December 17, 2000

Fighting Decoherence: Quantum Error-Correcting Codes

Sebastian Buhai

Utrecht University College
Postbus 81-081, Poscode 3508 BB
Utrecht, The Netherlands
Email: sbuhai@ucu.uu.nl

Abstract.

The hereby paper presents an overview of the current interpretation of decoherence in quantum theory, at the same time firmly stating that decoherence can be successfully fought against by means of the quantum error-correcting codes developed in the recent years. While decoherence itself is but a natural transition from quantum to classical, explaining the so disputed quantum origins of the classical world, its effects have to be combated or severely diminished if revolutionary techniques such as quantum communication or quantum computation are to be ever implemented. We will argue and try to prove by reference to existing leading research papers that quantum error-correction codes are a viable solution for the decoherence problem in particular settings. As a clear-cut example we tackle the five-qubit quantum circuit described by Shor, DiVincenzo and Terhal. Full generalization is in our view a simple problem of time as the theory describing it exists already and is continuously revised by top scientists. In this sense the general QECC framework developed by Knill and Laflamme is thoroughly analyzed and commented upon.

1. **Scene-Setting: Decoherence as Transition Concept between Quantum and Classical**

If we were to consider decoherence in its full generality[1], we would concisely define it as the phenomenon by which quantum mechanical systems behave as though they are described by classical probability theory *[2]*. In other words a given quantum mechanical system exhibits decoherence when all typical features of quantum mechanical probability are suppressed. In the remaining of this section we will try to clarify and detail this definition.

It seems to us nowadays that the quantum origin of the classical world was extremely difficult to imagine for the forefathers of quantum theory. Thus Bohr, in his formulation of

[1] Recent papers coin two distinct types of decoherence: the "environment induced decoherence" (or the very popular type of decoherence, usually referred to in the literature, concerning the "classicalisation" of a quantum system as a process that takes place in time), on the one hand, and the decoherence referring to the situation where a coarse-grained description of the system can be given in terms of classical probability theory, on the other hand. The former category of decoherence is considered only a particular case of the more general latter type. Thus by "full generality" we make a direct reference to the second type.

the Copenhagen theory, was willing to postulate the independent existence of the two worlds, while de Broglie or even Einstein to a lesser extent, were apparently willing to completely give up the quantum theory and search for something with more fundamental classical underpinnings *[7]*. We are of course aware now that the source of these problems was the quantum principle of superposition that exponentially expands the set of the available states to all conceivable superposition states. Hence, to cite maybe the most famous example, coherent superpositions of dead and alive cats have, in the light of the quantum theory, the same right to exist as either of the two classical alternatives. Within the Hilbert space describing a given state classically "legal" states are exceptional: the set of all states in the Hilbert space is enormous as compared with the size of the set of states where one finds classical systems. As an ironically enough consequence, it is a fact of life that classical objects are only found in a very small subset of all possible (and in principle, allowed) states. So one has to explain this apparent "super-selection" or "einselection" *[6]* rule that prevents the existence of most states in the Hilbert space of certain physical systems. It is decoherence that accounts for this experimental fact of life.

Decoherence is originated in the interaction between the system and its environment. In other words an entanglement between the state of the quantum system in question and the environmental degrees of freedom occurs *[3]*. As a consequence, the quantum system will evolve from a pure quantum state to a mixture of quantum states with no set phase difference between them. The problem is simply inherent to all quantum systems, as no technique has been so far developed in order to entirely isolate defined systems from their environment. The single truly isolated system is the whole macroscopic Universe itself, as the highest possible enlarged system to contain the information[2]. Otherwise, the isolation is especially hard or impossible to conceive when referring to macroscopic dimensions within our Universe: an environmental record-keeping will enter into function as soon as we try to measure a certain property of such an object[3]. Under a variety of conditions, particularly easy to satisfy for macroscopic objects, decoherence leads to the einselection of a small subset of quasi-classical states from within the enormous Hilbert space. Classicality is thus an emergent property induced in the system by its interaction with the environment. Arbitrary superpositions are immediately dismissed and a preferred set of states emerges; these preferred states are the classical states. They correspond to the definite readings of the apparatus pointer in quantum measurements and to the points in the phase space of a classical dynamical system.

