

Quantum Computation: Towards the Construction of a ‘Between Quantum and Classical Computer’

Diederik Aerts and Bart D’Hooghe

Center Leo Apostel for Interdisciplinary Studies (CLEA)

Foundations of the Exact Science (FUND)

Department of Mathematics, Vrije Universiteit Brussel

1160 Brussels, Belgium

E-Mails: diraerts@vub.ac.be, bdhooghe@vub.ac.be

Abstract

Using the ‘between quantum and classical’ models that have been constructed explicitly within the hidden measurement approach of quantum mechanics we investigate the possibility to construct a ‘between quantum and classical’ computer. In this view, the pure quantum computer and the classical Turing machine can be seen as two special cases of our general computer. We have shown in earlier research that the intermediate ‘between quantum and classical’ systems cannot be described within standard quantum theory. We argue that the general categorical approach of state property systems might provide a unified framework for the study of these ‘between quantum and classical’ models, and hence also for the study of classical and quantum computers as special cases.

1 Introduction

The theory of quantum computation (*i.e.*, calculations performed on a computer which has a quantum system as register [1, 2]) has gained importance after the discovery of quantum algorithms which allow to solve problems much faster than with the known (classical) algorithms written for a classical, digital computer. The most famous quantum algorithm is a factorization algorithm by P. Shor [3, 4] which allows to factorize integers in a number of steps polynomial in the size of the input. This would imply that if quantum computers could be built in practice, then the most important of modern cryptography systems could be broken easily, since they are based on the assumption that polynomial factorization algorithms can not be found for classical, digital computers [4, 5]. From a more theoretical and philosophical point of view quantum computing is also interesting since it contributes to the study of fundamental aspects of physics and information science: *e.g.* by the definition of a universal quantum Turing-machine [6, 7]; *e.g.* by putting the many world interpretation of quantum mechanics into a new perspective [7, 8].

In the first section we give a brief overview of how a quantum computer works. The quantum analogue of a classical bit is a so-called qubit, which has very different properties in comparison with a classical bit since in a sense it can be in any superposition of the two classical bit-values. The register of the quantum computer is given by a system of N spin- $\frac{1}{2}$ particles, such that the state of each qubit is encoded with the state of the corresponding spin- $\frac{1}{2}$ particle. Therefore, to study a quantum computer is to study its register, *i.e.*, study a system of N spin- $\frac{1}{2}$ particles.

In the second section we discuss the hidden measurement approach of quantum mechanics, which assumes that random fluctuations in the measurement context lead to a probability distribution over the set of outcomes, which coincides with the quantum probabilities if the random fluctuations are uniformly distributed. Not only is it possible to show that for any quantum entity one can define a hidden measurement model, also explicit hidden measurement models for quantum entities have been put forward. One of these models is a macroscopical model representing the spin properties of a spin- $\frac{1}{2}$ particle, such that each spin state is represented by a point on the unit sphere in three dimensions. Using this model, one can represent (the state of) a qubit by a point on the three-dimensional unit sphere. Two sphere models representing a spin- $\frac{1}{2}$ entity were coupled to give rise to a model that describes the situation of two coupled spin- $\frac{1}{2}$ entities by introducing so-called correlations of the first and of the second kind, and the model was realized by the concrete coupling of two ϵ -models by means of a rigid rod connecting the states of the two spins [9]. It was shown that this type of model can be generalized for the case of N coupled spin- $\frac{1}{2}$ particles [10, 11]. Later [12, 13] a new parameter ρ was introduced that parametrizes the coupling, in the sense that the model can evolve in a continuous way from ‘rigid’ coupling, making it a model for the quantum coupling of spin- $\frac{1}{2}$, hence the quantum coupling of qubits ($\rho = 1$), to ‘no-coupling’, making it a model for ‘separated’ spin- $\frac{1}{2}$ ($\rho = 0$). For the meaning of ‘separated’ and the problematic involved we refer to [14, 15]. This makes it possible to represent a quantum register by a hidden measurement model, using the parameters ϵ and ρ , and the models that have been constructed.

In the hidden measurement approach quantum mechanical probabilities arise due to a lack of knowledge about the precise interaction between the measurement equipment and the system. This lack of knowledge about the measurement interaction is described by the parameter ϵ , that as a consequence controls this uncertainty. The introduction of ϵ makes it possible to describe a continuous transition from the (quantum) sphere model towards a (classical) deterministic spin state particle [16, 17]. The parameter ρ makes it possible to describe a continuous transition from a (quantum) coupling to a completely decoupled situation, which means that both parameters allow a continuous transition from a quantum register to a classical register of N bits. The structure of the intermediate models has been studied in detail for the case of varying ϵ , and it can be proved that the model is neither quantum nor classical, since two axioms of the representation theorem of Piron [18] for quantum and classical physical systems are violated [19, 20, 16]. It has also been proven that the completely uncoupled situation cannot be described by standard quantum mechanics, because the same two axioms of traditional quantum axiomatics are not satisfied (see [14, 15] for an overview). In forthcoming work we will study the structure of the models from an axiomatic point of view for intermediate values of ρ .

