View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by CERN Document Server

arXiv:quant-ph/0611119v2 5 Feb 2007

Basic logic and quantum entanglement

P A Zizzi

Dipartimento di Matematica Pura ed Applicata
Via Trieste, 63 - 35121 Padova, Italy
e-mail: zizzi@math.unipd.it

Abstract

As it is well known, quantum entanglement is one of the most important features of quantum computing, as it leads to massive quantum parallelism, hence to exponential computational speed-up. In a sense, quantum entanglement is considered as an implicit property of quantum computation itself. But... can it be made explicit? In other words, is it possible to find the connective "entanglement" in a logical sequent calculus for the machine language? And also, is it possible to "teach" the quantum computer to "mimic" the EPR "paradox"? The answer is in the affirmative, if the logical sequent calculus is that of the weakest possible logic, namely Basic logic.

A weak logic has few structural rules. But in logic, a weak structure leaves more room for connectives (for example the connective "entanglement"). Furthermore, the absence in Basic logic of the two structural rules of contraction and weakening corresponds to the validity of the no-cloning and no-erase theorems, respectively, in quantum computing.

1 Introduction

Our purpose is to obtain an adequate sequent calculus [1] for quantum computation [2]. In particular, we look for logical connectives corresponding to the physical links existing among qubits in the quantum computer, and the associated inference rules. To this aim, we will exploit Basic logic [3] and its reflection principle between meta-language and object language. The sequent calculus we are looking for should be able to reproduce two main features of quantum computing namely quantum superposition and quantum entanglement. These two features taken together (the so-called quantum massive parallelism) are in fact very important as they lead to quantum computational speed-up [4]. A logical interpretation of quantum superposition is straightforward in Basic logic, and is given in terms of the additive connective &="with" (and of its symmetric, $\vee$="or") both present in linear [5] and Basic logics.

In this paper, we also propose a logical interpretation for quantum entanglement. Entanglement is a strong quantum correlation, which has no classical analogous. Then, the logic having room for the connective "entanglement", will be selected as the most adequate logic for quantum mechanics, and in particular for quantum computing. Quantum entanglement is mathematically expressed by particular superposition of tensor products of basis states of two (or more) Hilbert spaces such that the resulting state is non-separable. For this reason, one can expect that the new logical connective, which should describe entanglement, will be both additive and multiplicative, and this is in fact the case. We introduce the connective @="entanglement" by solving its definitional equation, and we get the logical rules for @. It turns out that @ is a (right) connective given in terms of the (right) additive conjunction & and of the (right) multiplicative disjunction $\wp$="par".

Then, we discuss the properties of @. In particular, we prove that @ is not idempotent, which is equivalent to formulate the "no self-referentiality" theorem in the meta-language.

Also, we show that, like all the connectives of Basic logic, @ has its symmetric, the (left) connective §, given in terms of the (left) additive disjunction, $\vee$="or", and the (left) multiplicative conjunction $\otimes$="times" (the symmetric of $\wp$).

Moreover, we provide Basic logic of a new meta-rule, which we name EPR-rule as it is the logical counterpart of the so-called EPR "paradox" [6].

The conclusion of this paper is that Basic logic is the unique adequate logic for quantum computing, once the connective entanglement and the EPR-rule are included.

2 A brief review of basic logic

Basic logic [3] is the weakest possible logic (no structure, no free contexts) and was originally conceived [7] as the common platform for all other logics (linerar, intuitionistic, quantum, classical etc.) which can be considered as its "extensions". Basic logic has tree main properties:

i) Reflection: All the connectives of Basic logic satisfy the principle of reflection, that is, they are introduced by solving an equation (called *definitional equation*), which "reflects" meta-linguistic links between assertions into the object-language. There are only two metalinguistic links: "yields", "and". The metalinguistic "and", when is outside the sequent, is indicated by and; when inside the sequent, is indicated by a comma.

$$\begin{array}{lcl} \textbf{Object language} \quad \underset{Reflection}{\longleftrightarrow} \ (= \mathit{iff}) & & \textbf{Meta-language} \\ \text{connectives} & & \text{meta-linguistic links} \begin{cases} \mathit{yelds} & \vdash \\ \text{“}\mathit{and}\text{”} & \begin{cases} \underline{\text{and}} & \mathit{outside\ the\ sequent} \\ ,(\mathit{comma}) & \mathit{inside\ the\ sequent} \end{cases} \end{cases} \end{array}$$

ii) Symmetry: All the connectives are divided into "left" and "right" connectives.

