Quantum Simulators and Quantum Repeaters

Mladen Pavičić[1]

University of Zagreb, GF, Kačićeva 26, POB-217, HR-10001 Zagreb, Croatia.

Abstract

Two elements of quantum computation are considered: quantum computer logic and quantum repeater. It is shown that the quantum gate logic does have two different models and that it is therefore ambiguous. It is also shown that without additional conditions imposed on quantum gates one cannot arrive at a general quantum computer machine language. In absence of such conditions quantum entanglement remains a selection protocol which makes quantum computer equivalent to many photon intensity interferometry. As an example for such an entanglement we discuss a quantum optical repeater.

1 Introduction

Classical computers are based on classical logic which has a numerical algebraic model (Boolean algebra) but also a probabilistic model: one takes the values of the logical propositions and map them to [0,1] interval arriving immediately at a Kolmogorovian probability theory.[3] For quantum computers we still do not know of a quantum logic which would—when mapped to [0,1]—give us a Hilbertian probability theory. What we do know is how to make quantum logic gates and superpose their inputs so as to enable novel quantum algorithms such as Shor's and Grover's [14] which in a polynomial time solve the problems for which classical algorithms apparently request an exponential time and how to "simulate" a Schrödinger equation. [1] Hence, we are still away from a "proper" quantum computer which would convert input values for quantum logic gates directly to mean values of observables in a polynomial number of steps, i.e., which would enable us to simply type in a Schrödinger equation and by simulating a molecule or whatever quantum system get a desired result. This kind of usage of quantum computers—which boils down to quantum mathematics—is what would represent not only qualitatively faster algorithms and a genuine parallel processing but an essentially new way of solving problems by simulating physical systems with the help of a direct conversion of the input gate values. In this paper we present some results which brings us closer to the goal.

In Sec. 2 we show that in addition to its well-known model—Boolean algebra—classical logic unexpectedly turn out to have yet another model which is not distributive. We explain why this discovery does not have an impact on classical computers. Then we present another result, which is that quantum logic also have two different models and explain why the latter discovery does have an impact on quantum computers, as opposed to the classical case. We also

[1] E-mail: mpavicic@faust.irb.hr; Web page: http://m3k.grad.hr/pavicic

stress that quantum gates do yield quantum entanglement but not a Hilbertian representation of a general quantum system. In this respect, physics of quantum gates corresponds to physics of the many photon intensity interferometry.

As an example of such an analogy in Sec. 3 we present an optical quantum repeater. A photon from a four photon system, obtained by a controlled entanglement of two downconverted photon pairs, is entangled with a photon from another such four photon system. As a result two other photons, each from one of the systems appear in a singlet state with an event probability arbitrary close to one. This is due to the fact that in such an entanglement, through a selection made by means of the remaining photons from the systems, the probability of photons coming out from the same side of a beam splitter can be made arbitrary small. By means of subpicosecond lasers with nanosecond oscillations locked to a master clock one can use the property to construct quantum repeaters for communication of EPR pairs. The repeater can be applied in quantum computer, in teleportation, quantum cryptography, and for loophole-free Bell experiments.

2 Quantum Computer Logic and Algebra

In classical logic used by classical computers it is enough to ascribe values, 0 and 1, to its propositions to arrive at Boolean algebra of the propositions. In quantum logic of elementary input propositions for quantum computers we cannot do the same because one cannot ascribe a definite value to every proposition (Kochen-Specker's theorem). Still one can obtain a partial algebra which is a lattice. Complete specification of such a quantum algebra is an open problem as we shall see below.

A computer is a computational device in which a 2×2 unitary matrices called *logic gates* act on elementary bits $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$ and on bits obtained by such operations. A classical gate is for example a NOT gate which flips bits in the following way: $\mathsf{NOT}|0\rangle = \mathsf{NOT}(1,0) = |1\rangle$ and $\mathsf{NOT}|1\rangle = \mathsf{NOT}(0,1) = |0\rangle$. A quantum gate which is characteristic of the existing experimental hardware is the *controlled* NOT gate which acts on two such bits (quantum bits, *qubits*) in a conditional way [as simple NOT gate on the second (target) qubit provided the first (control) qubit is 1], e.g., $\mathsf{CNOT}|10\rangle = |11\rangle$.

