensembles, that is, the "preferred basis" is not the only basis in which the density matrix of $A+B$ is diagonal. Thus it seems as if Zurek is putting things a bit too strongly, when he says: *A preferred basis ... has been singled out.* Klaus Mølmer and Yvan Castin hit the nail right on the head with the following critique, aimed especially at Zurek [32]:

> Let us finally, in this section, comment on the so-called decoherence obtained when the off-diagonal elements of the density matrix of a system tend to zero. This evolution has been interpreted as a sign of the system choosing randomly between different states ... there is nothing unique about the basis in which a system density matrix is diagonal: one *can* interpret the density matrix as a statistical mixture of such basis states, but one can, just as well, construct statistical mixtures of completely different state vectors ...

As far as we can see Mølmer, Castin and several others, e.g. [20, 24] are right when critizising Zurek: The theory of quantum mechanics does not contain any explanation of why one basis should be preferred to another basis. According to quantum theory all the bases which diagonalize the density matrix have equal claim of being a preferred basis.

However, it is an interesting fact that the density matrix is diagonal in the pointer basis if the interaction between the apparatus and the environment has the form (3.17) and (3.18) holds. A good example of this mechanism is localization: Macroscopic objects *are* localized, that is, their density matrices are diagonal in a basis of position eigenstates. To reach this result, an extra premise from *outside quantum theory* has to be drawn into the discussion, *viz* the fact that the macroscopic objects scatter the environment into mutually orthogonal states, cf. the discussion of the quantum channel in section 3.1.2, and if it really is true that the environment states *are* orthogonal, objects are – in a sense – localized.

Discussing the assumption (3.18) in any detail is clearly beyond the scope of this report, but the subject is immensely interesting, and the reader is referred to an article by Joos [26] for an in depth discussion of this assumption. In studying this article, it has become clear to us that, the focal point is that the ***locality of interactions*** in the physical world determine that the density matrix of macroscopic objects becomes diagonal in a basis of *position eigenstates* – no matter how spread out the wave function is, the interaction with the rest of the world always takes place in a single point.

3.2.3 Perspectives

Because decoherence takes place in (almost) any quantum system, a formal open system description is available. The only part that we have dealt with here is superoperators. To complete the picture, we shall mention the parts of the theory that we have *not* treated: In an open system approach to quantum mechanics superoperators take over for unitary transformations, but in the same sense, the Schrödinger equation is (at least to a good approximation [35]) replaced by the *Master Equation* and the Hamiltonian is traded in for the *Lindbladian.*

We have now studied the mechanisms behind decoherence and discussed some of the mathematical formalism. Decoherence is why errors in quantum computes arise; the fragile superposition states of the quantum register become entangled with an environment which we cannot keep track of and hence they decohere into mixtures. Furthermore we have seen that the process of decoherence can happen extremely fast. In the introduction we mentioned that the qubit is superior to the bit, but after the discussion of decoherence, we know that the price to pay for this superiority is eternal vigilance in maintaining coherence.

4 Quantum Error Correction

In the early days of quantum computing (until 1995), it was widely believed that experimental realization of quantum computers would be impossible on account of decoherence. In the following we start out by discussing why the principles of classical error correction are not directly transferable to quantum mechanics, and why this fact is an objection against the realization of practical quantum computers.

In 1995 Shor [39] and Steane [40] proved that most of the above problems can be circumvented. We will discuss Shor's code in some detail, and then proceed to investigate a general class of codes, the CSS-codes, of which Steane's 7-qubit code is the most famous example.

4.1 Classical Error Correction and Quantum Computers

Of course errors also arise in classical computers, and *very* sophisticated methods have been developed to correct errors in classical information. – Anyone who has acquainted themselves with the mammoth "bible" of classical error correction by MacWilliams and Sloane [30] knows that this is no understatement. Adapting these methods to quantum error correction is no easy task, and why this is so will be explored in the following.

The only type of error that can occur in a classical computer is a *bit flip*, $0 \to 1$ or $1 \to 0$. In quantum computers a variety of errors can occur. To understand the nature of these errors, we will simply look at the most general way in which a qubit can decohere:

4.1.1 Decoherence of a Qubit

The general process of decoherence of a qubit in a primary system which is connected to an environment E, is described by the following unitary process on both systems:

$$\mathbf{U}: \begin{array}{lcll} |0\rangle \otimes |e_I\rangle_E & \to & |0\rangle \otimes |e_{00}\rangle_E & + \quad |1\rangle \otimes |e_{01}\rangle_E \\ |1\rangle \otimes |e_I\rangle_E & \to & |0\rangle \otimes |e_{10}\rangle_E & + \quad |1\rangle \otimes |e_{11}\rangle_E \end{array} \tag{4.1}$$

where we assume that the environment is initially in the state $|e_I\rangle_E$ and that the states of the environment after the evolution are not necessarily orthogonal or normalized. An arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ evolves as:

$$\begin{array}{ll} \mathbf{U}: & (a|0\rangle + b|1\rangle) \otimes |e_I\rangle_E \\ \to & a(|0\rangle \otimes |e_{00}\rangle_E + |1\rangle \otimes |e_{01}\rangle_E) + b(|0\rangle \otimes |e_{10}\rangle_E + |1\rangle \otimes |e_{11}\rangle_E) \\ = & (a|0\rangle + b|1\rangle) \otimes \frac{1}{2}(|e_{00}\rangle_E + |e_{11}\rangle_E) + (a|0\rangle - b|1\rangle) \otimes \frac{1}{2}(|e_{00}\rangle_E - |e_{11}\rangle_E) \\ + & (a|1\rangle + b|0\rangle) \otimes \frac{1}{2}(|e_{01}\rangle_E + |e_{10}\rangle_E) + (a|1\rangle - b|0\rangle) \otimes \frac{1}{2}(|e_{01}\rangle_E - |e_{10}\rangle_E) \\ \equiv & \mathbf{1}|\psi\rangle \otimes |e_{\mathbf{1}}\rangle_E + \boldsymbol{\sigma}_x|\psi\rangle \otimes |e_x\rangle_E + \boldsymbol{\sigma}_z|\psi\rangle \otimes |e_z\rangle_E + i\boldsymbol{\sigma}_y|\psi\rangle \otimes |e_y\rangle_E, \end{array} \tag{4.2}$$

where we have defined:

$$\begin{array}{ll} |e_{\mathbf{1}}\rangle_E = \frac{1}{2}(|e_{00}\rangle_E + |e_{11}\rangle_E), & |e_x\rangle_E = \frac{1}{2}(|e_{00}\rangle_E - |e_{11}\rangle_E), \\ |e_z\rangle_E = \frac{1}{2}(|e_{01}\rangle_E + |e_{10}\rangle_E), & |e_y\rangle_E = \frac{1}{2}(|e_{01}\rangle_E - |e_{10}\rangle_E). \end{array}$$

A way to interpret the expansion (4.2) is that after the evolution, we can "act" as if one of the four *error operators* $\mathbf{1}$, $\boldsymbol{\sigma}_x$, $i\boldsymbol{\sigma}_y$, or $\boldsymbol{\sigma}_z$ have operated on the qubit. In the following we will refer to this as *the simplified error model.* But since the environment states in the last expression in (4.2) in general are not orthogonal, this interpretation is not unproblematic; or as Preskill [35] says it: ... *this classification should not be taken too literally, because unless the states* $\{|e_1\rangle, |e_x\rangle, |e_y\rangle, |e_z\rangle\}$ *of the environment are all mutually orthogonal, there is no conceivable measurement that could perfectly distinguish among the four alternatives.*

However, in the following we will use the simplified error model, i.e. we will assume that an error on a qubit state originating from decoherence can be described by one of the four operators $\mathbf{1}$, $\boldsymbol{\sigma}_x$, $i\boldsymbol{\sigma}_y$, and $\boldsymbol{\sigma}_z$. We will discuss this error model further in section4.6

Following the simplified error model, we assume that decoherence can cause the following types of errors:

1. No error, $\mathbf{1}$: $\begin{array}{lcl} |0\rangle & \to & |0\rangle \\ |1\rangle & \to & |1\rangle \end{array}$, or acting on an arbitrary state $\mathbf{1}: a|0\rangle + b|1\rangle \to a|0\rangle + b|1\rangle$.

2. Bit flips, $\boldsymbol{\sigma}_x$: $\begin{array}{lcl} |0\rangle & \to & |1\rangle \\ |1\rangle & \to & |0\rangle \end{array}$, or acting on an arbitrary state $\boldsymbol{\sigma}_x: a|0\rangle + b|1\rangle \to a|1\rangle + b|0\rangle$.

3. Phase flips, $\boldsymbol{\sigma}_z$: $\begin{array}{lll} |0\rangle & \rightarrow & |0\rangle \\ |1\rangle & \rightarrow & -|1\rangle \end{array}$, or acting on an arbitrary state $\boldsymbol{\sigma}_z : a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$.

4. Both, $i\boldsymbol{\sigma}_y$: $\begin{array}{lll} |0\rangle & \rightarrow & |1\rangle \\ |1\rangle & \rightarrow & -|0\rangle \end{array}$, or acting on an arbitrary state $i\boldsymbol{\sigma}_y : a|0\rangle + b|1\rangle \rightarrow a|1\rangle - b|0\rangle$.

That is, decoherence can lead to two (three) kinds of errors: Bit-flips, described by $\boldsymbol{\sigma}_x$, and phase-flips, described by $\boldsymbol{\sigma}_z$ (and both bit and phase-flips, described by $i\boldsymbol{\sigma}_y = \boldsymbol{\sigma}_x\boldsymbol{\sigma}_z$). Later it will prove useful to realize that a bit-flip in the standard basis corresponds to a phase-flip in the Hadamard rotated basis, cf. section 2.4.1, and that a phase-flip in the standard basis corresponds to a bit-flip in the Hadamard rotated basis, and conversely. This is easily seen, for example consider the two following calculations:

1. $\boldsymbol{\sigma}_x : (a|0\rangle + b|1\rangle) \rightarrow a|1\rangle + b|0\rangle$

2. $\boldsymbol{\sigma}_x : [\mathbf{H}(a|0\rangle + b|1\rangle)] = \boldsymbol{\sigma}_x : (a|+\rangle + b|-\rangle) \rightarrow a|+\rangle - b|-\rangle$,

where we have used the notation $|\pm\rangle = \frac{1}{2}(|0\rangle \pm |1\rangle)$ introduced in (2.12) for the Hadamard basis. We observe that in (1) a bit-flip takes place as usual, but in the Hadamard rotated basis (2) a phase-flip has occurred.