What is certain however is that one has to use a formalism more general than the quantum formalism to describe such entities and such transitions. Following the view that computation can be regarded as the evolution of a physical system – such that the initial state of the register corresponds with the input of the computation and the final state yields the output of the computation process – we can study the process of computation as the evolution of the state of the register during the computational process. We have developed a general approach where the ‘between quantum and classical’ models can be studied and characterized. The basic structure is the one of a state property system, where the physical entity is described by means of its states and properties [21, 22]. Evolution can be described by means of the standard procedure developed in theoretical physics: *i.e.* the one parameter group of time translations is represented in the group of automorphisms of the structure. This will give rise to unitary evolution in the special case of a pure quantum computer, and allows the description of evolution for the ‘between quantum and classical’ computers.

2 Quantum Computation: Main Concepts

In this section we give a quick overview of how a quantum computer works (following the presentation given in the paper by Pykacz et al. [23]) and how the quantum computational process can be interpreted as the free evolution of a physical system.

2.1 Qubits Versus Classical Bits

Let us first consider a classical computer from a more physical point of view. A classical bit of information can physically be represented with any bi-stable classical physical system, such that the two possible states represent the binary digits 0 and 1. The register of the computer consists of a number N of such bi-stable physical systems. To store the input data in the register requires the preparation of the register in a particular state. A classical N -bit register can be in 2^N different states. Any such state can be denoted by $|i\rangle$ where i is a number represented by a binary word of length N . During the calculation the state of the register follows a prescribed evolution induced by means of the processor, *i.e.*, the processor forces the necessary state evolution in order to obtain a final state containing the output of the computational process.

Contrary to a classical physical system, a quantum bi-stable system (*e.g.*, the spin state of a spin- $\frac{1}{2}$ particle) can be in a superposition state of the eigenstates for the 0 and 1 digits. Therefore, each spin- $\frac{1}{2}$ particle representing a bit in the register of a quantum computer is in general in a superposition state which can be written as a linear combination of the states $|0\rangle$ and $|1\rangle$ that encode 0 and 1 with complex coefficients such that the sum of their squared moduli is 1:

$$|s\rangle = c_0|0\rangle + c_1|1\rangle, \quad c_0, c_1 \in \mathbb{C}, \quad |c_0|^2 + |c_1|^2 = 1. \quad (1)$$

Although any measurement of the state $|s\rangle$ necessarily yields either 0 (with probability $|c_0|^2$) or 1 (with probability $|c_1|^2$), according to standard quantum mechanics $|s\rangle$ cannot be interpreted as an unknown state that represents either 0 or 1 with respective probabilities $|c_0|^2$ and $|c_1|^2$ (see the many no-go theorems for non-contextual hidden variable theories, *e.g.* [24, 25]. Because the coefficients c_0 and c_1 are complex, not real numbers, it does not represent a statistical mixture of $|0\rangle$ and $|1\rangle$. Neither it can be interpreted as representing some value “between” 0 and 1. It is an entirely new entity having no counterpart in classical physics and the unit of information it carries is customarily called qubit (= quantum bit).

2.2 A Conbit: A Contextual Bit

That a qubit is more general than a classical bit can be seen as follows. A classical bit is represented by a classical bi-stable physical device, *e.g.*, positive or negative charge, positive or negative voltage, light on or off. Therefore, no matter how one would measure the value of the bit, one would still get the same outcome, *i.e.*, a positive voltage or a negative one etc. For a qubit, the state of the entity representing a qubit can be in a superposition state, which means that for a measurement with the predefined eigenstates $|0\rangle$ and $|1\rangle$, one will only obtain a probabilistic outcome. However, if one would make a measurement such that the superposition state of the register is an eigenstate for the experiment, then one will get the outcome corresponding with this superposition state with certainty. Let us clarify this by the example of a qubit encoded in the spin state of a spin- $\frac{1}{2}$ particle. Let us consider the case where the eigenstates defining the bit value 0, resp. 1, are the states

$$|0\rangle_z = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |1\rangle_z = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