---

[2] The standard strategy to ensure isolation was to enlarge a system, that is to include the immediate environment

[3] One of the traditional examples used by quantum physics theorists in underlying the environmental record-keeping is the model of the "billiard ball". Suppose we want to know the position of a billiard ball (for all practical purposes, this can be any macroscopic object) to within some degree of precision, in the quantum universe. In formulating our question we ignore the quantum state of everything else in the cosmos. Subject to a certain condition we will use, we can use the possible positions of the billiard ball to partition the set of possible states of everything else into equivalence classes with respect to each of which the billiard ball is in a different position. The proviso enabling this partitioning is exactly that there must be a good degree of correlation between the state of the billiard ball and the state of everything else. That is, given the cosmos in a pure quantum state, we cannot separate off the billiard ball and be left with a billiard ball in a pure state and a rest-of-the cosmos in a pure state. Each subsystem is a mixed state and there are non-separable correlations between the two. In other words, the environment (the rest of the cosmos) contains information about the state of the billiard ball—just as the billiard ball contains information about its environment.

2. **Fighting against Decoherence: QECC**

2.1. **Decoherence, an Obstacle to Quantum Computation and Communication**

Within the past few years, quantum computation and communication have undergone a dramatic evolution. From being subjects of primarily and solely academic interest, they have become fields having an extreme potential for revolutionizing computer science and cryptography, as well as an impact on issues of national security, and even potentially commercial applications, to mention only a few of the recent practical functions *[1]*. This has resulted not only from the development of new algorithms such as quantum factoring, but also as a consequence of experimental work on implementations of individual quantum gates and of quantum cryptography. Unfortunately, the quantum states required to carry out a computation are more than sensitive to the imperfections of the hardware, and above all, to the decoherence caused by the inherent interaction with the environment[4].

It is by now clear that decoherence is a process having a crucial role in the quantum-to-classical transition. We find very interesting to pinpoint and discuss this transition; nonetheless in most of the cases physicists are interested in understanding the specific causes of decoherence just because we want to get rid of it. Decoherence is responsible for washing out the quantum interference effects we would very much want to see as a signal in some experiments *[5], [6]*. In particular, this is the type of situation that we are facing in quantum computation and in the physics of quantum information on a more generalized scale. A quantum computer is nothing but a gigantic interferometer whose wave function explores an exponential number of classical computations simultaneously: while conventional computers store data as bits with a value of 0 or 1, a quantum computer stores information in two-level quantum states, such as the spin of a proton. The crucial point is that these quantum states, known as qubits, can become "entangled" with each other, so that N qubits can exist in 2^N different states *[3]*. It is therefore more than necessary that coherence between branches of the computer wave function is maintained, as the existence of quantum interference between these branches is the primary reason why these computers can outperform their classical counterparts.

In few words, decoherence can cause a quantum computer to lose two of its key properties: entanglement between the qubits and interference phenomena. Specific examples describing both these implications as well as physical causes of decoherence for the two most popular types of quantum computers[5] are successfully and in detail discussed by David DiVincenzo and Barbara Terhal in *[3], pages 53-54*. Considering a reference to their work as sufficient for our purpose and also taking into consideration the limited amount of space and time for this paper, we will not insist more on these specific issues, nonetheless acknowledging their overwhelming importance. The conclusion of the short overview herein is that decoherence is a major problem within quantum computation and quantum information in general, therefore

[4] See the first Section for a more detailed discussion on the "environmental record-keeping" in the case of any quantum system

[5] The most popular quantum systems considered as potential quantum computers are the quantum computer composed of trapped ions (originally proposed in 1995 by I. Cirac and P. Zoller at the University of Innsbruck in Austria) and the quantum computer based on nuclear magnetic resonance, NMR, from aqueous solutions of organic molecules (originally proposed by I. Chuang from Stanford and N. Gershenfeld and D. Cory from MIT)

any measures aimed at reducing or eliminating decoherence effects are ineluctable for future progress in these areas.