But decoherence is not the only enemy. Even if we could completely isolate our system from the environment, we still could not expect to implement quantum gates with perfect accuracy. The errors in a quantum gate form a continuum, and these errors in the gates can accumulate over time – at some point causing failure. These errors do not stem from decoherence and therefore they are not relevant for our discussion. We will not discuss gate errors any further, but refer to [22] for an introduction.

4.1.2 Redundancy and Polling

So the number of possible errors has increased, but transferring the principles of classical error correction to quantum computers yields further problems. In order to understand these problems, it is instructive to discuss a simple classical error correcting code, the *3-bit repetition code*. In this code, one simply codes $0 \rightarrow 000$ and $1 \rightarrow 111$, i.e. we are using *redundancy*. If we furthermore assume that errors are rare, so that only one of the three bits are flipped, e.g. $000 \rightarrow 010$, we simply measure, or *poll* the three bits and infer that the minority bit is the one that suffered the flip. We correct the error by flipping the minority bit back again.

The two main principles of this approach, redundancy and polling, are not immediately applicable to quantum mechanics. In quantum mechanics polling is ruled out, since we cannot just measure a qubit. Measurement causes a collapse of the wave function, stripping the kets of the qubit, leaving a random classical bit. The problems do not end here, though, since redundancy is also out of the question – it turns out that we cannot make a perfect copy of an unknown quantum state. This fact is known as the *no-cloning theorem* and was proved by Wooters and Zurek in 1982 [44]. We will prove the no-cloning theorem in appendix B.

4.2 Shor's Nine Qubit Code

The nine qubit code is a good introduction to quantum error correction, since it brings out the principles of quantum error codes in a clear and uncomplicated manner. As the name suggests, this code was designed by Peter Shor in 1995 [39], but our discussion of this code will be based primarily on [35, 37].

4.2.1 Bit flips

We will not start out by presenting the full encoding, but consider a simple three-qubit code that is able to correct bit-flip errors. Using a three-qubit code makes the principles of the code more transparent and makes way for a more economical notation. We encode one qubit in three qubits as follows:

$$\begin{array}{lllll} |0\rangle & \rightarrow & |\bar{0}\rangle & \equiv & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ |1\rangle & \rightarrow & |\bar{1}\rangle & \equiv & \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \end{array} \tag{4.3}$$

where $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are the code qubits. That is, a general qubit state is coded into:

$$a|0\rangle + b|1\rangle \rightarrow a|\bar{0}\rangle + b|\bar{1}\rangle = \frac{1}{\sqrt{2}}[(a+b)|000\rangle + (a-b)|111\rangle)]. \tag{4.4}$$

Before we move on, we will make some assumptions; we assume that the qubits in the encoded state (4.4) decohere independently and that only one of the qubits decoheres. These assumptions are critical and we will discuss them in section 4.2.3.

With these assumptions in mind, we can assume that at most one qubit in the state (4.4) is subjected to a bit-flip. Let us start out by assuming that it is the first qubit of equation (4.4) that is flipped, or equivalently that the encoded state is acted upon by the unitary operator $\boldsymbol{\sigma}_x^{(1)} \otimes \mathbf{1}^{(2)} \otimes \mathbf{1}^{(3)}$.

$$\boldsymbol{\sigma}_x^{(1)} \otimes \mathbf{1}^{(2)} \otimes \mathbf{1}^{(3)} : \frac{1}{\sqrt{2}}[(a+b)|000\rangle + (a-b)|111\rangle) \rightarrow \frac{1}{\sqrt{2}}[(a+b)|100\rangle + (a-b)|011\rangle) \tag{4.5}$$

Assume that we measure the two commuting observables[10] $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)}$ and $\boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)}$. The encoded state (4.4) is an eigenstate of these observables with eigenvalues $+1$. The state (4.5) is also an eigenstate of these two observables, but with the eigenvalues $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)} = -1$ and $\boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)} = 1$. Similarly if any single qubit in (4.4) is subjected to a bit-flip error, we can diagnose it using these two observables. The results are summarized in figure 4. After this *syndrome measurement*, we can recover the original state

Eigenvalue of $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)}$	Eigenvalue of $\boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)}$	This qubit flipped	Recovery operation
1	1	none	$\mathbf{1}^{(1)} \otimes \mathbf{1}^{(2)} \otimes \mathbf{1}^{(3)}$
-1	1	first	$\boldsymbol{\sigma}_x^{(1)} \otimes \mathbf{1}^{(2)} \otimes \mathbf{1}^{(3)}$
-1	-1	second	$\mathbf{1}^{(1)} \otimes \boldsymbol{\sigma}_x^{(2)} \otimes \mathbf{1}^{(3)}$
1	-1	third	$\mathbf{1}^{(1)} \otimes \mathbf{1}^{(2)} \otimes \boldsymbol{\sigma}_x^{(3)}$

Figure 4: Measurement and recovery of bit-flips in the three qubit code

via the appropriate unitary recovery operation. The recovery operations are summarized in column 4 of the table.

The important idea in this scheme is that we are measuring the errors, not the actual state. When we measure $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)}$ and $\boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)}$ we gain no information about the encoded state (4.4); we only measure if a bit-flip relative to (4.4) has occurred, and in that case which qubit has flipped. This is why, we call the measurement a *syndrome* measurement.

It is important to understand that this method does not work if more than one of the three qubits flip. If we assume that both the first *and* the second qubit flip, our measurements of the two observables would have the outcomes $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)} = 1$ and $\boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)} = -1$. Following the prescribed method, we would then make the erroneous conclusion that the third qubit had flipped relative to the two others. We would try to recover the error by performing the unitary transformation $\mathbf{1}^{(1)} \otimes \mathbf{1}^{(2)} \otimes \boldsymbol{\sigma}_x^{(3)}$, and thereby worsen the error, since all the three qubits become flipped relative to the encoded state.

4.2.2 Phase flips: Shor's code

The code we have been discussing thus far, is able to correct bit-flips. But of course we want to construct a code that is able to correct both bit and phase-flips. We encode the basis states as follows:

$$\begin{array}{lcll} |0\rangle & \rightarrow & |\mathbf{0}\rangle & \equiv \quad |\bar{0}\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle, \\ |1\rangle & \rightarrow & |\mathbf{1}\rangle & \equiv \quad |\bar{1}\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle, \end{array} \tag{4.6}$$

where $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are defined in (4.4). We have now encoded our state in three clusters of three qubits, using a total of nine qubits. A general state is encoded as:

$$a|0\rangle + b|1\rangle \rightarrow a|\mathbf{0}\rangle + b|\mathbf{1}\rangle = a|\bar{0}\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle + b|\bar{1}\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle. \tag{4.7}$$

[10] In the following will use the notation $\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)} \equiv \boldsymbol{\sigma}_z^{(2)} \otimes \boldsymbol{\sigma}_z^{(3)} \otimes \mathbf{1}^{(3)}$, etc. for simplicity.

Notice that this state in general can*not* be written as a direct product of the three qubit encoded states (4.4). Thus we cannot expect the results from the previous section to be trivially transferable to Shor's nine qubit encoding. However we easily see that by augmenting the observable $\boldsymbol{\sigma}_z^{(1)} \otimes \boldsymbol{\sigma}_z^{(2)} \otimes \mathbf{1}^{(3)}$ to $\boldsymbol{\sigma}_z^{(1)} \otimes \boldsymbol{\sigma}_z^{(2)} \otimes \mathbf{1}^{(3)} \otimes \cdots \otimes \mathbf{1}^{(9)}$[11], etc. we can use the same arguments as in the previous section to correct bit-flips in the first cluster. To be able to correct bit-flips in all three clusters, we further extend the principles of the previous section, and measure the six observables:

$$\boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(2)}, \quad \boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)}; \qquad \boldsymbol{\sigma}_z^{(4)}\boldsymbol{\sigma}_z^{(5)}, \quad \boldsymbol{\sigma}_z^{(5)}\boldsymbol{\sigma}_z^{(6)}; \qquad \boldsymbol{\sigma}_z^{(7)}\boldsymbol{\sigma}_z^{(8)}, \quad \boldsymbol{\sigma}_z^{(8)}\boldsymbol{\sigma}_z^{(9)}. \tag{4.8}$$

Again it is not hard to see that we are now able to correct single bit-flips in all three clusters.

Now, assume that one of the nine qubits is subjected to a phase flip, i.e. that the error is of the form $\boldsymbol{\sigma}_z^{(i)}.$, $i \in 1, 2, \ldots, 9.$, and let us see what happens to (4.6). For instance, if the relative phase of one of the first three qubits in $|\mathbf{0}\rangle$ flips, equation (4.6) changes into:

$$\frac{1}{\sqrt{2^3}}(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) = |\bar{1}\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle, \tag{4.9}$$

or for a general state:

$$\boldsymbol{\sigma}_z^{(i)} : \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \rightarrow \alpha|\bar{1}\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle + \beta|\bar{0}\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle, \qquad i \in 1, 2, 3. \tag{4.10}$$

This time, let us measure the observable: $\boldsymbol{\sigma}_x^{(1)}\boldsymbol{\sigma}_x^{(2)}\boldsymbol{\sigma}_x^{(3)}\boldsymbol{\sigma}_x^{(4)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(6)}$. The state (4.10) is an eigenstate of this observable with the eigenvalue -1 and it is an eigenstate of $\boldsymbol{\sigma}_x^{(4)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(6)}\boldsymbol{\sigma}_x^{(7)}\boldsymbol{\sigma}_x^{(8)}\boldsymbol{\sigma}_x^{(9)}$, with eigenvalue $+1$. It is not hard to see that we can proceed in the same manner for all three clusters, as we did for single qubits in the previous section, and thus determine in which cluster the phase flip has occurred. Figure 5 summarizes these results; notice that the recovery operations are also listed. The

Eigenvalue of $\boldsymbol{\sigma}_x^{(1)}\boldsymbol{\sigma}_x^{(2)}\boldsymbol{\sigma}_x^{(3)}\boldsymbol{\sigma}_x^{(4)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(6)}$	Eigenvalue of $\boldsymbol{\sigma}_x^{(4)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(6)}\boldsymbol{\sigma}_x^{(7)}\boldsymbol{\sigma}_x^{(8)}\boldsymbol{\sigma}_x^{(9)}$	This cluster flipped	Recovery operation
1	1	none	$\bigotimes_{i=1}^{9} \mathbf{1}^{(i)}$
-1	1	first	$\boldsymbol{\sigma}_z^{(i)}, i \in 1, 2, 3$
-1	-1	second	$\boldsymbol{\sigma}_z^{(i)}, i \in 4, 5, 6$
1	-1	third	$\boldsymbol{\sigma}_z^{(i)}, i \in 7, 8, 9$

Figure 5: Measurement of phase-flips in Shor's code

phase flip recovery method will work if phase flips occur in only *one* of the three clusters; two phase flips in the same cluster neutralize the effect of each other and three phase flips are equivalent to a single phase flip. Thus the scheme will also work if there is more than one phase flip in a particular cluster. However, if phase errors take place in more than one of the clusters, we will classify the error wrongly, and our recovery operation will not work, cf. the discussion of bit-flips in the previous section.