i.e., the eigenstates of the spin down, resp. spin up outcome for a spin measurement along the z -direction (*i.e.*, the Stern-Gerlach apparatus used to measure the spin of the spin- $\frac{1}{2}$ particle is placed along the z -direction). Let us consider the case where the particle is in a superposition state such that its state is given by $s = \frac{1}{\sqrt{2}} (|0\rangle_z - |1\rangle_z) = |0\rangle_x$ then a measurement along the direction x will yield with certainty the outcome corresponding with the $|0\rangle_x$ state, *i.e.*, ‘spin down’ or in other words ‘bit value zero along direction x ’. In other words, the superposition of two eigenstates defined by a certain measurement direction, actually defines a pure state along some other direction. As such, one could interpret a qubit as a bit from which the value is determined by the highly contextual nature of how its value is measured, *i.e.*, one can regard the superposition states present in quantum computing as due to the possibility to define/apply different measurement contexts such that each defines a pure state for the qubit involved. Therefore, we could not only call such entity a qubit, emphasizing its quantum nature, but also put emphasis on its highly contextual nature by calling it a conbit (*contextual bit*). Indeed, depending on which context is chosen (*i.e.*, which direction is chosen for the Stern-Gerlach apparatus) different values for the bit will be found. If the Stern-Gerlach apparatus is placed along the z -direction, the superposition state

$$s = \frac{1}{\sqrt{2}} (|0\rangle_z - |1\rangle_z)$$

will yield the two bit values 0_z and 1_z with the same probability ($\frac{1}{2}$), but if we would place the Stern-Gerlach apparatus along the x -direction, we will obtain with certainty the outcome 0_x corresponding with the spin down eigenstate $|0\rangle_x$ for the x -direction. As such, we see that according to the used measurement context, the state of the system representing a bit yields different results for the bit value. Therefore, a qubit is highly contextual and we could call it a *conbit*, referring to this contextuality.

Using the concept of conbit we can consider any physical system with a set of bi-stable states, such that the outcomes of experiments are defined by the measurement context, to represent a ‘contextual’ bit. Therefore, if we could define a physical system in which the contextuality could be parametrized, we could in principle cover with the concept of conbit on the one hand the qubits, which are the highly contextual conbits, and on the other hand the classical bits which can be regarded as the non-contextual limit of a conbit. Hence, in the case that the entity is a quantum system, the conbit reduces to a qubit, and in the case of a classical system, where no contextuality occurs in the measurement situation and all experiments are deterministic, the conbit reduces to a classical bit.

2.3 Quantum Processing

Let us assume now that we have a register of N qubits. The theory of quantum computation tells how to encode an input to a quantum computer in a number of qubits that form the quantum register, and how to operate on them, with the aid of a quantum processor that works according to the laws of quantum mechanics, in order to get the desired output. Let us describe this process in a more detailed way.

The Hilbert space of a collection of quantum systems is the tensor product of the Hilbert spaces of the respective subsystems. Thus, the Hilbert space of an N -qubit quantum register is the tensor product of N 2-dimensional complex Hilbert spaces, each representing a single qubit. We will abbreviate the tensor product notation, *e.g.*, $|1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle$ by the notation $|1001\rangle$ which encodes also the binary expansion of the number 9 such that we can even write $|9\rangle = |1001\rangle$. These configurations in which each qubit is in an eigenstate of bit value one or bit value zero, coincide with the states of a classical register with N classical bits. However, while a classical system can be only in a classical configuration, the corresponding quantum system can be in any linear superposition (*i.e.*, linear combination with complex coefficients with squared moduli sum up to 1) of such configurations. Thus,

the possible quantum states form a subset of a complex linear space (a Hilbert space) spanned by the classical configurations. As such, the state of a quantum register of N qubits can be written in terms of the classical configurations as:

$$\sum_{i=0}^{2^N-1} c_i |i\rangle, \quad c_i \in \mathbb{C}, \quad (2)$$

where $|i\rangle$ denotes the state of the register that encodes the binary expansion of the number i , and $\sum |c_i|^2 = 1$. These 2^N pure states of the form $|\sigma_1, \dots, \sigma_N\rangle$ with $\sigma_k = 0, 1$, $k \in \{1, \dots, N\}$ form a basis of the register's state space which is called 'computational basis'.

The running of the quantum computer requires the application of various state manipulations according to some quantum algorithm. These manipulations are called 'quantum logic gates' and are given by unitary transformations. During these unitary transformations induced by the logic gates, the state of the quantum register evolves continuously in time. In the case of quantum computations usually one considers unitary transformations acting only on a few (1, 2 or 3) qubits at a time, called quantum gates. It can be shown (see, *e.g.*, [26]) that this does not restrict the variety of arithmetic operations which can be performed, *i.e.*, the set of logical gates acting on few qubits at a time is a so-called universal set of gates. This means that any logic circuit can be implemented using a number of these gates. This allows us to make numerical estimations of the time it would take on a computer to run a certain algorithm. Indeed, if we could estimate the number of logic gates used in the calculation and combine this with the time it takes to apply a certain logic gate to the register, we could estimate the time it will take the physical computational device to run a certain algorithm.

Let us conclude this section by giving some examples of elementary quantum gates, and construct the unitary matrices which represent the respective state transformation induced by each quantum logic gate.