2.2 **Can We Correct Decoherence Induced Errors?**

An obvious way of try to prevent decoherence from damaging quantum states should be by now straightforward: reducing the strength of the coupling between the system and its environment. Nonetheless, it is never possible to reduce this coupling to zero and eliminate decoherence in this way as it has been argued along the previous sections of this paper. Unless noise is totally eliminated, no hope in this sense. Hence, a radically different approach is required.

To ensure that the fragility of quantum states does not destroy our ability to extract the desired interference pattern requires techniques for correcting errors. The general idea would be to find some error-correcting procedure so that in the eventuality of an error corrupting the encoded quantum state, the initial quantum state is reconstructed. But before going into deeper details, one dilemma should be settled: does error correction exist at all for quantum states? Is this a reasonable issue to even start with?

Many researchers doubted that error correction could at all exist. Most objections centered on two straightforward arguments. Firstly, decoherence would irreversibly destroy the information contained in the quantum state, so the original state could not be recovered. Secondly, the quantum state is analogue—generally specified by a set of complex numbers—which suggests that the errors caused by decoherence come in an almost infinite variety. At least some of these errors would simply rotate the system into a different quantum state and so they could not be detected as errors *[3]*. Moreover and connected to the previously stated arguments, it was generally believed that to perform an error-correction step, knowledge of the exact state of the computer is required. Such knowledge would unavoidably destroy the quantum mechanical properties of the state *[1], [7]*. Clearly all these arguments had their point and it seemed for a while that is useless to even think about quantum error-correction. Luckily enough, things evolved positively.

Let us begin by noting that some of the present papers *[1]* rightfully draw an interesting parallel between the state of the art the quantum computation today and that of classical computers in the 40's. At that time it was commonly believed that classical computers could not be useful because errors in the computer itself would render the result untrustworthy. These doubts disappeared after the discovery of the powerful error-correction techniques for classical computers. In our era, quantum error-correcting codes, discovered by Shor and Steane in 1995, prove similar objections, pertaining to the use of quantum computers this time, fundamentally wrong.

The first objection argument remains valid if the rate of decoherence is high, but that is true of any error-correction scheme: it is overwhelmed if the errors occur faster than they can be corrected. It is known now that errors can be corrected as they occur provided that the error rate is below a certain threshold, currently estimated at about 10^{-5} per qubit per clock cycle *[3]*. It is further assumed that errors occur independently on individual qubits, perhaps the most important assumption, and that they appear uniformly throughout the quantum computer. Now, experience so far acknowledges practical the existence of systems with such properties, therefore this first argument cannot be regarded as a de facto objection, although it is the strongest counter-point.

The second argument is refuted by the following discovery: the continuum of all possible errors can change the quantum state in one of a total of three possible ways. Thus the quantum error correction is an analogue, but a digital process *[3]*. Once one of these three errors has been detected, it can be easily undone by one of the several error-correcting transformations. For the record, let us illustrate the action of the three error operations (and the identical operation) on a single qubit in the state $\alpha|0> +\beta|1>$:

I (identical operation): $\alpha|0> +\beta|1> \rightarrow \alpha|0> +\beta|1>$
X (bit flip operation): $\alpha|0> +\beta|1> \rightarrow \alpha|1> +\beta|0>$
Z (phase flip operation): $\alpha|0> +\beta|1> \rightarrow \alpha|0>-\beta|1>$
Y (bit/phase flip operation): $\alpha|0> +\beta|1>\rightarrow \alpha|1> -\beta|0>$,
where α and β are complex numbers, and |0> and |1> are the two levels of a single qubit.

It has been shown that all other errors can be decomposed in these "canonical error operations". In other words, an entangled state of a number of qubits (the quantum codeword, as the next section will make clear), where $|c_0>$ and $|c_1>$ are two carefully chosen entangled states of the encoding qubits, can still be written as $\alpha|c_0> +\beta|c_1>$ in its original form[6]. Implicitly all operation errors will operate as in the case of the single qubit.

As the last objection argument is concerned, Peter Shor has shown that in a restricted model of errors (the existence of which has been proved in the preceding paragraph), it is possible to restore a state using only partial knowledge of the state of the quantum computer. Hence we are not in the situation to apply Heisenberg's principle and thus to destroy the quantum states because we have the knowledge of the entire system. This is certainly an innovation in quantum theory and can be used within the whole field, not only in reducing decoherence effects. The whole Heisenberg's principle can apparently be "skipped" if a required operation is possible by using only partial knowledge of the quantum state.