We can now conclude that we have a scheme for correcting bit- and phase-flips in a state encoded according to Shor's recipe; first we check if a bit flip has occurred in the three clusters (again assuming that at most one of the qubits in each cluster flips) and then we correct the errors by performing a suitable unitary transformation. Secondly we check if a phase flips has occurred in one of the clusters (again assuming that phase-flips only take place in at most one of the clusters). We can then correct the phase error by performing a suitable unitary transformation on the 9-qubit state.

4.2.3 Discussing the Assumptions

In this section we will discuss some of the assumptions we made about the errors, following Shor's arguments, [39].

We have made the assumption that the encoded qubits decohere independently, that is, the decoherence of a single qubit does not affect the other encoded qubits. This assumption may seem physically

[11] Again, the tensor product with the identity on the remaining nine qubits is implicit in the following.

incorrect, since in a noisy quantum channel, we would expect that it could be the case that one of the three clusters is exposed more so to errors, than the two others.

In his paper Shor argues that codes used for error correction in classical computers are often based on the assumption that bit-flip errors act independently on the bits, that is, the probability that a particular bit has flipped, does not increase or decrease if we know that one of neighbor-bits has flipped; this assumption is not true in practice for classical channels, but the error correcting codes for classical computers can be constructed to work very well, utilizing the fact that the errors on bits far from each other are almost independent. But since we cannot transfer principles from classical error correction to quantum error correction directly, we cannot conclude that the same would for a quantum channel, or as Shor says [39]: *It is not clear what the corresponding property would be in a quantum channel, or whether it would hold in practice.* The conclusion of his discussion can be summarized as follows: We accept the assumption, but keep in mind that it may have to be modified in order to suit a more appropriate quantum channel.

If we accept the assumption that the qubits decohere independently, the probability that a particular qubit decoheres is not affected, if we know that one of the other qubits has decohered. But the assumption that only one of qubits in each cluster flips and that phase-flips only take place in one cluster, may still seem doubtful. However, if we assume the probability that one qubit decoheres is small, the probability that two qubits in in a particular cluster flip and the probability that phase flips take place in two different clusters is very small.

4.2.4 Redundancy without Cloning

One could be tempted to ask the question: Does the encoding suggested in (4.3) and (4.7) violate the no-cloning theorem? Or equivalently, how do we encode an unknown qubit-state $|\psi\rangle = a|0\rangle + b|1\rangle$ into the 9-qubit state $|\boldsymbol{\psi}\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle$?. In fact we can perform the encoding without cloning; we can encode the nine qubit state via legal unitary transformations: The Hadamard transformation and the CNOT gate, defined in §2.4. Figure 6 shows the circuit which implements the encoding.

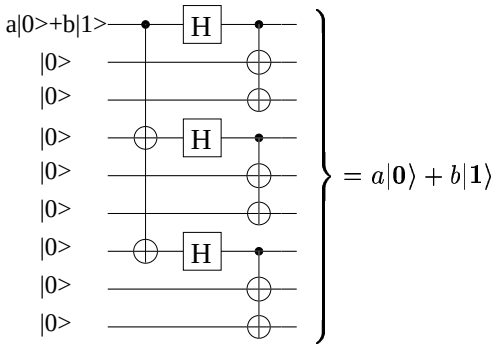

Figure 6: The encoding circuit for Shor's nine qubit code. The upper most horizontal line signifies the qubit $a|0\rangle + b|1\rangle$ which we want to encode. We encode it into the 9 qubit encoded state by using eight other qubits, initially in the state $|0\rangle$. The first gate is a double CNOT-gate, i.e. it is representing two CNOT-gates, cf. section 2.4.2. This double CNOT-gate entangles the three clusters. Then the single qubit Hadamard gate is performed on the first qubit of each cluster, and finally the entanglement within each cluster is established via three double CNOT gates. The circuit is adapted from[4].

Let us recapitulate what we have learnt so far. We have encoded one qubit into nine qubits, that is, we have encoded a general state in a redundant fashion by using the circuit in figure 6. The ressource exploited in the encoding is *entanglement*; by using Hadamard transformations and CNOT-gates we have encoded an arbitrary state into a highly entangled state of 9 qubits – we have encoded the information non-locally. When performing local measurements we do not have access to the coded information, and if the errors – as we have assumed – act locally on just a few bits, they cannot destroy the information. Preskill puts it very eloquently:

> The key conceptual insight that makes quantum error correction possible is that we can *fight entanglement with entanglement*[12]. Entanglement can be our enemy, since entanglement of our device with the environment can conceal quantum information from us, and so cause errors. But entanglement can also be our friend – we can encode the information that we want to protect in entanglement ... This information, then, cannot be accessed if we measure just a few qubits. By the same token, the information cannot be *damaged* if the environment interacts with just a few qubits [36].

The principles used in Shor's code are key principles in all quantum error correcting codes; we encode a qubit in an entangled state of a number of qubits in such a way that it is possible to measure the errors without measuring the state – we perform *syndrome* measurements. We can then recover from the error by a suitable unitary transformation. However, since Shor's code requires that each qubit is replaced by nine qubits, it is an expensive and impractical solution to our problems; we would like to construct codes that are more efficient.

4.3 Classical Error Correcting Codes

Our goal is to construct a more general class of quantum error correcting codes, the CSS codes. In order to understand the CSS codes we will have to introduce some results from classical error correction; that is, some general theory of classical linear codes. We will also present a classical *Hamming code* which is the framework behind Steane's 7 qubit code.

4.3.1 Basic Results of Classical Linear Error Correcting Codes

We will supply an introduction to the basic concepts and results of classical linear codes, necessary to understand the construction of the CSS codes. Since the theory is rather mathematical and non-physical, we will only state the main ideas, *not prove any of the results*. Our treatment of the subject will follow MacWilliams and Sloane [30] and Preskill [35].

In binary coding all calculations are carried out in the unique, finite field with only two elements, 0 and 1, the *Galois Field* $GF(2) \equiv F_2$[13]. This means that all calculations are done modulo 2. We wish to encode k bits in a string of n bits, $k < n$, that is, we choose 2^k of the 2^n n-bit strings to be our *codewords*. That the code is *linear* means that the codewords form a k-dimensional subspace of the 2^n n-bit string vector space F_2^n. This subspace is called the code subspace, C. If the k vectors $v_1, \ldots, v_k$ form a basis for C, an arbitrary codeword u can be written as a linear combination of the form:

$$u = u(a_1, \ldots, a_k) = \sum_i a_i v_i. \tag{4.11}$$

If G is the $k \times n$ matrix with rows consisting of the basis vectors $v_1, \ldots, v_k$;

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}, \tag{4.12}$$

and we use notation $a = (a_1, \ldots, a_k)$, we can write this equation in matrix form:

$$u(a) = aG. \tag{4.13}$$

The matrix G is called the *generator* matrix of our code. The reason G is called a generator is that the above equations generate an encoding of the k-bit message a into the n-bit codeword $u(a)$. Now the encoded message u is sent through a noisy channel and errors occur. The question is: Is it possible for a receiver to decode the message even though errors occur during the transmission? To answer this,

[12] We owe thanks to Preskill for the catchy wording of our title.

[13] We know from algebra that number of elements of a finite field always is of power of a prime, and that for every prime power p^n exactly one field with p^n elements exists, see for example [25].

the *parity check* matrix is of use; the parity check matrix of a linear code C is a $(n-k)\times n$ matrix H, with the property[14]:

$$Hu = \mathbf{0}, \qquad \text{where } \mathbf{0} \text{ denotes the zero vector,} \tag{4.14}$$

if and only if u is one of the codewords. Thus the receiver can check if the received message is one of the codewords by performing the parity check. But the receiver can do more: The only error available to a classical bit is the bit-flip, so an error acting on our n-bit message can be represented by an n-bit error vector e, containing 1's in the places where errors occur and 0's elsewhere. We can then express an error-stricken string of information u', as:

$$u \to u' = u + e. \tag{4.15}$$

If the receiver perform a parity check on the received message $u' = u + e$ he would obtain:

$$H(u') = H(u+e) = H(u) + H(e) = H(e). \tag{4.16}$$

$H(e)$ is called the *error syndrome* of the error e. If the syndrome is $\mathbf{0}$ the receiver assumes that the received message is the same as the one sent, but if it is different from $\mathbf{0}$, the she can conclude that errors have arisen during the transmission. Furthermore, if there is an unique correspondence between the errors we wish to be able to correct and the error syndromes, the receiver can tell which error has occurred by measuring the syndrome, and he can correct the error by flipping the bits back. If, for example, he measures the syndrome $H(e)$, he can turn the received message u' into the intended message u: $u' = u + e \overset{\text{correction}}{\longrightarrow} u + e + e = u$, by adding e to the received bit-string.