We describe the system of qubits by unit vectors in the Hilbert space $\mathcal{H}^2$ over the field of complex numbers. We denote the two orthogonal states by $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$. The states make an orthogonal basis for $\mathcal{H}^2$. In a quantum computer we deal with a big number n of qubits which build up a composite Hilbert space $\mathcal{H} = \mathcal{H}^2 \otimes \ldots \otimes \mathcal{H}^2$. The computational basis, i.e., the basis of this space, consists of the following 2^n vectors: $|00\cdots 00\rangle$, $|00\cdots 01\rangle, \ldots,$ $|11\cdots 11\rangle$, where, e.g., $|00\rangle$ means $|0\rangle \otimes |0\rangle$. Classical bits correspond to quantum states: $i_1 i_2 ... i_n \longleftrightarrow |i_n\rangle \equiv |i_1 .... i_n\rangle$.

To compute the function $f : i_1 i_2 ... i_n \longmapsto f(i_1, ... i_n)$. means to let the corresponding states evolve according to the time evolution unitary operator U (Schrödinger equation):

$$|i_1 i_2 ... i_n\rangle \longmapsto U|i_1 i_2 ... i_n\rangle = |f(i_1, ... i_n)\rangle. \tag{1}$$

The unitarity of U assures reversibility and therefore prevents energy dissipation. This can be achieved with classical devices as well but only at the cost of exponentially growing hardware or exponentially rising time. The reason for that is simple: n classical states describing a system in a classical computer can only be specified by ascribing values all 2^n basis states. So, in classical computation we have the input values for propositions and by means of logic gates we obtain new propositions with definite values. Hence we do have a *logic.*

Do we have such a logic in quantum computation? Quantum computers achieve speed and a parallel way of computing—which are their essential features—by using superposition which puts n quantum states in a superposition of all 2^n basis states in one step. To see this let us consider the following superposition of n qubits: $\sum_{i_1 i_2 \dots i_n=0}^{1} |i_1 i_2 \dots i_n\rangle$. Applying the linear unitary operation which computes f, from Eq. (1), to this state, yields: $\sum_{i_1,i_2,\dots,i_n=0}^{1} |f(i_1 i_2 \dots i_n)\rangle$. U computes f *parallelly* on all the 2^n possible inputs i and in the end by a wave packet collapse a final output.

To obtain such a parallel computing in an assumed realistic computer, we start with an initial state $|i\rangle$ which corresponds to an "input" to the computation. We then perform elementary operations on the system using the quantum gates defined above. The operations correspond to the computational steps in the computation, just like logic gates are the elementary steps in classical computers, and are performed on an isolated system, so the evolution can always be described by a unitary matrix operating on the state of the system. But can we translate a general Hamiltonian into a set of instructions for quantum gates on how to transform input states in time? The answer is currently in the negative. There is no known finite and definite receipt for such a correspondence. To make it possible we try to narrow the gap between an algebra of elementary propositions (corresponding to pure states) and the Hilbert space description. First, let us see whether we can unambiguously construct such an algebra starting with these propositions, i.e., with quantum logic.

Let us denote any Hilbert space subspaces (e.g., the afore-mentioned one and two dimensional ones) $\mathcal{H}_a$, $\mathcal{H}_b$, $\mathcal{H}_c, \dots$ by a, b, $c, \dots$. Let $\mathcal{C}(\mathcal{H})$ be a set of closed subspaces. We define orthocomplementation for $\mathcal{H}_a$, where $\mathcal{H}_a \subseteq \mathcal{H}$, as $a' = \{x \in \mathcal{H} | \langle x|y\rangle = 0,\ \forall y \in \mathcal{H}_a\}$. On $\mathcal{C}(\mathcal{H})$ we define meet $a \cap b$ as $\mathcal{H}_a \cap \mathcal{H}_b$ and join $a \cup b$ as the smallest closed subspace of $\mathcal{H}$ containing $\mathcal{H}_a \cup \mathcal{H}_b$, which always exists. We write 0 for the smallest element $\emptyset$ in $\mathcal{C}(\mathcal{H})$ and 1 for the largest element $\mathcal{H}$ in $\mathcal{C}(\mathcal{H})$. Ordering $a \le b$ is defined as $\mathcal{H}_a \subseteq \mathcal{H}_b$ which can be shown to be equivalent to $a = a \cap b$ and to $a \cup b = b$. The ordering corresponds (see below) to the operation of implication (Sasaki) which is defined as $a \to b \ = \ a' \cup (a \cap b)$. The orthogonality $\mathcal{H}_a \perp \mathcal{H}_b$ is given by $a \le b'$. Let us denote the set containing all a, b, $c, \dots$ by L°.