All these positive ideas have opened the path to a general theory of quantum error correction. We will aim at describing the outlines of this theory so far and its implications in the following sections of this paper.

2.3 **General Framework for the Quantum Error-Correction**

As also dwelled upon in the previous sections of work, coherent quantum states have a particular importance in quantum communication and quantum computation. Both situations involve the manipulation of states by unitary operations where some desired information is eventually extracted from parts of the state by measurement. There is a small difference between the two objectives; quantum communication involves multiple parties with limited communication capabilities and focuses more on the transmission of states over potentially

[6] A simple mathematical induction should suffice as a solid proof in the general case. For the case of the three or five qubit words this is straightforward.

noisy channels, while quantum computation involves only one party and focuses on the unitary transformations involved in achieving the final state. However, in both of the cases the loss of coherence results in a reduction of the probability of getting the correct answer after completion of the required operations. We need to focus on preserving a coherent state subject to unwanted interactions in a quantum memory or channel *[1]*.

Now, in classical communication and computer memories, the corrupted information can be introduced by introducing redundancy, for example by copying all or a part of the information to be preserved[7]. Unfortunately, such a simple redundancy scheme is incompatible with quantum states, primarily because the no-cloning theorem *[1], [3], [4], [5]* prevents the duplication of quantum information. Nevertheless, it has been recently found out that it is possible to correct a state against certain known errors by spreading the information over many qubits through an encoding. The goal is to find an encoding which behaves in a specific way under evolution by the interaction "superoperator" *[1], [5]*. The behavior must be such that it permits recovery of the original state.

Let us consider the simplest non-trivial case of encoding a single qubit. The general state to be protected is of the form: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The idea is to map $|\psi\rangle$ into a higher dimensional Hilbert space:

$$(\alpha|0\rangle + \beta|1\rangle)|000\ldots\rangle \rightarrow \alpha|0_L\rangle + \beta|1_L\rangle \quad [1]$$

The equation above defines the code. $|0_L\rangle$ and $|1_L\rangle$ are called the "logical zero" and the "logical one" of the qubit which we want to preserve, respectively. The new state in this equation should be such that any error induced by an incorrect functioning of the computer maps it into one of a family of two-dimensional subspaces that preserve the relative coherence of the quantum information. A measurement is then performed which projects the state into one of these subspaces. The original state can be recovered by a unitary transformation which depends on which of these subspaces has been observed. All these issues have been converted into a fascinating mathematical theory in recent papers. Maybe one the best examples in this sense is the work of the researchers from the Los Alamos National Laboratory, Emanuel Knill and Raymond Laflamme. In *[1]* they describe a general theory of quantum error-correcting codes in an excellent manner. In what follows we will refer to some of their findings and add our comments when considered necessary.

First of all, assuming that the initial state is $|\psi_i\rangle$, the interaction with the environment will leave the system (let this be a quantum computer, for instance) in the reduced density matrix $\rho_f = \$ (|\psi_i\rangle)$, where \$ is the superoperator associated with the interaction (the notation herein is the original notation used in the Knill & Laflamme paper). Further, in the case where the environment is not initially entangled with the system ρ_f, we have:

$$\rho_f = \sum_a A_a \rho_i A_a^\dagger$$

A choice of operators A_a can be determined from an orthonormal basis $|\mu_a\rangle$ of the environment, the environment's initial state $|e\rangle$ and the evolution operator U of the whole

[7] The reader is of course aware of the backup information created every time an important operation (such as installing a new operating system) is performed. Ironically, redundancy plays here a positive role, while in programming as such it should be avoided as much as possible. That is, intrinsic redundancy is undesired, while redundancy in preserving the achieved final "program" is very necessary.

system: $A_a = <\mu_a|U|e>$. We can immediately see that $\sum_a A_a^\dagger A_a = I$. The A_a are linear operators of the Hilbert space of the system and describe the effect of the environment. They are called interaction operators. Any family of operators A_a that satisfy the identity above define a superoperator.