Of course this scheme cannot correct any number of possible errors; not all error strings e can have distinct syndromes. However, it is possible to deduce strict criteria for how many errors a given code is able to correct. To do so, we first have to introduce further concepts:

Definition: *The weight of a bit-string u, $wt(u)$, in the code subspace C is defined as the number of 1's in the code. The minimum distance, or distance, of a linear code C is the minimum weight of all nonzero vectors in C.*

The following theorem is one of the main results of the theory of error correcting codes. We use the notation $[a]$ for the greatest integer less that or equal to a.

Theorem: *A linear code with minimum distance d can correct $[\frac{1}{2}(d-1)]$ errors, that is, a code of minimum distance $d = 2t+1$ can correct t* errors.

When we say that a code can correct t errors, we mean that the code assigns a distinct syndrome to each vector of weight t, so if there is less than t bit-flip errors, the syndrome tells us where the the errors have occurred. But if there is more than t bit-flip errors, the scheme does not work.

To describe a linear code it is customary to use certain parameters; a linear code used for coding a k-bit string in an n-bit string, $k < n$, with minimum distance d, is called an $[n,k,d]$ code. There are 2^k message strings in a $[n,k,d]$ code (since we are encoding k bits).

We have now seen how a classical linear $[n,k,d]$ code works; we encode our message in a redundant fashion, so if (not too many) errors occur during the transmission, we can reconstruct the original message by using the parity check to measure the error, and finally rectify it.

If C is a linear code the parity check matrix H and the generator matrix G satisfy the identities:

$$HG^T = \bar{0}, \qquad GH^T = \bar{0}, \tag{4.17}$$

where the $\bar{0}$'s are zero matrices. The relations in equation (4.17) encourage us to turn things around and construct an $(n-k)$-dimensional code, $C^\perp$ with H^T as generator matrix and G as parity check matrix. This code is called the *dual* of C. $C^\perp$ consists of the vectors in F_2^n that are orthogonal to all the codewords in C, that is, all the vectors v in F_2^n satisfying $v \cdot u = 0$ for all $u \in C$. However, the

[14] Here u represents a column vector instead of a row vector. In general we will use the notation u for both the n bit column vector and the n bit row vector.

the word orthogonal can be misleading, since the scalar product in F_2^n is not an inner product – for instance, a vector in F_2^n can be self orthogonal (if it contains an even number of 1's), and hence C and $C^\perp$ can intersect. The dual code will turn out to be an important part of the CSS codes.

We will also need to utilize the concept of a *sub-code* of a classical linear code. C_2 is called a sub-code of C_1 if C_2 is a subspace of C_1. Since any codeword in C_2 is also a codeword in C_1 the codewords of C_2 have to satisfy additional constraints, that is, the number of rows in C_2's parity check matrix is greater than the number of rows in the parity check matrix of C_1.

4.3.2 The $[7,4,3]$ Hamming code

An important example of a classical linear code is the $[7,4,3]$ Hamming code C_1, since Steane's seven qubit code is constructed from it. It has the following parity check and generator matrices:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \qquad G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4.18}$$

The above generator matrix G encodes a four bit message in a seven bit message, and thus there are $2^4 = 16$ message strings in the corresponding code subspace C. These message strings are:

$$\begin{array}{llll} 0000000, & 1010101, & 0110011, & 1100110, \\ 0001111, & 1011010, & 0111100, & 1101001, \\ 1111111, & 0101010, & 1001100, & 0011001, \\ 1110000, & 0100101, & 1000011, & 0010110. \end{array} \tag{4.19}$$

The dual of the $[7,4,3]$ Hamming code – the code with H as generator matrix – is the sub-code of the $[7,4,3]$ Hamming code, which contains precisely the codewords with even weight[15]. Therefore the dual of the $[7,4,3]$ Hamming code is a $[7,3,4]$ code. We will refer to the dual code as the even sub-code, and denote it by C_2. Since $(C^\perp)^\perp = C$, we see that $C_2^\perp = C_1$, that is, the dual of the even sub-code is the $[7,4,3]$ Hamming code.

4.4 Theory of CSS Codes

We have now completed the mathematical treatment of classical linear codes, and are ready to utilize this knowledge to describe a general class of quantum error correcting codes, the *Calderbank Shor Steane* codes. Our review is based on [35, 22, 40, 5].

Our starting point is a classical $[n, k_1, d_1]$ linear code, C_1, with a $[n, k_2, d_2]$ sub-code C_2, where $k_2 < k_1$. We denote the parity check matrices of C_1 and C_2, H_1 and H_2, respectively. This means that H_1 is a $(n - k_1) \times n$ matrix and H_2 is a $(n - k_2) \times n$ matrix.

We can use the sub-code C_2 to define an equivalence relation in C_1. We say that two codewords u, v in C_1 are equivalent if and only if $u = v + w$ for some $w \in C_2$. This is easily seen to be an equivalence relation, and hence it divides C_1 into equivalence classes; these equivalence classes are called the *cosets* of C_2 in C_1. The number of different cosets are $\frac{2^{k_1}}{2^{k_2}} = 2^{k_1 - k_2}$. The basic idea is to use these cosets to construct a quantum code, so before we move move on, note that we are now discussing *qubits*, not bits; that is, we identify a string u of n classical bits with the corresponding n-qubit state $|u\rangle$.

The key principle in this construction is to assign a codeword to each of the cosets; this is done by taking the equally weighted superposition of all the codewords in each coset and using these superpositions as codewords:

$$|\mathbf{w}(w)\rangle_B \equiv |\mathbf{w}\rangle_B = \frac{1}{\sqrt{2^{k_2}}} \sum_{u \in w\text{'s coset}} |u\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{v \in C_2} |v + w\rangle. \tag{4.20}$$

The states $|\mathbf{w}\rangle_B$ are clearly normalized and mutually orthogonal[16]. For quantum error correcting codes we will use the word *codespace* to refer to the Hilbert space spanned by the words of each coset. Since

[15] That is, the dual code consists of the two top rows of codewords in (4.19).

[16] Of course this time the orthonormality refers to the Hilbert space of the qubits, $\langle \mathbf{w}' | \mathbf{w} \rangle = \delta_{\mathbf{w}',\mathbf{w}}$.

$|\mathbf{w}\rangle_B = |\mathbf{v}\rangle_B$ if v and w belong to the same coset, we infer that the number of codewords defined by (4.20) is equal to the number of cosets, i.e. the codespace has dimension $2^{k_1-k_2}$. Hence we are encoding a $(k_1 - k_2)$-qubit state into an n-qubit state. A code constructed via this procedure is called a CSS code, and the states defined by (4.20) are naturally called the *basis states* of the CSS code.

4.4.1 Correcting Bit-flips

Now suppose that $d_1 \geq 2t_B + 1$, where d_1 is the minimum distance of C_1. We then know from section 4.3.1 that C_1 is able to correct t_B (classical) bit-flip errors. As we will proceed to show, the quantum code defined by (4.20) is also able to correct t_B qubit-flip errors.

Assume that we have a general encoded state $|\mathbf{a}\rangle$ which is a superposition of the words in (4.20), $|\mathbf{a}\rangle = \sum_i c_{\mathbf{w}}|\mathbf{w}\rangle_B$, and that t_B bit-flips occur. We can describe these bit-flips with the operator $\boldsymbol{\sigma}_x$ acting on at most t_B qubits where, of course, the identity acts on the remaining undisturbed qubits. Another way to describe the bit-flip errors is to use an error vector $|e\rangle$, where e is a bitstring with 1's on the entry's where bit-flip errors occur and 0's elsewhere. If the state $|u\rangle$, where $u \in C_1$, is subjected to these bit-flip errors, it changes according to:

$$|u\rangle \longrightarrow |u'\rangle = |u + e\rangle \tag{4.21}$$

If we now let system A consists of a suitable number $(n - k_1)$ of *ancilla*[17] qubits, initially in the state $|I\rangle_A$, then we can perform the unitary transformation defined by:

$$|u'\rangle \otimes |I\rangle_A \longrightarrow |u'\rangle \otimes |H_1 u'\rangle_A = |u'\rangle \otimes |H_1 u + H_1 e\rangle_A = |u'\rangle \otimes |H_1 e\rangle_A, \tag{4.22}$$

where we have utilized the fact that $H_1 u = 0$ since $u \in C_1$. But we can do more than this; the basis states of the CSS code (4.20) are superpositions of C_1 codewords, and if such a basis state $|\mathbf{w}\rangle_B$ is subjected to the bit flips described by the error bitstring e, it changes to the error state $|\mathbf{w}'\rangle_B$, according to:

$$|\mathbf{w}\rangle_B = \frac{1}{\sqrt{2^{k_2}}} \sum_{u \in w\text{'s coset}} |u\rangle \overset{\text{bitflip error}}{\longrightarrow} |\mathbf{w}'\rangle_B = \frac{1}{\sqrt{2^{k_2}}} \sum_{u \in w\text{'s coset}} |u + e\rangle \tag{4.23}$$

Hence, if we perform the unitary transformation defined by (4.22) on the error afflicted superposition $|\mathbf{w}'\rangle_B$, the resulting state would be $|\mathbf{w}'\rangle_B \otimes |H_1 e\rangle_A$; thus if one of the basis states of the CSS code is exposed to less than t_B bit-flip errors, we can measure the syndrome by measuring the ancillas, and finally recover the state by performing a suitable unitary transformation. The most general encoded state is a linear superposition of the basis codewords $|\mathbf{a}\rangle = \sum_i c_{\mathbf{w}}|\mathbf{w}\rangle_B$, so we easily see that if a general state is subjected to bit-flip errors, then – by using ancilla qubits – we can perform a syndrome measurement by measuring the ancilla system A; we measure the ancilla qubits in the standard basis, and obtain the result $|H_1 e\rangle_A$. If less than t_B bit-flip errors have occurred, the syndrome $|H_1 e\rangle_A$ tells us the value of the string e, which discloses the positions of the bit-flip errors. Again we are measuring the errors and not the state.