One of the frequently used quantum gates is the controlled-NOT gate that operates on two qubits and changes the second bit iff the first bit is 1:

$$\begin{aligned} C_{not} : |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned} \quad (3)$$

The C_{not} gate is usually represented graphically by a following circuit:

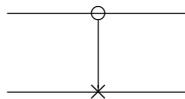


Fig. 1. Graphical representation of the controlled-NOT gate

where the circle represents the first (control) bit and the cross represents the conditional negation of the second bit. If we represent the involved bits in \mathbb{C}^4 , *i.e.*,

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

then the unitary matrix $U_{C_{cnot}}$ representing the operation C_{cnot} is given by

$$U_{C_{cnot}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The controlled-controlled-NOT gate, also called Toffoli gate, which operates on three qubits and negates the third bit iff the first two bits are 1 is represented by a circuit of the form:

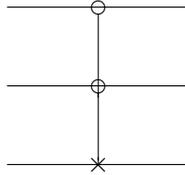


Fig. 2. Graphical representation of the Toffoli gate

This operation on the triple of qubits can be represented with the unitary matrix $U_{C_{cc-not}}$

$$U_{C_{cc-not}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

such that indeed *e.g.* $U_{C_{cc-not}} \cdot |110\rangle = |111\rangle$ etcetera.

To conclude, a quantum computer is constructed as follows. For the register one uses an N spin- $\frac{1}{2}$ particle system, such that the spin up state of a qubit corresponds with bit value +1 and spin down with bit value 0. The computation process can be regarded as the free evolution of the state of the register by running the quantum processor, *i.e.*, by applying various unitary state transformations induced by the (quantum) logic gates. However, during this unitary evolution the state of the register does not necessarily have to stay a product state of spin up and spin down eigenstates of the individual spin- $\frac{1}{2}$ entities, in general the register will be in a superposition state of such product states.

Therefore, during a quantum computation, the processor induces an evolution of the state of the quantum register along a path in Hilbert space which is not accessible for a classical device. One could expect that this larger set of available states allows a quantum computer to solve some problems faster than any classical algorithm can. And indeed, Shor's factorizing algorithm for a quantum computer allows to factorize an integer in a time polynomial in the size of the input. Despite all efforts, the best known classical algorithm still needs a time exponential in the size of the input. Whether it is actually impossible to find a classical polynomial time factorization algorithm, remains an open question.

3 Intermediate Models Between Quantum and Classical

In the hidden measurement approach to quantum mechanics the quantum probability is interpreted as due to a lack of knowledge about the precise measurement interaction which leads to indeterministic

outcomes (see, *e.g.*, [16, 17, 19, 20, 27, 28, 29, 22, 30, 31]). In this approach, an experiment is identified with a family of deterministic sub-measurements with a lack of knowledge about which sub-measurement actually takes place during a measurement. A concrete model has been put forward, which allows to visualize the concept of hidden measurement on a macroscopic model for a spin- $\frac{1}{2}$ measurement. Depending on the amount of uncertainty about which sub-measurement actually takes place, one obtains a continuous transition from a classical, deterministic system towards a quantum-like system in the sense that it has quantum-like state transitions induced by the measurement procedure with a quantum probability distribution over the set of outcomes. This uncertainty was modelled by a continuous real parameter, as we will discuss now in some more detail in next sections.

3.1 The Quantum Description of a Spin- $\frac{1}{2}$ Entity

In quantum theory a spin- $\frac{1}{2}$ particle is described in a two-dimensional complex Hilbert space. Pure states of the entity are represented by rays in that Hilbert space. It is well known that the unit vectors of the 2-dimensional complex Hilbert space can be represented on the surface of a unit sphere in three dimensions, usually called the Poincaré sphere. In this procedure we make use of the connection between the measurement direction u of a Stern-Gerlach experiment in three-dimensional space and the eigenstate s_u^+ for the spin up outcome corresponding with the spin observable S_u for this direction. The operator representing the spin observable along direction u is given by the Hermitian matrix S_u :

$$S_u = \frac{1}{2} \begin{pmatrix} \cos \theta & \sin \theta e^{-i\varphi} \\ \sin \theta e^{i\varphi} & -\cos \theta \end{pmatrix} \quad (4)$$