We made this entire rather cumbersome introduction in order to facilitate the understanding of the necessary and sufficient conditions for the recovery of the state $|\psi_i>$. These conditions are:

$$<0_L|\, A_a^\dagger A_b|1_L> = 0,$$
$$<0_L|\, A_a^\dagger A_b|0_L> = <1_L|\, A_a^\dagger A_b|1_L>$$

While the first condition states that the logical zero and one must go to orthogonal states under any error, the second one implies that the length and inner products of the projections of the corrupted logical zero and one should be the same. These results are also found in [3] by DiVincenzo and Terhal: the codewords have to be still distinguishable after the error has occurred (orthogonality) and the codewords should be such that the most significant error map the encoded state outside the space spanned by the two qubit states (or codeword states) in a way independent of α andβ (partially in the requirement that the length and inner products of the different projections should be the same).

We need to precise that for realistic quantum computers only a subset of possible errors can be corrected. An appropriate measure of the quality of a recovered code is the fidelity, defined as the overlap between the final state ρ_f of a system ρ and the original state $|\psi_i>$. If the combined superoperator consisting of an interaction with the environment followed by a recovery operation is given by A= $\{A_0,\ldots.\}$, as we assumed in this section, then the fidelity is defined as:

$$F\,(|\psi_i>,A) = <\psi_i|\rho_f|\psi_I> = \sum_a <\psi_i\,|A_a|\psi_i>\ <\psi_i\,|A_a^\dagger|\psi_i>.$$

It gives the probability that the final state would pass a test checking whether it agrees with the initial state. As Knill and Laflamme perfectly reason, as we are thinking of encoding arbitrary states, we do not know in advance the state that will be used *[1]*. Thus we need to use the minimum fidelity which is obviously the worst case fidelity:

$$F_{min} = \min_{|\psi>} <\psi|\rho_f|\psi>$$

The best quantum code will definitely maximize F_{min}.

But let us see the exact form that the decoherence takes if we consider all the notations above:

$$<\psi_i| = \alpha|0> + \beta|1> \rightarrow \rho \begin{pmatrix} \alpha a^* & \alpha\beta^* e^{-\gamma} \\ \alpha^*\beta e^{-\gamma} & \beta\beta^* \end{pmatrix},$$

where $e^{-\gamma}$ (γ>=0) parameterizes the amount of decoherence. Moving further, decoherence can be understood in terms of the following interaction with the environment

$|e>|0> \rightarrow |e_0>|0>$ and
$|e>|1> \rightarrow |e_1>|1>$,

with $<e_0|e_1> = e^{-\gamma}$. We notice how much the Dirac notation simplifies the equations. Using as environment basis $|\mu_0> = |e_0>|$ and $|\mu_1> = |e_1>| - e^{-\gamma}\,|e_0>)/\sqrt{1-e^{-2\gamma}}$ we obtain the interaction operators

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\gamma} \end{pmatrix} \text{ and } A_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{1-e^{-2\gamma}} \end{pmatrix}.$$

Now, for a single qubit which is corrupted by decoherence, the minimum fidelity is given by

$$F = \frac{1+e^{-\gamma}}{2} \sim 1-\frac{\gamma}{2}+\dots ,$$

with the last approximation valid for small γ.
It is important to realize that the quantum-error correction code in this shape corrects perfectly only if at most one error occurs *[1]*. In this respect the fidelity just approximated plays the greatest role. As long as the decoherence is small (that is the same as small γ), the probability of having two or more errors will be much smaller than that of having one error. Therefore the framework for the further performing of the quantum error-correction operations (requiring perfect fidelity) as such, is set.