4.4.2 Phase-flips: Rotating the Basis

In section 4.1.1 we noted that a bit-flip in the standard basis corresponds to a phase-flip in the Hadamard rotated basis and that phase-flips in the standard basis corresponds to bit-flips in the Hadamard rotated basis and *vice versa*. We will now use this fact to correct phase-flip errors with the general CSS code. Consider the action of the bitwise Hadamard gate $\mathbf{H}^{(n)}$ on the code basis state $|\mathbf{w}\rangle_B$, cf. (4.20):

$$\begin{aligned} \mathbf{H}^{(n)}: \quad |\mathbf{w}\rangle_B &= \frac{1}{\sqrt{2^{k_2}}} \sum_{v \in C_2} |v + w\rangle \\ \longrightarrow \quad |\mathbf{w}\rangle_P &= \frac{1}{\sqrt{2^n}} \sum_u \frac{1}{\sqrt{2^{k_2}}} \sum_{v \in C_2} (-1)^{u \cdot v} (-1)^{u \cdot w} |u\rangle \\ &= \frac{1}{\sqrt{2^{n-k_2}}} \sum_{u \in C_2^\perp} (-1)^{u \cdot w} |u\rangle, \end{aligned} \tag{4.24}$$

[17] The correct usage of of this word would be *ancillary* qubits, but we will follow the tradition and use the wording, ancilla qubits.

where we have used the expression (2.13) to obtain the second equality and the identity known from classical coding theory:

$$\sum_{v\in C}(-1)^{u\cdot v} = \begin{cases} 2^k & u \in C^\perp \\ 0 & u \notin C^\perp \end{cases}, \tag{4.25}$$

to derive the final equality. We will not prove (4.25) here, but a simple proof can be found in [35]. Notice that the dot products are done modulo 2. We see that the result of the bitwise Hadamard transformation is a superposition of the words in the dual code $C_2^\perp$. This time it is not an equally weighted superposition; every word $|u\rangle$, where $u \in C_2^\perp$, is weighted by $\frac{(-1)^{u\cdot v}}{\sqrt{2^{n-k_2}}}$.

Suppose that $C_2^\perp$ has minimum distance $d_2^\perp \geq 2t_P + 1$. Then we know from §4.3 that $C_2^\perp$ is able to correct t_P classical bit-flip errors. We also know that the parity check matrix of the code $C_2^\perp$ is the generator matrix of the code C_2, G_2. So we can re-use the arguments from the previous section to show that by means of k_2 ancilla qubits and the following unitary transformation, we can detect t_P bit-flip errors in the rotated basis given by (4.24):

$$|u\rangle \otimes |I\rangle_A \longrightarrow |u\rangle \otimes |G_2 u\rangle_A \tag{4.26}$$

Since phase-flips in the standard basis are equivalent to bit-flips in the Hadamard rotated basis, phase-flips in the codebasis (4.20) emerge as bit-flips in the rotated codebasis (4.24). Since we are able to correct t_P bit-flips in the rotated codebasis, we are able to correct t_P phase-flips in the standard codebasis.

4.4.3 Correction of Errors

Our procedure for correcting the errors in a CSS code is as follows: First we perform a syndrome measurement of bit-flips and correct these, secondly we perform a syndrome measurement of phase-flips and correct these[18].

So far we have not discussed how to correct the errors, but only stated that a suitable unitary transformation should be performed. However, the correctional procedure is not a difficult task: Our bit-flip syndrome measurement tells us where bit-flips have occurred (if the number of bit-flip errors is less than t_B) and in order to correct the errors, we simply flip the afflicted qubits back, using $\boldsymbol{\sigma}_x$ on the qubits subjected to bit-flip errors. In order to correct phase-flips, we first let $\mathbf{H}^{(n)}$ act on the state, and then perform a bit-flip syndrome measurement in the rotated basis, that is, phase-flip syndrome measurement in the codebasis. If less than t_P phase errors have occurred, the syndrome measurement tells us which qubits have suffered phase-flips.

We can now do two things to correct these phase-flips. We can apply $\boldsymbol{\sigma}_x$ to the afflicted qubits, i.e correct bit-flips in the rotated basis, and afterwards apply $\mathbf{H}^{(n)}$ again to rotate the codewords back to the codebasis. *Or* we can apply $\mathbf{H}^{(n)}$ first and then correct the phase-flip errors in the codebasis, using $\boldsymbol{\sigma}_z$ on the qubits that have been exposed to phase-flip errors. As an famous example to make these notions more explicit, we will now take a look at Steane's seven-qubit code [40] from 1995.

4.5 Steane's Seven Qubit Code

The results from the previous section will now be implemented to construct a seven qubit error correcting code. Our discussion of this code will be based on [35] and on articles by Preskill [36] and Steane [40].

Our starting point is the classical $[7, 4, 3]$ Hamming code, discussed in §4.3.2, which we will identify with C_1. The even subcode of the $[7, 4, 3]$ Hamming code will be identified with C_2. Since we know from §4.3.2 that the even subcode is a $[7, 3, 4]$ code, we see that C_2 divides C_1 into $2^{4-3} = 2$ cosets (equivalence classes). Thus these two classical codes induce a CSS code with two basis codewords, *viz.*

[18] Of course we can postpone the recovery operations until after all of our measurements have been made, since bit-flip errors in the standard basis emerge as phase errors in the Hadamard rotated basis, and therefore have no bearing on the outcome of the measurement of bit errors in the Hadamard rotated basis (phase errors in the standard basis). We have merely divided the process into two separate parts for transparency

the equally weighted superposition of codewords in each coset, cf. (4.20);

$$\begin{aligned} |\mathbf{0}\rangle_B &= \tfrac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &\quad +|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\ |\mathbf{1}\rangle_B &= \tfrac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &\quad +|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle) \end{aligned} \tag{4.27}$$

So if we decide for $|\mathbf{0}\rangle_B$ to be the encoded $|0\rangle$ and for $|\mathbf{1}\rangle_B$ to be the encoded $|1\rangle$, we code $|0\rangle$ into the equally weighted superposition of all the $[7,4,3]$ Hamming codewords with even weight and $|1\rangle$ into the superposition of the $[7,4,3]$ Hamming codewords with odd weight. The classical $[7,4,3]$ Hamming code is able to correct one classical bit-flip error since it has minimum distance $3 = 2 \cdot 1 + 1$; then from the previous section, we know that the quantum code defined by (4.27) is able to correct a single bit-flip error. We now introduce an ancilla system A with 3 ancilla qubits, so we can perform the unitary transformation defined by:

$$|u\rangle \otimes |I\rangle_A \longrightarrow |u\rangle \otimes |Hu\rangle_A. \tag{4.28}$$

H denotes the parity check matrix for the $[7,4,3]$ Hamming code defined by (4.18) and as we will see later, the initial state of the ancilla system A, $|I\rangle$, can be chosen to be $|000\rangle_A$. As described in §4.4, by measuring the ancilla system, and assuming that at most one bit-flip error occurs, we can perform a syndrome measurement on a general state in the codespace. In §4.5.1 we will describe how we actually will perform the syndrome measurement.

In order to correct phase flips we perform the bitwise Hadamard transformation $\mathbf{H}^{(n)}$ on the code basis states (4.27), cf. (4.24). Since the dual code of the even subcode C_2 is the original $[7,4,3]$ Hamming code C_1, both the Hadamard rotated basis codewords become superpositions of all the 16 codewords in the $[7,4,3]$ Hamming code.

$$\begin{aligned} \mathbf{H}^{(7)} : |\mathbf{0}\rangle_B &\rightarrow |\mathbf{0}\rangle_P = \tfrac{1}{\sqrt{2}}(|\mathbf{0}\rangle_B + |\mathbf{1}\rangle_B) \\ \mathbf{H}^{(7)} : |\mathbf{1}\rangle_B &\rightarrow |\mathbf{1}\rangle_P = \tfrac{1}{\sqrt{2}}(|\mathbf{0}\rangle_B - |\mathbf{1}\rangle_B) \end{aligned} \tag{4.29}$$

We then perform the unitary transformation given by (4.26), using the fact that the generator matrix of C_2 is the parity check matrix of $C_2^{\perp} = C_1$:

$$|u\rangle \otimes |I\rangle_A \longrightarrow |u\rangle \otimes |Hu\rangle_A \tag{4.30}$$

We know from section 4.4 that we by performing the operation (4.30) are able to correct one bit-flip error in the Hadamard rotated basis (since $C_2^{\perp} = C_1$ has minimum distance 3), that is, one phase-flip error in the standard basis.

4.5.1 The Syndrome Measurements

So far the general treatment of Steane's code has been rather abstract, and in this section we will take a look at how the encoding and the syndrome measurements are performed. Figure 7 shows how the encoding is performed. Understanding what takes place in figure 7 is not so difficult [22]. First, the double CNOT gate, acting on $\{1\}$ as source and $\{2\}$ and $\{3\}$ as target qubits, takes the seven qubits to the state $a|0000000\rangle + b|1110000\rangle$, and the three Hadamard gates (on $\{5\}$, $\{6\}$, $\{7\}$) produce the equally weighted superposition of all eight possible values of the last three qubits. The last three triple CNOT gates then generate the state $a|\mathbf{0}\rangle_B + b|\mathbf{1}\rangle_B$, cf. (4.27).