This self-adjoint spin operator has two orthogonal eigenvectors which are a basis for the Hilbert space \mathbb{C}^2 , namely

$$s_u^+ = \begin{pmatrix} \cos \frac{\theta}{2} e^{-i\frac{\varphi}{2}} \\ \sin \frac{\theta}{2} e^{i\frac{\varphi}{2}} \end{pmatrix}, \quad s_u^- = \begin{pmatrix} -\sin \frac{\theta}{2} e^{-i\frac{\varphi}{2}} \\ \cos \frac{\theta}{2} e^{i\frac{\varphi}{2}} \end{pmatrix} \quad (5)$$

with eigenvalue $+\frac{1}{2}$ and $-\frac{1}{2}$, respectively. The physical meaning of these eigenvectors is that if the entity is in a state s_u^+ we will find with certainty the outcome $+\frac{1}{2}$ for the spin measurement along the direction defined by u . Therefore the property ‘the spin entity is in a state such that spin up will be measured with certainty in a Stern-Gerlach experiment along direction u ’ can be represented with the eigenstate s_u^+ . We now associate the measurement direction u with the eigenstate s_u^+ and simply represent the spin state s_u^+ by the point u on the Poincaré sphere. In short we let correspond a point $u \in \mathbb{R}^3$ on the surface of the Poincaré sphere with a quantum state vector $s_u^+ \in \mathbb{C}^2$, eigenvector of S_u with eigenvalue $+\frac{1}{2}$. This correspondence between the set of (pure) states of quantum spin- $\frac{1}{2}$ particles and the points on the surface of the Poincaré sphere is one to one.

A measurement on a quantum entity induces a state transition from the initial state towards an eigenstate of the observed outcome. Therefore, if the eigenvalues are not degenerated (and this is the case in spin measurements), we can identify each outcome with its eigenstate. As such, we can regard the probability for each outcome as the probability with which a state transition from the initial state towards an eigenstate of the observed outcome will occur. According to standard quantum mechanics, such a state transition happens with a probability given by the squared amplitude of the inner product of the initial and the final state. Written in spherical coordinates such that $\theta_u = 0$, the probability $P(\psi_u | \psi_p)$ for a state transition from initial state ψ_p towards final state ψ_u , is given by:

$$P(\psi_u | \psi_p) = |\langle \psi_u | \psi_p \rangle|^2 = \left| \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos \frac{\theta}{2} e^{-i\frac{\varphi}{2}} \\ \sin \frac{\theta}{2} e^{i\frac{\varphi}{2}} \end{pmatrix} \right|^2$$

$$= \left| \cos \frac{\theta}{2} e^{-i\frac{\phi}{2}} \right|^2 = \cos^2 \frac{\theta}{2}$$

3.2 The ϵ -Model

Let us now describe the hidden measurement model for a spin- $\frac{1}{2}$ entity which was first given by D. Aerts [19]. The entity consists of a point particle on the sphere. Hence, its set of states is given by the points p on the Poincaré sphere. The experiments e_u^ϵ are defined as follows. We put an elastic of length 2ϵ centered around the origin between the point u and its antipode $-u$, and attach the end points of the elastic to the points u and $-u$ with unbreakable cords. Let us denote the segment between u and $-u$ with the interval $[-u, u]$. Next, the particle falls from its position p orthogonally onto the interval $[-u, u]$ in the point p' and stays attached there. Then the elastic breaks randomly and two things can happen. If the elastic breaks between p' and $-u$, the elastic will pull the point particle towards u where it stays attached and the experiment is said to yield the outcome $+1$. If on the other hand the elastic breaks between u and p' , then the elastic will pull the particle towards $-u$, where it stays attached, and the measurement is said to yield outcome -1 . If the string breaks at exactly the point where the particle is attached, then we assume that in such a case the measurement always yields the outcome $+1$. However, we remark that these events are physically irrelevant since they have measure zero, but we include these situations here anyway to make the definition of the measurement complete.

Let us use the notation θ to denote the angle between the state p of the entity and the direction u of the measurement device. If $\cos \theta \geq \epsilon$, then the elastic will always pull the particle towards u , resulting in an outcome $+1$ with certainty. Analogously, if $\cos \theta \leq -\epsilon$, the measurement always yields -1 . If p is such that $-\epsilon < \cos \theta < \epsilon$, the measurement yields one of the two possible outcomes $+1$ or -1 . According to the definition of the experiment e_u^ϵ , the probabilities of the respective outcomes for this situation are as follows. The probability for outcome $+1$ is given by the length of the elastic between the projection point p' and the point $-\epsilon$, normalized by the total length of the elastic. This is

$$P(u | p) = \frac{\cos \theta + \epsilon}{2\epsilon} \quad (6)$$

Similarly we can calculate the probability for the outcome -1 as

$$P(-u | p) = \frac{\epsilon - \cos \theta}{2\epsilon} \quad (7)$$

Let us now consider the special cases $\epsilon = 1$ and $\epsilon = 0$. If $\epsilon = 1$ the probabilities are given by

$$P(u | p) = \frac{1 + \cos \theta}{2} = \cos^2 \frac{\theta}{2} \quad (8)$$

$$P(-u | p) = \frac{1 - \cos \theta}{2} = \sin^2 \frac{\theta}{2} \quad (9)$$

These probabilities coincide with the quantum probabilities for a spin measurement of a spin- $\frac{1}{2}$ particle. If $\epsilon = 0$, the experiment is deterministic, and therefore this is called the deterministic or even classical limit of the sphere model. Hence, depending on the value of the parameter ϵ controlling the lack of knowledge about the fluctuations in the measurement interaction, one obtains a physical entity varying from a quantum probabilistic spin- $\frac{1}{2}$ model towards a classical deterministic entity.