Definition. An ortholattice is algebra OL $= \langle L^\circ_{\mathrm{OL}}, ', \cup\rangle$ in which the following conditions are satisfied for any $a, b, c \in L^\circ$:

L1. $a \le a'' \quad \& \quad a'' \le a$

L2. $a \le a \cup b \quad \& \quad b \le a \cup b$

L3. $a \le b \quad \& \quad b \le a \quad \Rightarrow \quad a = b$

L4. $a \le 1$

L5. $a \le b \quad \Rightarrow \quad b' \le a'$

L6. $a \le b \quad \& \quad b \le c \quad \Rightarrow \quad a \le c$

L7. $a \le c \quad \& \quad b \le c \quad \Rightarrow \quad a \cup b \le c$

An ortholattice is orthomodular (OML) if and only if $\forall a, b \in L^\circ_{\rm OL}$:

L8a. $b \le a \quad \& \quad c \perp a \qquad \Longrightarrow \qquad a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$,

or

L8b. $a \cup b = ((a' \cup b') \cap a) \cup b$,

or both; it is modular (ML) if and only if $\forall a, b \in L^\circ_{\rm OL}$:

L9a. $b \le a \qquad \Longrightarrow \qquad a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$

or

L9b. $a \cap (b \cup (a \cap c)) = (a \cap b) \cup (a \cap c)$

or both, and it is distributive (DL) if and only if $\forall a, b \in L^\circ_{\rm OL}$

L10. $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$

It is well-known that $\mathcal{C}(\mathcal{H})$ is orthomodular if $\mathcal{H}$ is infinite dimensional and modular if $\mathcal{H}$ is finite dimensional (von Neumann and Birkhoff). Subspaces of a classical phase space build a distributive lattice, i.e., the Boolean algebra.

It is also well-known that in an orthomodular lattice the following equivalences holds: $a \le b \Leftrightarrow \ a \to b = 1$, where $a \to b \ =^{\rm def} \ a' \cup (a \cap b)$, and $a = b \ \Leftrightarrow \ a \equiv b = 1$, where $a \equiv b =^{\rm def} (a \to b) \cap (b \to a)$. In a Boolean algebra the following ones hold: $a \le b \ \Leftrightarrow \ a \rightharpoonup b = 1$, where $a \rightharpoonup b \ =^{\rm def} \ a' \cup b$, and $a = b \ \Leftrightarrow \ a \sim b = 1$, where $a \sim b \ =^{\rm def} \ (a \rightharpoonup b) \cap (b \rightharpoonup a)$.

Using these equivalences one can mimic any valid logical expression (wff), $\vdash A$ by $a = 1$. So, we easily arrive at either quantum (for either infinite or finite Hilbert spaces) or classical logic. We shall denote wwf's derivable in these quantum logics from a set Γ of their axioms and/or their consequences by $\Gamma \vdash_{\rm OM} A$ and $\Gamma \vdash_{\rm M} A$ and in classical logic by $\vdash_{\rm D} A$. However, once we go "there" we cannot go back.