2.4. **Quantum Error-Correcting Codes Implemented**

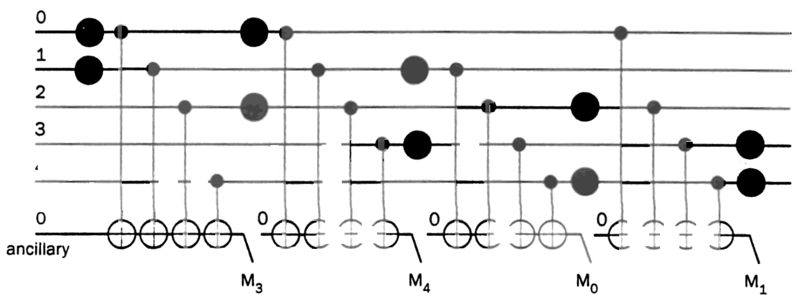
While Knill and Laflamme present a full abstract theory describing the fundamentals of the QECC[8] and obtain the recovery operations after a fascinating chain of deductions and de facto calculus *[1]*, we will limit ourselves to describing the implementation of these quantum-error correcting codes in practice.

The past years have witnessed an astonishing rate of progress in the development of error-correction schemes for quantum memory and quantum computation. The discovery that a qubit, when suitably encoded in a block of qubits, can withstand a substantial degree of interaction with the environment without degradation of its quantum state has been followed by many other contributions which have identified many new coding schemes *[4]* .

The first code developed by Peter Shor used nine qubits to encode a single qubit; this coded qubit could be restored when any one of the nine qubits had experienced some arbitrary disturbance. After this scheme was introduced, everybody came to understand the precise requirements for quantum error-correcting codes. Out of the many “entangled codewords” that are in use today, one of the most popular is the five-qubit code discovered by Raymond Laflamme at Los Alamos and independently by Charles Bennett at IBM. This code is currently considered the most economical encoding of a single qubit that can fully correct an arbitrary error on any of the code’s qubits.

[8] This paper will make use of the acronym QECC as standard abbreviation within quantum theory denoting Quantum Error-Correcting Codes

- Figure 1 – *([3], page 55)*



M_3	M_4	M_0	M_1	P
+1	+1	+1	+1	I
+1	+1	+1	-1	Z_4
+1	+1	-1	+1	X_1
+1	+1	-1	-1	Z_3
+1	-1	+1	+1	X_3
+1	-1	+1	-1	X_0
+1	-1	-1	+1	Z_2
+1	-1	-1	-1	Y_3
-1	+1	+1	+1	Z_0
-1	+1	+1	-1	X_2
-1	+1	-1	+1	X_4
-1	+1	-1	-1	Y_4
-1	-1	+1	+1	Z_1
-1	-1	+1	-1	Y_0
-1	-1	-1	+1	Y_1
-1	-1	-1	-1	Y_2

One possible error-correcting circuit for the five-qubit code consists of four stages. A single qubit is encoded as an entangled state of five qubits, which travel through the four stages of the circuit from left to right. At each stage, the coded qubit is acted on by a sequence of two logic operations: the one-bit Hadamard transform (green circle) and the two-bit controlled-NOT gate. In this last operation, one of the input qubits (marked with the blue dot) acts as the control qubit while the other qubit (marked with a crossed circle) is the target qubit. A sixth ancillary qubit, set to |0⟩ at the beginning of each stage, is measured at the end of each stage. The outcome of the M_3, M_4, M_0 and M_2 measurements can be +1 or −1, and the pattern of +1s and −1s indicates which error operators have acted on the coded qubit (see table).

We have included above a figure of a quantum circuit consisting of four stages, as represented in *[3]*. When the qubit enters the circuit, it is encoded as one particular entangled states of the five qubits, $\alpha|c_0> +\beta|c_1>$. There are many possibilities of choosing the basis states $|c_0>$ and $|c_1>$, provided that the conditions discussed in the previous sections are fully met (orthogonality and independence of parameters). Herein it was chosen that $|c_0>$ is composed of states with an odd number of zeros in the codewords, while $|c_1>$ has states with an odd number of 1s *[3], [4]*. To write the codewords completely, we have:

$|c_0>$ = |00000> + |11000> + |01100> + |00110> + |00011> + |10001> - |10100> - |01010> - |00101> - |10010> - |01001> - |11110> - |01111> - |10111> - |11011> - |11101>

and

$|c_1>$ = |11111> + |00111> + |10011> + |11001> + |11100> + |01110> - |01011> - |10101> - |11010> - |01101> - |10110> - |00001> - |10000> - |01000> - |00100> - |00010>[9]