3.3 Representing a Conbit with the ϵ -Model

If we would use the ϵ -model to represent a so-called ‘conbit’ (*i.e.*, a bit for which the value can only be measured in a contextual way), we can define a continuous family of physical systems representing

a conbit, from a quantum spin- $\frac{1}{2}$ entity, and hence a qubit, towards a classical deterministic entity, hence a classical bit.

It could be remarked that the deterministic limit of the sphere model is not a bi-stable state particle, since all points on the sphere are possible states. A true classical bit only has two possible states: either it is in a state of bit value zero or of bit value one. One way to solve this problem would be to associate the set of eigenstates of the outcome $+1$ with the bit value one, and the eigenstates of the outcome -1 with the bit value zero. As such, each bit is defined by a hemisphere containing the eigenstates of the corresponding outcome. (The set of states lying in the intersection of the two hemispheres has measure zero and as such is physically irrelevant.) In the deterministic limit of the ϵ -model, the only measurements which are considered meaningful (*i.e.*, defining a value for a bit) are the ones with a fixed measurement direction, *e.g.* along the z -direction. Hence the value of a classical bit is determined by the state of the ϵ -model entity in the deterministic limit $\epsilon = 0$, such that if the state is in the upper hemisphere the value of the conbit(classical bit) is one, and zero if the state is in the lower hemisphere.

3.4 Generalization to N Spin- $\frac{1}{2}$ Entities

It is possible to show that for any quantum entity of which the set of outcomes is in a finite dimensional space, a hidden measurement representation can be found. More specifically, in the case of an N -spin entity it was shown that a hidden measurement model exists as follows. First, the Majorana representation is used to represent the system by a system of $2N$ coupled spin- $\frac{1}{2}$ entities. Secondly, for this system a hidden measurement representation can be constructed using correlations between the so-called proper states of the $2N$ spin- $\frac{1}{2}$ entities in the system. Since for each such spin- $\frac{1}{2}$ entity there exists a concrete hidden measurement model, one can come to the conclusion that for any N -spin system a hidden measurement model can be constructed, given by $2N$ sphere models with so-called correlations of the first and the second kind. We refer to the references for a more detailed discussion of these hidden measurement models. More importantly, as a corollary, these results show how to construct a hidden measurement model for a system of N correlated spin- $\frac{1}{2}$ quantum entities, *i.e.*, a register of a quantum computer.

4 Computers ‘Between Quantum and Classical’

Within the hidden measurement approach, we can represent the quantum register by N correlated sphere models. By introducing the parameter ϵ , we can construct a continuous family of physical entities with in one limit N correlated quantum-like spin- $\frac{1}{2}$ entities, and in the other limit a system consisting of N deterministic entities, representing N classical digital (stable) bits. For each value of ϵ we obtain a physical model of a computational device with a register of N conbits, such that the set of states and properties is determined by the parameter ϵ . Depending on the structure of the set of properties, one obtains different families of possible algorithms, since these depend on the nature of the physical device used to perform the computation. Let us explain this in more detail in the following subsections.

4.1 Algorithms Identified by State Transformations: Computation as Evolution of a Physical System

We consider classical and quantum computation from a physical point of view, *i.e.*, we interpret the process of computation as the evolution of the state of the physical device representing the register of the computer. Feeding the input to the computer is done by preparing the state of the computer

register in a certain state. Then the processor induces some state transformations following a set of instructions encoded in a circuit of logic gates leading to a final state from which the output of the computer can be obtained. Therefore, from a physical point of view the classical and quantum computer can be treated within the same formalism. During a computation the state of the register undergoes a state transformation according to the used algorithm, and therefore one can identify an algorithm with the state transformation it induces. To get a better classification of the possible state transitions, and hence of the possible algorithms, we propose in the next subsection a general scheme to identify a physical system (in this case the register of the computer) with its set of states and the structure on its set of properties.