For, an ortholattice is weakly orthomodular (WOML) if and only if $\forall a, b \in L^\circ_{\rm OL}$:

L11. $a \cup b \equiv ((a' \cup b') \cap a) \cup b = 1$;

a WOML is weakly modular (WML) if and only if $\forall a, b \in L^\circ_{\rm WOML}$:

L12. $a \cap (b \cup (a \cap c)) \equiv (a \cap b) \cup (a \cap c) = 1$;

and a WOML is weakly distributive (WDL) if and only if $\forall a, b \in L^\circ_{\rm WOML}$:

L10. $a \cap (b \cup c) \sim (a \cap b) \cup (a \cap c) = 1$.

None of these lattices are orthomodular. Even more, we are able to prove the following soundness and completeness theorem for them

Theorem 2.1 [Pavičić and Megill][10, 11] $\Gamma \vdash_{\rm X} A$ *if and only if* A *is true in all* WXL *models, where* X *is either* OM*, or* M*, or* D.

in addition to the standard theorems

Theorem 2.2 $\Gamma \vdash_{\rm X} A$ *iff* A *is true in all* XL *models, where* X *is either* OM*, or* M*, or* D.

In other words, all the logics do have at least two different models for which both soundness and completeness can be proved. In the parlance of the model theory: they are non-categorical. The meaning and the repercussions of this finding are as follows. As we have shown in [11], as soon as we ascribe ordered numerical values to propositions of classical logic it can have only one model—the Boolean algebra. What is peculiar though is that the syntax of the classical logic literally corresponds to the syntax of the weakly distributive lattice and not to the one of the Boolean algebra. To all propositions of the quantum logic, on the other hand, one cannot ascribe definite numerical values in principle. Therefore one can impose two different algebras on input states (acting as propositions of quantum logic) which we will still discuss in Sec. 4. However, whatever algebra we choose one can show [4] that any of them should be much more structured than the algebra of plain quantum gates endowed with superpositions and entanglement, if we wanted to obtain a proper Hilbert space representation—whether infinite or finite dimensional—and turn quantum computer in a genuine quantum simulator.

We have already stressed that the quantum entanglement which obtain by controlled quantum gates corresponds to the second quantization of the standard quantum theory. In other words, it enables basic quantum algebra endowed with superposition but it does not add anything new to the algebra of quantum gates.

Consider for example the following *entangled* state of 2 particles which can then be used for a teleportation of states or Bell experiments or quantum cryptography (we omit the normalization factors):

$$|00\rangle + |11\rangle \tag{2}$$

Here none of the two qubits has a definite state: the state of the system is not a tensor product of the states, and we cannot find a_1, a_2, b_1, b_2 such that

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$$

since

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

and $a_1b_2 = 0$ implies that either $a_1a_2 = 0$ or $b_1b_2 = 0$. These states represent situations that have no classical counterpart in the sense of many photons intensity interferometry. In a quantum computer we can obtain them by combining the Hadamard transformation ($|0\rangle \longmapsto |0\rangle + |1\rangle$, $|1\rangle \longmapsto |0\rangle + |1\rangle$) and the controlled NOT (CNOT) transformation and enable executing algorithms (Shor's, Grover's, Bogoshian's) or constructing parts such as the repeater we present in the next section. But without a general algebraic syntax they do not enable imposing an arbitrary Hamiltonian on them.

3 Quantum Optical Repeater

Sending EPR pairs over distances as well as their entanglement is essential for quantum cryptography, teleportation [2], and computation. A serious drawback of such sending is that a quantum signal cannot be amplified.

Here we give a physical model of a quantum optical repeaters not as a realistic proposal but in order to discuss its characteristic. We start with the devices we described in detail here in Trieste three years ago and elsewhere. [6, 7, 9] They "prepare entanglements between photons that nowhere interacted and whose paths nowhere crossed... and put together two photons ... from two photon pairs and make them interfere ... at a beam splitter. As a result one finds polarization correlations between the other companion photons from the pairs whose paths nowhere crossed each other ... [and] we can consider them event-ready prepared in an entangled state. [8]