Until now, our only prescription for "measuring" the bit-flip errors has been performing the unitary transformation (4.28); subsequently measuring the three ancilla qubits then makes us able to diagnose possible single bit-flip errors. This may seem quite abstract, so we will now take a look at how this is actually done to bring things down to earth, Figure 8 displays the circuit for detecting errors. The three ancilla qubits are initially prepared in the state $|000\rangle_A$. We will now explain how to diagnose bit-flip errors using this circuit. We first notice that this circuit is a quantum circuit version of the parity check matrix H of the $[7,4,3]$ Hamming code, cf. section 4.3.2, equation (4.18). – The first cluster of four CNOT gates corresponds to the row (0001111), since there are CNOT gates working

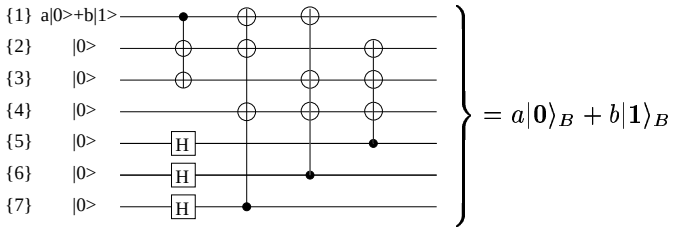

Figure 7: The encoding circuit for Steane's seven bit code. Innocent looking as it is, this circuit takes an arbitrary state $a|0\rangle + b|1\rangle$ (represented by the uppermost horizontal line) and using the six $|0\rangle$ states below it, it encodes the state, $a|0\rangle + b|1\rangle$, into a highly entangled superposition of the encoded basis states of Steane's code (4.27). The circuit is adapted from [36]

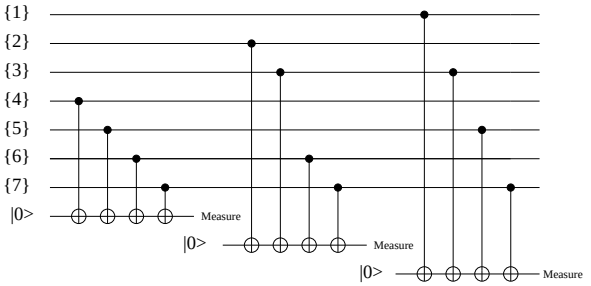

Figure 8: The error correcting circuit for Steane's seven bit code. A detailed explanation of how this circuit works is in the main text. This circuit is adapted from [22].

on the final four qubits: {4}, {5}, {6}, and {7}. These gates are equivalent to final sting of ones in the string (0001111), the second cluster of four CNOT gates corresponds to the row (0110011) and the third to (1010101).

If the circuit acts on any state $|u\rangle$, where u is one of the codewords in the $[7,4,3]$ Hamming code, the state of the ancilla qubits is easily seen to be $|000\rangle_A$. But if for example qubit 4 flips, and we run the circuit, the output in the ancilla qubits will be $|100\rangle$, generally we have:

This qubit flipped	Ancilla state (syndrome)
none	$\|000\rangle$
{1}	$\|001\rangle$
{2}	$\|010\rangle$
{3}	$\|011\rangle$
{4}	$\|100\rangle$
{5}	$\|101\rangle$
{6}	$\|110\rangle$
{7}	$\|111\rangle$

Since any state encoded in Steane's code, $a|\mathbf{0}\rangle_B + b|\mathbf{1}\rangle_B$, is a superposition of the states $|u\rangle$, where u is a $[7,4,3]$ Hamming codeword, we see that this syndrome applies equally well to any encoded state. Thus we see that this circuit is able to detect a single bit-flip. After the bit-flip error has been diagnosed, we can proceed to flip it back, using $\boldsymbol{\sigma}_x$. Furthermore the circuit is devised so cleverly that the measured state of the ancilla qubits is the binary representation of which qubit was flipped, e.g. $\{4\} \sim 100$. But if more than one qubit flips, the scheme will miscategorize the error; since there are only eight distinct syndromes, two bit-flips will necessarily result in a syndrome, which will be interpreted as a single bit-flip.

We recall that phase-flip errors in the standard basis are equivalent to bit-flip errors in the Hadamard rotated basis, so in order to correct phase-flip errors, we simply repeat the syndrome measurement procedure in the bitwise Hadamard rotated basis, using the fact that the parity check matrix of $[7,4,3]$

Hamming code both detects bit-flip errors in the standard basis and in the bitwise Hadamard rotated basis, cf. (4.28) and (4.30).

4.6 Discussion of the Error Model

So far we have used the simplified error model, that is, we have assumed that the only errors decoherence can cause on a qubit are bit-flips, phase-flips and both bit- and phase-flips. This is not a realistic assumption; we know from section 3 that decoherence generally causes an initial pure state of an open system to evolve into a mixed state, so assuming that errors occur as described by the simplified error model is clearly too crude an assumption. However it turns out that the simplified error model is not as simplified as it may seem at first sight; we will now justify our use of it by reconsidering the decoherence process of a qubit following Preskill [35] and Gottesman [9].

Recall from section 4.1.1 that if the qubit is initially in the state $|\psi\rangle$ and the environment initially is in the state $|e_I\rangle_E$, the most general unitary evolution of qubit and environment can be represented as:

$$\mathbf{U} : |\psi\rangle|e_I\rangle_E \to \mathbf{1}|\psi\rangle \otimes |e_\mathbf{1}\rangle_E + \boldsymbol{\sigma}_x|\psi\rangle \otimes |e_x\rangle_E + \boldsymbol{\sigma}_z|\psi\rangle \otimes |e_z\rangle_E + i\boldsymbol{\sigma}_y|\psi\rangle \otimes |e_y\rangle_E, \tag{4.31}$$

where the states $|e_\mathbf{1}\rangle_E$, $|e_x\rangle_E$,$|e_z\rangle_E$, and $|e_y\rangle_E$ are not necessarily mutually orthogonal or normalized.

This result is trivial, it follows naturally from the fact that the matrices

$$\{\mathbf{1}, \boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y, \boldsymbol{\sigma}_z\} \tag{4.32}$$

are a basis for the vector space of 2×2 matrices. We can obtain a similar result for a general n qubit state; any $2^n \times 2^n$ matrix acting on a Hilbert space of n qubits can be written in terms of tensor product strings of the single qubit operators in (4.32), that is in terms of the $4^n = 2^{2n}$ unitary operators

$$\{E_a\} \equiv \{\mathbf{1}, \boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y, \boldsymbol{\sigma}_z\}^{\otimes n}. \tag{4.33}$$

Let us assume that the n qubit system is initially in the state $|\psi\rangle$ and the environment initially is in the state $|e_I\rangle_E$. The most general unitary evolution of the n qubit system and the environment can be written:

$$U : \quad |\psi\rangle \otimes |e_I\rangle_E \longrightarrow \sum_{\{E_a\}} E_a|\psi\rangle \otimes |e_{E_a}\rangle_E \tag{4.34}$$

where the states $\{|e_{E_a}\rangle_E\}$ of the environment are not assumed to be mutually orthogonal or normalized. We can think of this expansion as if the state of our n qubit system and the environment evolves into a linear combination of error stricken states $E_a|\psi\rangle \otimes |e_{E_a}\rangle_E$.

Now, we choose a subspace of the 2^n dimensional Hilbert space of the n qubit system to be the code subspace $\mathcal{H}_{code}$, and we let $\{|\mathbf{i}\rangle\}$ be a orthonormal basis of this subspace. We can also choose a subset S of the operators in (4.33) to be the errors we wish to correct, that is, to be the most likely errors. We assume that the following condition is satisfied:

$$\langle\mathbf{j}|E_b^\dagger E_a|\mathbf{i}\rangle = \delta_{ab}\delta_{ij} \tag{4.35}$$

for all $E_a, E_b \in S$ and all i, j. This establishes the fact that the errors E_a map the code subspace onto *mutually orthogonal* subspaces, called *error subspaces*:

$$\mathcal{H}_a = E_a\mathcal{H}_{code} \tag{4.36}$$

If a general encoded state $|\varphi\rangle$ is subjected to errors from the set S, the resulting state of the n qubit system and the environment is, cf (4.34),

$$\sum_{E_a \in S} E_a|\varphi\rangle \otimes |e_{E_a}\rangle_E. \tag{4.37}$$

Since the E_a's take the code subspace to mutually orthogonal subspaces, we can perform an orthogonal measurement that projects the n qubit state onto one of the error subspaces, $\mathcal{H}_a$, and thus the state of the system collapses into:

$$E_a|\varphi\rangle \tag{4.38}$$

This measurement projects the state of the system onto a state $E_a|\varphi\rangle$, that is, the original encoded state subjected to one of the errors E_a. The measurement outcome tells us which error has occurred, and since the E_a's are unitary, we can reverse the error by performing the unitary transformation $E_a^\dagger = E_a$.

To summarize the discussion: Decoherence, that is, the unitary evolution of system and the environment, leads to a non-unitary evolution of the n qubits (the system) alone. Accordingly, the initial n qubit state alone evolves into a mixture (as the observer does not have access to the environment), and this could lead one to assume that it is impossible to recover the original state. But by clever encoding we are in fact able to *digitize* the errors. By performing a suitable measurement of the n qubit system we project the n qubit state onto a state which is either the encoded state (if $E_a = \mathbf{1}^{(1)} \otimes \mathbf{1}^{(2)} \otimes \ldots \otimes \mathbf{1}^{(n)}$), or onto a state with an error that can be described using the simplified error model. Finally we can measure and recover from the error via an unitary transformation.

4.6.1 The Seven Qubit Code Revisited

We will now justify the use of the simplified error model in the discussion of Steane's seven qubit code, cf. section 4.5. We first note that we can describe Steane's code in a manner similar to the way we described syndrome measurements in Shor's nine qubit code. Measuring bit-flips and phase-flips by running the circuit in figure 8 in the standard basis and the Hadamard rotated basis, respectively, is equivalent to measuring the six commuting observables:

$$\begin{aligned} &\boldsymbol{\sigma}_z^{(4)}\boldsymbol{\sigma}_z^{(5)}\boldsymbol{\sigma}_z^{(6)}\boldsymbol{\sigma}_z^{(7)}, \quad \boldsymbol{\sigma}_z^{(2)}\boldsymbol{\sigma}_z^{(3)}\boldsymbol{\sigma}_z^{(6)}\boldsymbol{\sigma}_z^{(7)}, \quad \boldsymbol{\sigma}_z^{(1)}\boldsymbol{\sigma}_z^{(3)}\boldsymbol{\sigma}_z^{(5)}\boldsymbol{\sigma}_z^{(7)}, \\ &\boldsymbol{\sigma}_x^{(4)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(6)}\boldsymbol{\sigma}_x^{(7)}, \quad \boldsymbol{\sigma}_x^{(2)}\boldsymbol{\sigma}_x^{(3)}\boldsymbol{\sigma}_x^{(6)}\boldsymbol{\sigma}_x^{(7)}, \quad \boldsymbol{\sigma}_x^{(1)}\boldsymbol{\sigma}_x^{(3)}\boldsymbol{\sigma}_x^{(5)}\boldsymbol{\sigma}_x^{(7)}, \end{aligned} \tag{4.39}$$

where each cluster of four CNOT gates in the circuits corresponds to an observable.