A left connective has formation rule acting on the left, and a reflection rule acting on the right. In Basic logic, every left connective has its symmetric, a right connective, which has a formation rule acting on the right, and a reflection rule acting on the left (and vice-versa).

Left connectives	$\underset{Symmetry}{\longleftrightarrow}$	**Right connectives**
$\vee$="*or*" (Additive disjunction)		&="*with*" (Additive conjunction)
$\otimes$="*times*" (Multiplicative conjunction)		$\wp$="*par*" (Multiplicative disjunction)
$\leftarrow$ (Counterimplication)		$\rightarrow$ (Implication)

iii) Visibility: There is a strict control on the contexts, that is, all active formulas are isolated from the contexts, and they are *visible*.

In Basic logic, the identity axiom $A \vdash A$ and the cut rule: $\dfrac{\Gamma \vdash A \quad A \vdash \Delta}{\Gamma \vdash \Delta}$ *cut* hold.

The cube of logics [3] [7] is a geometrical symmetry in the space of logics, which becomes apparent once one takes Basic logic as the fundamental one. As we said above, Basic logic is the weakest logic, and all the other logics can be considered as its extensions. All the logics, which have no structural rules (called substructural logics or resources logics) are the four vertices of one same face of the cube, considered as the basis. They have many connectives, less structure, and less degree of abstraction. On the upper face of the cube, we have all the structural logics (they have fewer connectives, more structure, and a higher degree of abstraction). See Fig. 1.

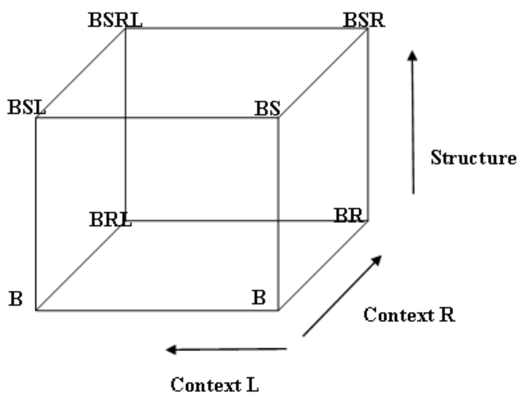

Figure 1: The cube of logics

Substructural logics:	**Structural logics:**
B = Basic logic	**BS** = quantum logic
BL = Basic logic + context on the left	**BSR** = paraconsistent logic
BR = Basic logic + context on the right	**BSL** = intuitionistic logic
BRL = Linear logic	**BSRL** = classical logic

3 Reasons why Basic logic is the logic of quantum computing

Basic logic has the following features, which are essential to describe quantum computation in logical terms:

a) It is **non-distributive** (because of the absence, on both sides of the sequent, of active contexts), and this is of course a first necessary requirement for any logic aimed to describe a quantum mechanical system.

b) It is **substructural**, i.e., it has no structural rules like contraction: $\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}$ (data can be copied) and weakening: $\dfrac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}$ (data can be deleted), accordingly with the no-cloning theorem [8] and the no-erase theorem [9] respectively, in quantum computing. The only structural rule, which holds in Basic logic, is the exchange rule:

$$exchL\,\frac{\Gamma, A, B, \Gamma' \vdash \Delta}{\Gamma, B, A, \Gamma' \vdash \Delta} \qquad\qquad exchR\,\frac{\Gamma \vdash \Delta, A, B, \Delta'}{\Gamma \vdash \Delta, B, A, \Delta'}$$

Then, for example, standard quantum logic [10] although being non-distributive, is excluded as a possible candidate for quantum computing because it has structural rules.