4.2 Between Quantum and Classical Computers and Generalized Evolution

We mentioned already that the ‘between quantum and classical’ models entail a structure that cannot be modelled by standard quantum mechanics. The reason is that two of the traditional axioms of standard quantum mechanics (when described axiomatically within standard quantum axiomatics) are not satisfied for the ‘between quantum and classical’ situations. We have investigated this aspect of the ‘between quantum and classical models’ in great detail [16, 17, 20, 29, 30, 31], and developed a general (quantum-like) categorical formalism (of state property systems) where these models can be described [21, 22, 32]. Concretely this means that within this formalism we can describe quantum systems, classical systems, and ‘between quantum and classical’ systems. The formalism is still in full development, so we cannot call it a full fledged theory yet. However, since for quantum computation, we only need finite systems (N spins), the specific models (the ϵ -model and the ϵ, ρ -model) that we mentioned already are sufficient for our purpose, we do not in principle need the general formalism that is under development. These specific models are on the same level of concreteness as the standard quantum mechanical models. Where the fact that the specific models fit into the general theory that we are developing is important is for the description of evolution of these specific models. Indeed, the aspects of the specific models that have been studied in great details are the aspects related to their quantum nature (measurement, state transition due to measurement, entanglement, probability, etc...), but little has been investigated to their evolution. Since the unitary evolution is also an intrinsic part of the quantum computation process we will have to study in detail the evolution aspect of the ‘between quantum and classical’ models to be able to define a ‘between quantum and classical’ computer. It is in this study that we want to consider the specific models as concrete entities within this general categorical formalism that we developed [21, 22, 32]. There is indeed a straightforward way in theoretical physics to introduce dynamical evolution into a theory: one looks for representations of the one parameter group of time translations into the group of automorphisms of an entity in this theory. It is possible that we encounter unexpected and deep problems here, which may even make it impossible to conceive of a ‘between quantum and classical’ computer. For example, it might turn out that the type of evolution that we can derive for the ‘between quantum and classical’ models only entails the specific aspects of the quantum computation process that makes it so powerful in the limit case for a pure quantum system and unitary evolution. Even in this case however we will have learned something more about the nature of the quantum computation process and what makes it so different from the classical computation process. If, on the other hand, we can derive evolutions that allow us to also realize a ‘between quantum and classical’ computation process, with the same (although probably less strong) gain of power as the pure quantum computation process, we might be able to see in which way such a process could be realized in reality.

5 Conclusions

Using results obtained within the hidden measurement approach of quantum mechanics, we propose a way how to construct explicit macroscopical models for the register of a quantum computer, such that the quantum register is represented by a set of sphere models coupled by correlations of the first and second kind.

Secondly, by varying the uncertainty about the measurement interaction ϵ and the coupling ρ between the ϵ -models, one can construct a family of physical systems representing a register of N coupled contextual bits (called conbits) with a continuous transition from a quantum system with quantum entanglement (the register of the quantum computer) towards a classical system of N ‘separated’ bits (register of a classical digital computer). This way, quantum and classical computation can be studied in a uniform way.

Since for the intermediate sphere models, *i.e.*, for $\epsilon \in]0, 1[$, no quantum nor classical description is possible, these intermediate entities have to be described in a more general formalism, namely within the categorical setting of the state property systems. In this formalism, state transformations are described by automorphisms of the state property system. As such, the running of an algorithm (which is just a continuous state transformation from the initial state (representing the input) towards the final state (representing the output)) can be characterized, and therefore, one can study classical and quantum computation in the same formalism, namely by the automorphisms on the set of properties.

6 Acknowledgments

Part of the research for this article took place in the framework of the bilateral Flemish-Polish project 127/E-335/S/2000. B. D’Hooghe is a Postdoctoral Fellow of the Fund for Scientific Research - Flanders (Belgium)(FWO - Vlaanderen).

References

- [1] R. Feynman, Simulating physics with computers, *Int. J. Theor. Phys.*, **21**, 467 (1982).
- [2] R. Feynman, Quantum mechanical computers, *Found. Phys.*, **16**, 507 (1986).
- [3] P. W. Shor, Algorithms for quantum computation, discrete logarithms and factoring, *Proc. 35th Annual symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 124 (1994).
- [4] P. W. Shor, Polynomial-time algorithms for integer factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, **26**, 1484 (1997).
- [5] C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, Quantum cryptography, or unforgeable subway tokens, in *Advances in Cryptology: Proceedings of Crypto ‘82*, eds. Chaum, D., Rivest R. L. and Sherman, A. T., Plenum Press, New York and London (1983).
- [6] C. H. Bennett, G. Brassard, C. Crépeau and M. Skubiszewska, Practical quantum oblivious transfer, in *Advances in Cryptology – CRYPTO ‘91*, ed. Feigenbaum, J., volume 576 of Lecture Notes in Computer Science, Springer-Verlag, Berlin (1992).
- [7] B. S. DeWitt and N. Graham, eds., *The Many-Worlds Interpretation of Quantum Mechanics*, Princeton University Press, Princeton (1973).