In Steane's seven qubit code, we encode one qubit state into a seven qubit state. The general evolution of such a seven qubit state and the environment is given by (4.34), where the $\{E_a\}$'s range over the set:

$$\{E_a\} \equiv \{\mathbf{1}, \boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y, \boldsymbol{\sigma}_z\}^{\otimes 7}. \tag{4.40}$$

The errors out of this set which we want to be able to correct, are the ones, which we were able to correct using the simplified error model, that is, $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$ acting on at most one qubit each, possibly on the same qubit, that is, $\boldsymbol{\sigma}_y$ acting on a single qubit (of course the identity is acting on the remaining qubits). We denote this subset of (4.40) by S. Using a code subspace with (4.27) as a basis, we encode one qubit into seven qubits. We easily see that the condition (4.35) is satisfied for all the errors we wish to correct; i.e. the errors we wish to be able to correct map the code subspace to mutually orthogonal subspaces. Now, let us assume that the error operators $\{E_a\}$ in the expansion (4.34) belong to S, and as was discussed in the previous section, we are able then to digitize the errors: By measuring the observables in (4.39) the state of the seven qubit system is projected onto either the code subspace or onto one of the error subspaces. In other words, we project the state of the seven qubits onto a state which is the encoded state acted upon by one of the operators from the set S, that is, the encoded state subjected to at most a single bit-flip and at most a single phase-flip. Hence the use of the simplified error model has been justified.

In Steane's code we perform the measurement of the observables in 4.39, using CNOT gates and ancilla qubits. An instructive way to think about this is to consider it a Von Neumann measurement, cf. section 3.2.1, in which the seven qubits can be considered the system and the ancilla qubits the pointer. The CNOT gates establish the coupling between the system and the pointer (the ancilla qubits), and by measuring the pointer we perform an orthogonal measurement of the system.

4.6.2 The Nine Qubit Code Revisited

Steane's code is a *non-degenerate* code, because measuring the observables in 4.39 uniquely determines which error has occurred, this is because the condition (4.35) is fulfilled; this is not the case for Shor's code. It is *degenerate*. The reason it is called degenerate is that phase-flip errors acting on the different qubits in each cluster affect the code subspace in exactly the same way:

$$\boldsymbol{\sigma}_z^{(i)} : \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \to \alpha|\bar{1}\rangle \otimes |\bar{0}\rangle \otimes |\bar{0}\rangle + \beta|\bar{0}\rangle \otimes |\bar{1}\rangle \otimes |\bar{1}\rangle, \qquad i \in 1, 2, 3., \tag{4.41}$$

and so forth. This is no problem; even tough we cannot determine which qubit suffered the error, we can easily correct it. As we have already explained in section 4.2 we simply apply the recovery operation to one of the qubits in the afflicted cluster. For example in equation (4.41), we simply apply any one of the three operators: $\boldsymbol{\sigma}_z^{(i)}, i \in 1,2,3$. The rest of the justification the use of the simplified error model for this code is analogous to one presented for Steane's code in the previous section. Thus we will not go into further detail here, but merely state that the use of the simplified error model *is* justified for Shor's nine qubit code.

5 Perspectives

This concludes the stringent theory, and what have we learnt so far? Via the examples, we have been able to distill the most important elements of quantum error correcting codes from the theory. We should construct our quantum error correcting code to utilize the following central ideas

1. The syndrome measurements
2. Fighting entanglement with entanglement
3. Digitizing the errors

These principles are the mechanism which make the codes that we have discussed so effective, and a clever use of these principles is the cornerstone of the modern quantum error correcting codes

One might think that a review of the most recent theory of quantum error correction would have been on its place at this point of the report, but we have decided not to discuss the subject here, as the theory is not very intuitive and the mathematical contents of the codes makes it difficult to present in popular writing. We have carefully choosen the codes used so far in this report, because they contain a minimum of formalism and still illustrate all the principles of quantum correction.

In this concluding section we will instead take a look at the experiments that have been performed, in order for us to put all of the theory in perspective. As was the case, when we investigated the technological progress, we will see that the theory is far, far ahead of the experiments.

5.1 Experimental Quantum Error Correction

Now, one might also put the question: does all of this theory hold in practice? If quantum error correction is not experimentally applicable, the entire project of quantum error correction would be like trying to remedy a futile theory with an unusable one. Luckily error correction works! So far the world has seen two experiments, both using simple quantum error correcting codes[19].

Both of the experiments use NMR technology[20] as quantum computers, and because of the limited number of qubits, both are only able to correct phase errors. In one of the experiments, performed by a group from Los Alamos National Laboratory and MIT [14], one qubit was encoded into three qubits. Subsequently two of the qubits (ancillas) were measured to see if an error had occurred, in which case, the damage could be repaired. Their conclusion is very positive: *These experiments confirm ... the validity of theories of quantum error correction in a simple case* [14].

The second experiment was conducted by a group from IBM/Almaden and Standford University [15]. In this experiment a simple two qubit code that detects a single phase error in either one of the two qubits. This code is a *detection* code, which means that the errors are not corrected, but merely rejected. Again the conclusion is positive: *We have demonstrated experimentally, in a bulk NMR system, that using a two bit phase dampening detection code, the distortion of the accepted output states can be largely removed* [15].

All in all we find that the evidence that quantum error correction is applicable is convincing, and we conclude that quantum error correction is a successful tool for battling decoherence and performing quantum computing.

[19]The codes have to be simple, since the maximum number of qubits is very limited, cf. section 1.2. Furthermore, the gates used for encoding are very primitive

[20]cf. section 1.2.4

5.2 A Concluding Remark

Quantum error correction has been the fastest growing field within quantum computing, a branch of physics which in itself has experienced an almost uncontrollable growth. Furthermore, as we have seen in the previous section, *quantum error correction works!*. So on the end note of this report, we feel some of the same reluctant optimism that Laflamme displays in the initial quote. We think that, with the help of quantum error correction, quantum computing will be possible in 20, 30, 40 years maybe ...

Appendices

A The Reduced Density Matrix

Usually the density matrix is derived by considering an *ensemble* of pure quantum states, cf. [17, 3]; in the following, we will consider the *reduced* density matrix. The reduced density matrix is deduced by examining a subsystem of a larger system. Our treatment of the subject will follow Preskill [35].

We will assume that we have a bipartite system consisting of the two subsystems A and B, and let us denote an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$ by $\{|i\rangle_A \otimes |j\rangle_B\}$, where $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Any pure state $|\psi\rangle_{AB}$ of the bipartite system can be expanded in this basis:

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij}|i\rangle_A \otimes |j\rangle_B, \qquad \sum_{i,j} |c_{ij}| = 1. \tag{A.1}$$

Now let $\mathbf{O}_A$ be an observable of system A only. The expectation value of the operator $\mathbf{O}_A \otimes \mathbf{1}_B$ which also only acts on system A, is given by:

$$\begin{aligned} \langle \mathbf{O}_A \rangle &= {}_{AB}\langle\psi|(\mathbf{O}_A \otimes \mathbf{1}_B)|\psi\rangle_{AB} \\ &= \Big(\sum_{i,j} c^*_{ij}({}_A\langle i| \otimes {}_B\langle j|)\Big)(\mathbf{O}_A \otimes \mathbf{1}_B)\Big(\sum_{k,l} c_{kl}(|k\rangle_A \otimes |l\rangle_B)\Big) \\ &= \Big(\sum_{i,j} c^*_{ij}({}_A\langle i| \otimes {}_A\langle j|)\Big)\Big(\sum_{k,l} c_{kl}(\mathbf{O}_A|k\rangle_A \otimes |l\rangle_B)\Big) \qquad = \sum_{i,k,l} c^*_{il}c_{kl}\langle i|\mathbf{O}_A|k\rangle. \end{aligned} \tag{A.2}$$

We see that this equation can be written:

$$\langle \mathbf{O}_A \rangle = \mathrm{tr}(\mathbf{O}_A \boldsymbol{\rho}_A), \tag{A.3}$$

where the density matrix $\boldsymbol{\rho_A}$ is defined by

$$\boldsymbol{\rho_A} = tr_B(|\psi\rangle_{AB\,AB}\langle\psi|) = \sum_{i,k,l} c_{kl}c^*_{il}|k\rangle_{A\,A}\langle i| \tag{A.4}$$

We easily see that $\boldsymbol{\rho_A}$ satisfy:

1. $\boldsymbol{\rho}_A$ is hermitian; $\boldsymbol{\rho}_A = \boldsymbol{\rho}^\dagger_A$
2. $\boldsymbol{\rho}_A$ has unit trace: $\mathrm{tr}(\boldsymbol{\rho}_A) = \sum_{k,l} |c_{kl}|^2 = 1$
3. $\boldsymbol{\rho_A}$ is nonnegative, ie. ${}_A\langle\psi|\boldsymbol{\rho}_A|\psi\rangle_A = \sum_l |\sum_k c_{kl}\,{}_A\langle\psi|k\rangle|^2 \geq 0$, for all $|\psi\rangle_A$.

From the properties (1)-(3) we see that $\boldsymbol{\rho}_A$ can be diagonalized and that it has real, nonnegative eigenvalues. Since the trace-operation is invariant under change of basis, we also infer that the eigenvalues sum to one.

If we express $\boldsymbol{\rho}_A$ in the eigenstate basis, i.e. in the basis in which it is diagonal, we get:

$$\boldsymbol{\rho_A} = \sum_a p_a|\psi_a\rangle\langle\psi_a|, \qquad 0 < p_a \leq 1, \qquad \sum_a p_a = 1. \tag{A.5}$$

The expectation value of an observable $\mathbf{O}_A$ acting on system A can be written:

$$\langle \mathbf{O}_A \rangle = \mathrm{tr}(\mathbf{O}_A\boldsymbol{\rho}_A) = \sum_a p_a\langle\psi_a|\mathbf{O}_A|\psi_a\rangle. \tag{A.6}$$

By calculating the quantum mechanical expectation value $\langle\psi_a|\mathbf{O}_A|\psi_a\rangle$ of all the states $|\psi_a\rangle$ and then computing the ensemble average of these expectation values, using the ensemble in which the states $|\psi_a\rangle$ each occur with probability p_a, we can find the expectation value of any observable $\mathbf{O}_A$. This makes us able to interpret $\boldsymbol{\rho}_A$ as describing an ensemble of quantum states $|\psi_a\rangle$, each occurring with

probability p_a. If there is only one term in (A.5) the state of system A is pure, but if there are more than one term, the state is mixed, so the system can be in any of several states. Since the diagonal form of the density matrix (A.5) follows from the properties (1)-(3) one can also say that any linear operator satisfying these conditions can be interpreted as representing a statistical ensemble of quantum states. As pointed out in §2.3.1, the ensemble interpretation is not unique; a mixed state density operator can be realized by many different ensemble preparations.