Fig. 1

We combine three such devices as shown in Fig. 1. Each device is a source of a photon singlet and can work, e.g., as a non-linear crystal in which a downconversion occurs. For example, an ultra-short laser beam simultaneously pumps up three type-II crystals. Looking at polarization, we find the photons 1 and 6 entangled and we might say that a state is teleported from photon 1 to photon 6: we put parallel polarizer in the paths 1 and 6 and find that either all detectors react or only 2-5. But, however intriguing this might be the device has no application: it cannot transmit a genuine quantum state. It is said that by such a device we can carry out a genuine teleportation between photon 2 and 6. This is true but such a teleportation also has no application because a downconverted EPR pair (obtained at intersections of crystal output cones) is uncontrollable. What we need in quantum computing is a teleportation of a particular definite quantum state from one part of a quantum computer to another without destroying it (i.e., without finding it out) so that we can use it for further computation.

There are several practical reasons why we cannot do that with the available sources and detectors. First, in order to have coincidence detection instead of coincidental sub-picosecond pumping of crystals we should have sub-picosecond responding time detectors which do not exist. Then we should have controllable sources and this is in principle impossible with spontaneous downconversion. Let us however assume that we found a controllable EPR pair source.

The next problem are the beam splitters because we must discard events whenever photons come out from the same side of a beam splitter which is 75% of events for each beam splitter and 42% for all three. [5] Let us consider asymmetrical (highly transparent or highly reflective) beam splitters. Each successful entanglement corresponds to a nonmaximal singlet state [6, 9] which has the following representation

$$|\Psi\rangle = \frac{1}{\sqrt{R^2+T^2}}(R|\rightarrow\rangle_1|\uparrow\rangle_2 - T|\uparrow\rangle_1|\rightarrow\rangle_2)\,, \qquad (3)$$

Now we combine two such outputs at the middle beam splitter as shown in Fig. 1. Singlets from each unit combine to the following input product for the repeater:

$$|\Psi\rangle = \frac{1}{R^2+T^2}(R|\rightarrow\rangle_1|\uparrow\rangle_{1''} - T|\uparrow\rangle_1|\rightarrow\rangle_{1''})\otimes(T|\rightarrow\rangle_1|\uparrow\rangle_2 - R|\uparrow\rangle_1|\rightarrow\rangle_2)\,. \qquad (4)$$

Coincidental firing of detectors over all beam splitters puts the photons 1 and 6 into following nonmaximal singlet:

$$|\Psi\rangle = \frac{1}{R^2+T^2}(R^3|\rightarrow\rangle_1|\uparrow\rangle_2 - T^3|\uparrow\rangle_1|\rightarrow\rangle_2)\,. \qquad (5)$$

If we had such a source which would always produce only one pair we would have a completely feasible and reliable loophole-free Bell experiment at hand, because the probability of obtaining the above state for, e.g., $R = 0.9999$ is 0.9998. Explicitly $P_{\rightarrow\uparrow} = 1-TR(2-TR)/(1-2TR)$. All the other probabilities (for P1", P2" oriented as ↑→, or →→, or ↑↑ and for both photons exiting from the same side of BS") contain T as a factor and are therefore all less than $T = 1 - 0.9999 = 0.0001$ in the above example. This means that we would not be forced to rely on coincidental firing of detectors 1 and 6 to obtain reliable singles probabilities: firing of, e.g., detector 1 would mean that photon 6 emerges from the source *III* with a probability arbitrary close to one (provided all the detectors over the beam splitters fired).

But an assymetrical state is of little use for a teleportation within a quantum computer. To teleport a state by EPR singlets we have to have symmetrical singlets and they waste 75% of events in the above scheme. And the scheme is general and can also be obtained by means of Hadamar and CNOT gates within a quantum computer itself. Whether one can re-use the waste in calculation remains to be seen.

4 Conclusion

In Sec. 2 we show that there are two non-isomorphic models of the propositional calculus of quantum logic corresponding to an infinite dimensional Hilbert space representation: an orthomodular lattice and a weakly orthomodular lattice; that there are two non-isomorphic models of the propositional calculus of quantum logic corresponding to a finite dimensional Hilbert space representation: a modular lattice and a weakly modular lattice; and that there are two non-isomorphic models of the propositional calculus of classical logic: a distributive lattice (Boolean algebra) and a weakly distributive lattice. Hence, all calculuses are non-categorical and none of them does map its syntactical structure to both models. They do so to one of the models and do not to the other. Surprisingly the models which do preserve the syntactical structure of the logics are not the standard ones (Boolean algebra and the orthomodular lattice) but the other ones: weakly distributive and weakly orthomodular lattices.