Linear logic is substructural, but has both left-side and right-side free contexts, then is excluded because of distributivity. (In particular, as we will see, for the connective @ =“entanglement”, the distributive property does not hold, then Linear logic cannot accommodate @).

c) It is **paraconsistent**: the non-contradiction principle is invalidated, and quantum superposition can be assumed.

4 The logical connective & for quantum superposition

The unit of quantum information is the qubit $|Q\rangle = a|0\rangle + b|1\rangle$, which is a linear combination of the basis states $|0\rangle$ and $|1\rangle$, with complex coefficients a and b called probability amplitudes, such that the probabilities sum up to one: $|a|^2 + |b|^2 = 1$. In logical terms, we will interpret the atomic proposition A as bit $|1\rangle$, and its primitive negation $A^\perp$ as bit $|0\rangle = NOT|1\rangle$, where NOT is the 2×2 off-diagonal matrix $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The atomic assertion $\vdash A$ will be interpreted as the quantum state $\vdash A \equiv |A\rangle = b|1\rangle$, and the asserted negation as $\vdash (A^\perp) \equiv |A^\perp\rangle = aNOT|1\rangle = a|0\rangle$. Notice that making the negation of the atomic assertion $\vdash A$ is not the same as asserting the negation of the atomic proposition, in fact $(\vdash A)^\perp \equiv NOT|A\rangle = b|0\rangle$.

In the meta-language, quantum superposition means that both propositions A and $A^\perp$ are asserted, that is, on the right-hand side of the definitional equation, we will have: $\vdash A$ $\underline{\text{and}}$ $\vdash (A^\perp)$. On the left-hand side, we look for the connective \$=“superposition”, such that $\vdash A\$A^\perp$ $\underline{\text{iff}}$ $\vdash A$ $\underline{\text{and}}$ $\vdash (A^\perp)$.

This is the definitional equation of & [3]:

$$\Gamma \vdash A\&B \qquad \underline{\text{iff}} \qquad \Gamma \vdash A \quad \underline{\text{and}} \quad \Gamma \vdash B$$

in the particular case with $B = A^\perp$ and $\Gamma = \emptyset$.

So that we can write the definitional equation for the connective “quantum superposition” as:

$$\vdash A\&A^\perp \qquad \underline{\text{iff}} \qquad \vdash A \quad \underline{\text{and}} \quad \vdash (A^\perp) \tag{1}$$

Then, of course, the rules of the connective “quantum superposition” are the same rules of & [3], with $B = A^\perp$ and $\Gamma = \emptyset$.

$$\& - \ form \, \frac{\vdash A \quad \vdash (A^\perp)}{\vdash A\&B}$$

This is obtained from the RHS to the LHS of the definitional equation (1).

$$\& - \ implicit\, refl \, \frac{\vdash A\&A^\perp}{\vdash A} \quad \frac{\vdash A\&A^\perp}{\vdash (A^\perp)}$$

This is obtained from the LHS to the RHS of the definitional equation (1).

By trivializing the &-implicit reflection, i.e., putting $\Gamma = A\&A^\perp$, we get the two &-axioms:

$$A\&A^\perp \vdash A, \qquad A\&A^\perp \vdash A^\perp$$

Suppose now $A \vdash \Delta(A^\perp \vdash \Delta)$. By composition with the “axiom” $A\&A^\perp \vdash A(A\&A^\perp \vdash A^\perp)$ we get the &-explicit reflection rule:

$$\& - \text{exp}l.refl \, \frac{A \vdash \Delta}{A\&A^{\perp} \vdash \Delta} \qquad \frac{A^{\perp} \vdash \Delta}{A\&A^{\perp} \vdash \Delta}$$

As we have completely solved the definitional equation (1) we can express quantum superposition in the object language with the composite proposition $A\&A^{\perp}$. Asserting: $A\&A^{\perp}$ (i.e. $\vdash A\&A^{\perp}$) is then equivalent to $(\vdash A)\&(\vdash A^{\perp})$.