B The No-Cloning Theorem

In this section, we will prove the so-called *no-cloning theorem* – it states the simple fact that an unknown quantum state cannot be perfectly copied. This theorem was first proved by Wooters and Zurek in 1982 [44]. Our discussion will follow [35]:

The No-Cloning Theorem: *An unknown quantum state cannot be copied; there exists no unitary transformation which can clone two different, nonorthogonal states.*

Proof : Assume that we have two *non*orthogonal and distinct quantum states $|\phi\rangle$ and $|\chi\rangle$. We assume that a single unitary transformation which is capable of cloning both the states $|\phi\rangle$ and $|\chi\rangle$ exists. We must allow our unitary copy transformation to act on a Hilbert space of the form $\mathcal{H}_O \otimes \mathcal{H}_C \otimes \mathcal{H}_E$, where $\mathcal{H}_O$ is the Hilbert space of the **o**riginal quantum state, $\mathcal{H}_C$ is the Hilbert space of the **c**opy, and $\mathcal{H}_E$ is the Hilbert space of a system E which we must take into account, in order to consider the most general unitary copy transformation. If we denote the original (normalized) states of the systems C and E, as $|I\rangle_C$ and $|I\rangle_E$, the most general unitary copy transformation act as:

$$U: \begin{array}{lcl} |\chi\rangle_O|I\rangle_C|I\rangle_E & \rightarrow & |\chi\rangle_O|\chi\rangle_C|K\rangle_E \\ |\phi\rangle_O|I\rangle_C|I\rangle_E & \rightarrow & |\phi\rangle_O|\phi\rangle_C|J\rangle_E \end{array} \tag{B.1}$$

Since U preserves inner product we see that:

$$_O\langle\phi|\chi\rangle_O\,{}_C\langle I|I\rangle_C\,{}_E\langle I|I\rangle_E = {}_O\langle\phi|\chi\rangle_O = {}_O\langle\phi|\chi\rangle_O\,{}_C\langle\phi|\chi\rangle_C\,{}_E\langle J|K\rangle_E. \tag{B.2}$$

Since $|\phi\rangle_C$ and $|\chi\rangle_C$ are copies of $|\phi\rangle_O$ and $|\phi\rangle_O$ respectively, we can write ${}_O\langle\phi|\chi\rangle_O = {}_C\langle\phi|\chi\rangle_C \equiv \langle\phi|\chi\rangle$. We assumed that $|\phi\rangle_O$ and $|\chi\rangle_O$ were nonorthogonal, i.e. $\langle\phi|\chi\rangle \neq 0$, so from (B.2) we immediately see:

$$\langle\phi|\chi\rangle_E\langle J|K\rangle_E = 1 \quad \Longrightarrow \quad |\langle\phi|\chi\rangle|\,|_E\langle J|K\rangle_E| = 1 \tag{B.3}$$

The states are normalized so we can conclude that $|\langle\phi|\chi\rangle| = |_E\langle J|K\rangle_E| = 1$, i.e. $|\phi\rangle$ and $|\chi\rangle$ actually are the same state, up to an overall phase, which contradicts our assumption that the states were distinct. We have thus proved that it is not possible to construct a single unitary transformation, which is able to copy two distinct, nonorthogonal states, $|\phi\rangle_O$ and $|\chi\rangle_O$. Thus there is no transformation which is able to copy an arbitrary, unknown quantum state. □

References

[1] Quantum computation, quantum optics and spectroscopy (prof. r. blatt). World Wide Web, 2000. http://heart-c704.uibk.ac.at/quantumcomputation.html.

[2] Paul A. Benioff. Quantum mechanical hamiltonian models of discrete processes that erase their own histories: Applications to turing machines. *International Journal of Theoretical Physics*, 21(3/4):177–202, 1982.

[3] Karl Blum. *Density Matrix Theory and Applications*. Physics of Atoms and Molecules. Plenum Press, New York, 1996.

[4] S. L. Braunstein. Quantum computation. In S. L. Braunstein, editor, *Quantum Computing*, pages 1–19. Wiley-VCH, Weinheim, 1999.

[5] A. R. Calderbank and P. W. Shor. Good quantum error correcting codes exist. *Physical Review A*, 54(2):1098–105, 1996.

[6] Isaac L. Chuang. Experimental realization of a quantum algorithm. *Nature*, 393:143–6, 1998.

[7] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Physical Review Letters*, 74:4091–4, 1995.

[8] A. F. Fahmy D. G. Cory and T. F. Havel. Nuclear magnetic resonance spectroscopy: and experimentally accessible paradigm for quantum computation. In *Proc. of the 4th Workshop on Physics and Computations*, Boston, New England, 1996. Complex Systems Institute.

[9] Daniel Gottesman. *An introduction to quantum error correction*, xxx.lanl.gov/abs/quant-ph/0004272, 2000. Talk given at AMS short course on quantum computation.

[10] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439:553–8, 1992.

[11] David DiVincenzo. Quantum gates and circuits. *Proceedings of the Royal Society of London, Series A*, 454:261–76, 1998.

[12] A. Barenco et al. Elementary gates of quantum computation. *Physical Review A*, 52(5):3457–67, 1995.

[13] C. A. Sackett et al. Experimental entanglement of four particles. *Nature*, 404:256–8, 2000.

[14] Cory et al. Experimental quantum error correction. *Physical Review Letters*, 81(10):2152–5, 1998.

[15] D. Leung et al. Experimental realization of a two qubit phase dampening quantum code. *Physical Review A*, 60(3):1924–43, 1999.

[16] Lieven M.K. Vandersypen et al. Implementation of a three-quantum-bit search algorithm. *Applied Physics Letters*, 76(5), 2000.

[17] Walther Greiner *et al. Thermodynamics and Statistical Mechanics*. Springer Verlag, Heidelberg, first edition, 1994.

[18] Richard P. Feynmann. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467–88, 1982.

[19] N. A. Gershenfeld and I. L. Chuang. Bulk spin-resonance quantum computation. *Science*, 275:350–6, 1997.

[20] Nicolas Gisin. Negotiating the tricky border between quantum and classical. *Physics Today*, pages 14–5, April 1993.

[21] Lov K. Grover. Quantum computer can search arbitrarily large databases by a single querry. *Physical Review Letters*, 97:4709–4712, 1997.

[22] Jozef Gruska. *Quantum Computing.* McGraw-Hill, Cambridge, first edition, 1999.

[23] Serge Haroche and Jean Michel Raimond. Quantum computing – dream or nightmare. *Physics Today*, pages 51–2, August 1996.

[24] Peter R. Holland. Negotiating the tricky border between quantum and classical. *Physics Today*, pages 81–2, April 1993.

[25] Christian U. Jensen. Klassisk algebra. HCØ tryk, København, 1999. Lecture Notes from Matematisk Afdeling.

[26] E. Joos. Decoherence through interaction with the environment. In *Decoherence and the Apperance of a Classical World in Quantum Theory*, chapter 2, pages 35–136. Springer-Verlag, Heidelberg, 1996.

[27] Leander Kahney. Quantum leap in computing. *Wired*, pages http://www.wired.com/news/–technology/0,1282,35121,00.html, 2000.

[28] Karl Kraus. *States, Effects, and Operations (Fundamental Notions of Quantum Theory)*, volume 190 of *Lectures in Mathematical Physics at the University of Texas Austin.* Springer-Verlag, Heidelberg, 1983.

[29] Rolf Landauer. Is quantum mechanics useful? *The philosophical Transactions of The Royal Society of London, Series A*, 353:367–76, 1995.

[30] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes.* North-Holland Mathmatical Library. North-Holland, Amsterdam, 1978.

[31] Eugen Merzbacher. *Quantum Mechanics.* Wiley, New York, third edition, 1998.

[32] Klaus Mølmer. Monte carlo wave functions in quantum optics. *Quantum Semiclassical Optics*, 8:49–72, 1996.

[33] J. V. Neumann. *Matematische Grundlagen der Quantenmechanik.* Springer-Verlag, Heidelberg, 1996.

[34] Apoorva Patel. What is quantum computation? In *Probing Fundamental Problems with Lasers and Cold Atoms*, India, January 1999. IIA, Bangalore. Invited talk presented at the Indo-French workshop.

[35] John Preskill. Lecture notes for physics 229 – quantum information and computation. World Wide Web, http://www.theory.caltech.edu/-people/preskill/ph229/.

[36] John Preskill. Fault-tolerant quantum computation. In H.-K. Lo S. Popescu and T. P. Spiller, editors, *Introduction to Quantum Computation.* or preprint; xxx.lanl.gov/abs/quant-ph/9712048, 1997.

[37] John Preskill. Battling decoherence: The fault tolerant quantum computer. *Physics Today*, 52(6):24–30, 1999.

[38] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proc. 35th Annual Symp. on Foundations of Computer Science*, Santa Fe, 1994. IEEE Computer Society Press.

[39] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 54:R2493–6, 1994.

[40] Andrew M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77:793–7, 1996.

[41] Andrew M. Steane. The ion trap information processor. *Applied Physics B*, 64:623–42, 1997.

[42] Andrew M. Steane. Quantum computing. *Reports on Progress in Physics*, 61:117–73, 1998.

[43] W. G. Unruh. Maintaining coherence in quantum computers. *Physical Review A*, 51:992–7, 1995.

[44] W.K. Wooters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–3, 1992.

[45] W. Zurek. Pointer basis of quantum apperatus: Into what mixture does the wave packet collapse. *Physical Review D*, 24(6):1516–25, 1981.

[46] Wojciech H. Zurek. Decoherence and the transition from quantum to classical. *Physics Today*, October 1991.