Classical computer applications are not affected by this finding since the usual ordered numerical valuation of classical logic excludes the weakly distributive model: two-valued classical logic admits only the two-element Boolean algebra—and the usual many-valued classical logic also admits only Boolean algebra as its model. Weakly distributive model for classical logic cannot be numerically valuated. It admits only a non-archimedean (non-ordered) valuation. This opens a possibility of using non-ordered lattice models for a faithful reflection of the syntax of the logic.

With quantum logic it is just the opposite—yes-no values cannot be ascribed to all quantum propositions due to the Kochen-Specker theorem. [13] This is the difference between quantum and classical computation: the classical one proceeds by switching logic gates and ascribing values to propositions by the gate on the way till the final output of a sequence of calculation; the quantum one proceed in a syntactical way, e.g., by combining Hadamar transformation, `CNOT` transformation, phase shifts, etc., arriving at a genuinely entangled state in which no one of the subsystems (propositions) is in any definite state. On the example of a quantum repeater we argued that without a complete syntax quantum computer is but a huge interfometer which always requires special algorithms to work.

We have shown above that there are two possible syntaxes corresponding to two possible algebras: an orthomodular one and a weakly orthomodular one for a most general case, and a modular and a weakly modular one for the finite dimensional one. Orthomodular and modular algebras enable can mathematically be made isomorphic to infinite and finite Hilbert space, respectively. Whether one can do that by a quantum computer is an open question because one first have to solve the problem of translating additional mathematical conditions into commands and transformations for quantum gates. On the other hand, one should see whether weakly orthomodular and modular algebras might offer a simpler syntax and whether it might turn out that a non-archimedean valuation is manageable. After all, finite-dimensional Hilbert spaces allow nonstandard non-archimedean Keller fields in addition to the standard (real, complex, and quaternionic) ones and it has been shown that this does not disable their usage for proper physical measurements.

Acknowledgments

M. P. acknowledges a support of the Ministry of Science of Croatia.

References

[1] B. M. Boghosian and W. Taylor, *Physica D* **120**, (1998) 30.

[2] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, *Phys. Rev. Lett.* **80**, (1998) 1121.

[3] H. Leblanc, in *Handbook of Philosophical Logic*, D. Gabbay and F. Guenthner, Eds., vol. I (D. Reidel, Dordrecht, 1983), pp. 189–274.

[4] N. D. Megill, and M. Pavičić, [submitted] (1999).

[5] M. Pavičić, *Phys. Rev. A* **50**, (1994) 3486.

[6] M. Pavičić, *J. Opt. Soc. Am. B* **12**, (1995) 821.

[7] M. Pavičić, in *Quantum Interferometry; Proceedings of the Adriatico Workshop, Trieste, March 1996*, F. De Martini, G. Denardo, and Y. Shih, Eds., (VCH Publishing Division I, Weinheim-New York, 1996), pp. 193–204.

[8] M. Pavičić, in *Abstracts of papers presented at the Adriatico Workshop, Trieste, March 1996*, F. De Martini, Ed., (The Abdus Salam Int. Centre of Theor. Phys., Trieste, 1996).

[9] M. Pavičić, *Optics Commun.* **142**, (1997) 308.

[10] M. Pavičić and N. D. Megill, *Helv. Phys. Acta* **71**, (1998) 610.

[11] M. Pavičić and N. D. Megill, http://xxx.lanl.gov/abs/quant-ph/9906101.

[12] M. Pavičić and J. Summhammer, *Phys. Rev. Lett.* **73**, (1994) 3191.

[13] A. Peres, *Found. Phys* **26**, (1996) 807.

[14] V. Vedral and Martin B. Plenio, *Prog. Quant. Electron.* **22**, (1998) 1.

Figure 1: Outline of the device which entangles photons 1 and 6.