The logical expression of the qubit $|Q\rangle = a|0\rangle + b|1\rangle$ is then:

$$\vdash Q \equiv \vdash A\&A^{\perp} \tag{2}$$

5 The logical connective @ for quantum entanglement

Two qubits $|Q\rangle_A = a|0\rangle_A + b|1\rangle_A$, $|Q\rangle_B = a'|0\rangle_B + b'|1\rangle_B$ are said entangled when the two qubits state $|Q\rangle_{AB}$ is not separable, i.e., $|Q\rangle_{AB} \neq |Q\rangle_A \otimes |Q\rangle_B$, where $\otimes$ is the tensor product in Hilbert spaces. In particular, a two qubit state is maximally entangled when it is one of the four Bell states [11]:

$$|\Phi_{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B\right), \quad |\Psi_{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B\right).$$

For simplicity, in this paper we will consider only Bell states. As we have seen in Sect. 3, expressing the qubit $|Q\rangle_A$ in logical terms leads to the compound proposition $Q_A \doteq A\&A^{\perp}$, where & stands for the connective "and". In the same way, we can associate a proposition B to the bit $|1\rangle_B$ and its primitive negation $B^{\perp}$ to the bit $|0\rangle_B$ so that the second qubit $|Q\rangle_B$ is expressed, in logical terms, by a second compound proposition $Q_B \doteq B\&B^{\perp}$. Bell states will be expressed, in logical terms, by the expression $Q_A@Q_B$, where @ is the new logical connective called "entanglement". Like all the other connectives, @ will be defined by the reflection principle, which translates meta-language into object language. We have at our disposal a meta-language which comes from our knowledge of the physical structure of Bell states. This leads us to figure out the logical structure for, say, the Bell states $|\Phi_{\pm}\rangle_{AB}$, namely $\vdash (A \wp B)\&(A^{\perp} \wp B^{\perp})$. Similarly, the logical structure for the Bell states $|\Psi_{\pm}\rangle_{AB}$ will be: $\vdash (A \wp B^{\perp})\&(A^{\perp} \wp B)$. In the following, we will consider only the logical expression for the states $|\Phi_{\pm}\rangle_{AB}$, as the case for $|\Psi_{\pm}\rangle_{AB}$ is obtained exchanging A with $A^{\perp}$. Eventually, we get the following definition: Two compound propositions $Q_A \doteq A\&A^{\perp}$, $Q_B \doteq B\&B^{\perp}$ will be said (maximally) entangled if they are linked by the connective @ = "entanglement". The definitional equation for @ is:

$$\Gamma \vdash Q_A@Q_B \qquad \underline{\text{iff}} \qquad \Gamma \vdash A, B \quad \underline{\text{and}} \quad \Gamma \vdash A^{\perp}, B^{\perp} \tag{3}$$

On the right-hand side of the definitional equation, we have the meta-language, coming from our knowledge of the physical structure of Bell states. On the left-hand side, instead, we have the object language. Also, it should be noticed that, on the right hand side of the definitional equation, each of the two commas is reflected into a $\wp$ while the meta-linguistic link <u>and</u> is reflected into & Thus the connective @ is an additive as well as multiplicative connective (more exactly, an additive conjunction and a multiplicative disjunction) which reflects two kinds of "and" on the right: one outside the sequent (<u>and</u>) and one inside the sequent (the comma). Finally, the connective @, is a derived connective which, nevertheless, has its own definitional equation: this is a new result in logic. Solving the definitional equation for @ leads to the following rules:

$$@-\text{formation} \qquad \frac{\Gamma \vdash A, B \qquad \Gamma \vdash A^{\perp}, B^{\perp}}{\Gamma \vdash Q_A @ Q_B} \tag{4}$$