- [8] D. Deutsch, *The Fabric of Reality*, The Penguin Press, London (1997).
- [9] D. Aerts, “A mechanistic classical laboratory situation violating the Bell inequalities with $2\sqrt{2}$, exactly ‘in the same way’ as its violations by the EPR experiments”, *Helv. Phys. Acta* **64**, 1-23 (1991).
- [10] B. Coecke, Representation of a spin-1 entity as a joint system of two spin- $\frac{1}{2}$ entities on which we introduce correlations of the second kind, *Helvetica Physica Acta*, **68**, 396 (1995).
- [11] B. Coecke, A representation for a Spin-S entity as a compound system in \mathbb{R}^3 consisting of $2S$ individual spin- $\frac{1}{2}$ entities, *Foundations of Physics*, **28**, No. 8, 1347 (1998).
- [12] D. Aerts, S. Aerts, B. Coecke and F. Valckenborgh, “The meaning of the violation of Bell’s inequalities: non-Local correlation or quantum behaviour?” preprint, Foundations of the Exact Sciences, Brussels Free University (1995).
- [13] D. Aerts, S. Aerts, J. Broekaert and L. Gabora, “The violation of Bell inequalities in the macroworld”, *Found. Phys.* **30**, 1387-1414 (2000).
- [14] D. Aerts and F. Valckenborgh, “The linearity of quantum mechanics at stake: the description of separated quantum entities”, this volume.
- [15] D. Aerts and F. Valckenborgh, “Linearity and compound physical systems: the case of two separated spin 1/2 entities”, this volume.
- [16] B. D’Hooghe, From quantum to classical: A study of the effect of varying fluctuations in the measurement context and state transitions due to experiments, *doctoral dissertation*, VUB (2000).
- [17] D. Aerts, S. Aerts, B. Coecke, B. D’Hooghe, T. Durt and F. Valckenborgh, A model with varying fluctuations in the measurement context, in *New Developments in Fundamental Problems in Quantum Physics*, eds. Ferrero, M. and van der Merwe, A., Kluwer Academic, Dordrecht (1996).
- [18] C. Piron, *Foundations of quantum physics*, Reading, Mass (1976).
- [19] D. Aerts, A possible explanation for the probabilities of quantum mechanics, *J. Math. Phys.*, **27**, 202 (1986).
- [20] D. Aerts and T. Durt, Quantum, classical and intermediate, an illustrative example, *Found. Phys.*, **24**, 1353 (1994).
- [21] D. Aerts, “Foundations of quantum physics: a general realistic and operational approach”, *Int. J. Theor. Phys.* **38**, 289-358 (1999), lanl archive ref: *quant-ph/0105109*.
- [22] D. Aerts, E. Colebunders, A. Van der Voorde and B. Van Steirteghem, State property systems and closure spaces: a study of categorical equivalence, *Int. J. Theor. Phys.*, **38**, 259 (1999), lanl archive ref: *quant-ph/0105108*.
- [23] J. Pykacz, B. D’Hooghe and R. R. Zapatrin, Quantum Computers as Fuzzy Computers, *Lecture notes in computer science*, **2206**, Computational intelligence: theory and applications, ed. B. Reusch, Springer-Verlag, 526 (2001).
- [24] J.M. Jauch and C. Piron, Can hidden variables be excluded in quantum mechanics?, *Helv. Phys. Acta*, **36**, 827 (1963).

- [25] S. Kochen and E.P. Specker, The problem of hidden variables in quantum mechanics, *The Logico-Algebraic Approach to Quantum Mechanics, II*, ed. C. A. Hooker, Reidel Publishing Company, 293 (1967).
- [26] V. Vedral, A. Barenco and A. Ekert, Quantum Networks for Elementary Arithmetic Operations, *Phys. Rev. A*, **54**, 147 (1996).
- [27] D. Aerts, Classical theories and non classical theories as a special case of a more general theory, *J. Math. Phys.*, **24**, 2441 (1983).
- [28] D. Aerts, Construction of a structure which makes it possible to describe the joint system of a classical and a quantum system, *Rep. Math. Phys.*, **20**, 421 (1984).
- [29] D. Aerts, T. Durt and B. Van Bogaert, Quantum probability, the classical limit and non-locality, in the proceedings of the *International Symposium on the Foundations of Modern Physics 1992, Helsinki, Finland*, ed. T. Hyvonen, World Scientific, Singapore, 35 (1993).
- [30] D. Aerts and T. Durt, Quantum, classical and intermediate: a measurement model, in the proceedings of the *International Symposium on the Foundations of Modern Physics 1994, Helsinki, Finland*, eds. Montonen, C. et al., Editions Frontieres, Givès Sur Yvettes, France (1994).
- [31] D. Aerts and B. D’Hooghe, Operator structure of a non quantum and a non classical system, *Int. J. Theor. Phys.*, **35**, 2241 (1996).
- [32] D. Aerts, “Being and change: foundations of a realistic operational formalism”, this volume.