Coming back to the description on the figure, a sequence of quantum-gate operations act on the encoded qubit passing through each state of the circuit. For the sake of illustration, only 2 operations are used on this circuit: the one-bit Hadamard operation and the two-qubit controlled-NOT gate[10]. The 4 stages of the circuit conclude with a measurement M_3, M_4, M_0 and M_1 on a sixth ancillary qubit, set to |0> at the beginning of each stage (see Figure 1). The idea is very ingenious as this ancillary qubit is provided with information about the state of disrepair of the coded qubit. Each of the 5 qubits can be acted on by one of the three canonical error discussed in section 2.2, hence a total of 15 possible errors can occur. They are all embodied in the table next to the figure above. The outcomes of the measurement can be as one can follow on the table, –1 or 1, depending on which of the errors actually occurs. We can identify from the values of the measurement (this 4 values are the so-called error syndrome) which error occurred. For instance, to use a different example than the one used by the authors of the quoted paper, if the 4 measurements yield –1, -1, -1, +1, we know that

[9] Another class of very popular 5-qubit codes is the Laflamme class where the one bit rotation is applied to qubits 0 and 1 in order to obtain the final representation. As long as one starts with a particular symmetric presentation for |0> and |1>, respectively, and takes care of the conditions, infinitely many representations can be obtained (see *[4]*, pages 3260-3262 for details)

[10] The one-bit Hadamard operation transforms the qubits as follows: |0>→$2^{-1/2}$(|0> + |1>) and |1>→$2^{-1/2}$(|0> - |1>). The two-qubit controlled-NOT gate flips the lower target bit if the upper control bit is 1: |00>→|00>, |01>→|01>, |10>→|11>, |11>→|10>. These are elementary operations used here for the sole purpose of didactical exemplification

qubit number 1 has been disturbed and that the decoherence acting on it was a bit/phase flip error. Obviously the error correction is very simple; using a final quantum gate, the state of bit 1 is phased/flipped back to its correct state.

It has been rigorously proven in *[4]* that this five-qubit code error correction circuit is fault-tolerant, that is any error that occurs during the operations can be repaired at a later stage. However, as explicitly pointed out in *[3]*, this scheme can only tolerate an error on one of the qubits. For extensions of this result work is currently undergone.

3. **Possible Conclusions**

We have tried in this paper to present an overview of the present scientific conception of decoherence as transition concept between the quantum and classical domains. Whether physically or philosophically justified, decoherence certainly plays a leading role in explaining the quantum origins of the classical and the quantum world. On the other hand we have pointed out that decoherence is mainly investigated for finding a way to combat its effects in order to practically implement quantum communication or quantum computation systems. The results in this sense can be considered amazing and future optimism seems to dominate within this particular area of the quantum theory. QECC techniques have reached high development stages making us think of practical applicability somewhere in the very near future. At the same time however, we have shown that only particular errors can be so far completely corrected and all in the framework of perfect fidelity. The study of imperfect reality codes is far from completed. Both the sources of introduced error, and its propagation when recovery is attempted many times require further study. But, to end in an optimistic manner, we have shown that the theory is there and that it works perfectly for particular systems. Hence there is no reason why generalization and further improvement should be insurmountable tasks.

References

[1] E. Knill & R. Laflamme, A Theory of Quantum Error-Correcting Codes, http://qso.lanl.gov/qc/theory.html (set to appear in Physical Review A)

[2] C. Anastopoulos, Frequently Asked Questions about Decoherence, arXiv: quant-ph/0011123, November 20, 2000

[3] D. DiVincenzo & B. Terhal, Decoherence: the obstacle to quantum computation, Physics World, March 1998

[4] D. DiVincenzo & P. Shor, Fault-Tolerant Error Correction with Efficient Quantum Codes, Physical Review. Letters volume 77, p. 3260

[5] H. Stapp, The importance of quantum decoherence in brain processes, arXiv: quant-ph/0010029, October 6, 2000

[6] J.P. Paz & W. H. Zurek, Environment-induced decoherence and the transition from quantum to classical, arXiv: quant-ph/0010011, October 2, 2000

[7] B.H. Bransden & C.J. Joachain, Quantum mechanics (Second Edition), Pearson Education, Essex, England, 2000