$$@-\text{implicit reflection} \qquad \frac{\Gamma \vdash Q_A @ Q_B}{\Gamma \vdash A, B}\text{ (i)} \qquad \frac{\Gamma \vdash Q_A @ Q_B}{\Gamma \vdash A^{\perp}, B^{\perp}}\text{ (ii)} \tag{5}$$

$$@-\text{axioms} \qquad Q_A @ Q_B \vdash A, B \text{ (i)} \qquad Q_A @ Q_B \vdash A^{\perp}, B^{\perp} \text{ (ii)} \tag{6}$$

$$@-\text{explicit reflection} \qquad \frac{A \vdash \Delta \qquad B \vdash \Delta'}{Q_A @ Q_B \vdash \Delta, \Delta'}\text{ (i)} \qquad \frac{A^{\perp} \vdash \Delta \qquad B^{\perp} \vdash \Delta'}{Q_A @ Q_B \vdash \Delta, \Delta'}\text{ (ii)} \tag{7}$$

Eq. (4) is equivalent to the @-definitional equation from the right hand side to the left hand side. Eqs. (5) are equivalent to the @-definitional equation from the left hand side to the right hand side. The @-axioms in (6) are obtained from (5), by the trivialization procedure, that is, setting $\Gamma = Q_A @ Q_B$. The @-explicit reflection rules (i), (ii) in (7) are obtained by composition of the @-axioms (i) and (ii) in (6) with the premises $A \vdash \Delta$ and $B \vdash \Delta'$, and $A^{\perp} \vdash \Delta$ and $B^{\perp} \vdash \Delta'$, respectively.

The properties of @ are:

1) **Commutativity:**

$$Q_A @ Q_B \doteq Q_B @ Q_A \tag{8}$$

Commutativity of @ holds if and only if, the exchange rule is assumed (on the right). And in fact, exchange is a valid rule in Basic logic.

2) **Semi-distributivity**

¿From the definitional equation of @ with $\Gamma = \emptyset$, that is:

$$\vdash Q_A @ Q_B \qquad \underline{\text{iff}} \qquad \vdash A, B \quad \underline{\text{and}} \quad \vdash A^{\perp}, B^{\perp}$$

we get:

$$(A \& A^{\perp}) @ (B \& B^{\perp}) \doteq (A \wp B) \& (A^{\perp} \wp B^{\perp}) \tag{9}$$

We see that two terms are missing in (9) namely $(A \wp B^{\perp})$ and $(A^{\perp} \wp B)$, so that @ has distributivity with absorption, which we call semi-distributivity.

3) **Duality**

Let us define now the dual of @: $(Q_A @ Q_B)^{\perp} \equiv [(A \wp B) \& (A^{\perp} \wp B^{\perp})]^{\perp} = (A \otimes B) \vee (A^{\perp} \otimes B^{\perp})$ and let us call it §, that is: $(Q_A @ Q_B)^{\perp} \equiv Q_A \S Q_B$ (vice-versa, the dual of § is @: $(Q_A \S Q_B)^{\perp} \equiv Q_A @ Q_B$).

The definition of the dual of @ is then:

$$Q_A \S Q_B \doteq (A \otimes B) \vee (A^{\perp} \otimes B^{\perp}) \tag{10}$$

4) **Non Associativity:**

$$Q_A @ (Q_B @ Q_C) \neq (Q_A @ Q_B) @ Q_C \tag{11}$$

To discuss associativity of @, a third qubit Q_C is needed, and $Q_A @ (Q_B @ Q_C) \doteq (Q_A @ Q_B) @ Q_C$ cannot be demonstrated in Basic logic, as Q_C acts like a context on the right.

We remind that the maximally entangled state of three qubits is the GHZ state [12].

5) **Non-idempotence:**

$$Q_A @ Q_A \neq Q_A \tag{12}$$

The proof of (12) and its interpretation will be given in a forthcoming paper [13].

6 The EPR rule

Let us consider the cut:

$$\frac{\vdash Q_A \qquad Q_A \vdash A}{\vdash A}\, cut \tag{13}$$

which corresponds, in physical terms, to measure the qubit $|Q_A\rangle_A$ in state $|1\rangle_A$ (with probability $|b|^2$). In the same way, the cut: $\dfrac{\vdash Q_A \quad Q_A \vdash A^{\perp}}{\vdash A^{\perp}}\, cut$, corresponds to measure the qubit $|Q_A\rangle_A$ in state $|0\rangle_A$ (with probability $|a|^2$).

The cut (over entanglement) is:

$$\cfrac{\vdash Q_A @ Q_B \qquad Q_A @ Q_B \vdash A, B}{\cfrac{\vdash A, B}{\vdash A \wp B}\, \wp - formation}\, cut \tag{14}$$

Where, in (14), the rule of $\wp - fomation$ [3] is: $\wp - form\, \dfrac{\Gamma \vdash A, B}{\Gamma \vdash A \wp B}$.

Performing the cut in (14) corresponds, in physical terms, to measure the state $|1\rangle_A|1\rangle_B$. If we replace A and B in (14) with $A^{\perp}$, $B^{\perp}$ the cut corresponds to measure the state $|0\rangle_A|0\rangle_B$. It should be noticed, that, if we make a measurement of Q_A (supposed entangled with Q_B) and get A, then by semi-distributivity of @, we have:

$$A @ Q_B \equiv A @ (B \& B^{\perp}) \doteq A \wp B \tag{15}$$

As it is well known, if two quantum systems S_A and S_B are entangled, they share a unique quantum state, and even if they are far apart, a measurement performed on S_A influences any subsequent measurement performed on S_B (the EPR "paradox" [6]). Let us consider Alice, who is an observer for system S_A, which is the qubit Q_A, that is, she can perform a measurement of Q_A. There are two possible outcomes, with equal probability 1/2:

(i) Alice measures 1, and the Bell state collapses to $|1\rangle_A|1\rangle_B$.

(ii) Alice measures 0, and the Bell state collapses to $|0\rangle_A|0\rangle_B$.

Now, let us suppose Bob is an observer for system S_B (the qubit Q_B). If Alice has measured 1, any subsequent measurement of Q_B performed by Bob always returns 1. If Alice measured 0, instead, any subsequent measurement of Q_B performed by Bob always returns 0. To discuss the EPR paradox in logical terms, we introduce the EPR rule:

$$\cfrac{\Gamma \vdash Q_A @ Q_B \qquad Q_A \vdash A}{\cfrac{\cfrac{\Gamma \vdash A @ Q_B}{\Gamma \vdash A, B}\, @ - impl.refl.}{\Gamma \vdash A \wp B}\, \wp - form.} \tag{16}$$

Where the semi-distributivity of @, i.e. $A @ Q_B \doteq A, B$ has been used in the step "@-impl.refl".

Notice that the consequences of the EPR rule are the same of the cut over entanglement (14), because of semi-distributivity of @. It was believed that no other rule existed, a part from the cut rule, or at least some rule equivalent to it, which could cut a formula in a logical derivation. Nevertheless, the EPR rule does cut a formula, but it can be proved that it is not equivalent to the cut rule over entanglement (and, vice-versa, the cut rule over entanglement is not equivalent to the EPR rule). This is a new result in logic.

Let us show first that the EPR rule is not equivalent to the cut rule. We start with the premises of the EPR rule and apply the cut rule:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma\vdash Q_A@Q_B}{\Gamma\vdash Q_A@Q_B \quad Q_A@Q_B\vdash A,B}\,@-axiom}{\Gamma\vdash A,B}\,cut \qquad Q_A\vdash A}{\Gamma\vdash A,B,Q_A \qquad Q_A\vdash A}\,weak.L}{\Gamma\vdash A,A,B}\,cut}{\Gamma\vdash A,B}\,contr.R \tag{17}$$

It is clear that it is impossible to demonstrate that the EPR rule is equivalent to the cut rule (over entanglement) in Basic logic, where we don't have the structural rules of weakening and contraction. And in any logic with structural rules, the connective entanglement disappears, and the EPR rule collapses to the cut rule.

Now, we will show the vice-versa, i.e., that the cut rule (over entanglement) is not equivalent to the EPR rule. We start with the premises of the cut rule (14) and apply the EPR rule (16):

$$\dfrac{\Gamma\vdash Q_A@Q_B \qquad \dfrac{Q_A@Q_B\vdash A,B}{Q_A@Q_B,Q_A\vdash A,B}\,weak.L}{\Gamma,Q_A@Q_B\vdash A@Q_B,B}\,EPR^C \tag{18}$$

Where in (18), EPR^C means EPR rule in presence of contexts (here $Q_A@Q_B$ on the left and B on the right). But contexts are absent in Basic logic (visibility). Furthermore, the weakening rule is not present in Basic logic. These facts lead to the conclusion that in Basic logic it is impossible to prove that the cut is equivalent to the EPR rule. Moreover, this is impossible also in sub-structural rules with contexts (like BL, BR, and BLR) because one cannot use weakening, and in structural logics because the connective entanglement disappears.

The EPR rule is a new kind of meta-rule peculiar of entanglement, which is possible only in Basic logic. It is a stronger rule (although less general) than the cut, as it uses a weaker premise to yield the same result. Hence, instead of proving $Q_A@Q_B$ in (14) that is $\vdash Q_A@Q_B$, we can just prove Q_A, i.e., $\vdash Q_A$, perform the usual cut (13) (over Q_A), and leave the result A entangled with Q_B. Roughly speaking, if two compound propositions are (maximally) entangled, it is sufficient to prove only one of them. This is the logical analogue of the EPR "paradox".

7 Conclusions

Basic logic, once endowed with the new connective "entanglement" and the EPR rule, provides the unique adequate sequent calculus for quantum computing. We list below the main features of quantum information and quantum computing, and the corresponding required properties for the associated logic. The main features of quantum computing are:

- 1) Quantum Information cannot be copied (no-cloning theorem).
- 2) Quantum Information cannot be deleted (no-erase theorem).
- 3) Heisenberg uncertainty principle.

- 4) Quantum superposition
- 5) Quantum entanglement
- 6) Quantum non-locality, EPR "paradox".

The corresponding logical requirements are:

- 1') No contraction rule
- 2') No weakening rule
- 3') Non-distributivity, then no free contexts on both sides.
- 4') Connective &="superposition"
- 5') Connective @ ="entanglement"
- 6') The EPR rule

Requirements 1'–3' exclude all logics apart from Basic logic **B** (and **BR**, **BL**, for more than two qubits).

B satisfies the remaining requirements 4'–6'.

Acknowledgements. I wish to thank G. Sambin for useful discussions. I am grateful to the Organizers of DICE 2006, where this work was presented for the first time, for their kind interest, and encouragement, in particular to Giuseppe Vitiello for discussions and advices.

References

[1] G Gerhard. *The collected papers of Gerhard Gentzen.* Edited by M. E. Szabo. Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Co., Amsterdam, 1969.

[2] M A Nielsen and I L Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[3] G Sambin, G Battilotti, and C Faggian. Basic logic: reflection, symmetry, visibility. *J. Symbolic Logic*, 65(3):979–1013, 2000.

[4] R Josza and N Linden. On the role of entanglement in quantum computational speed-up. arXiv: quant-ph/0201143.

[5] J Y Girard. Linear logic. *Theoret. Comput. Sci.*, 50(1):1–102, 1987.

[6] B Einstein, B Podolsky, and N Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 41(777), 1935.

[7] G Battilotti and G Sambin. Basic logic and the cube of its extensions. In *Logic and foundations of mathematics (Florence, 1995)*, volume 280 of *Synthese Lib.*, pages 165–186. Kluwer Acad. Publ., Dordrecht, 1999.

[8] W K Wootters and W H Zureck. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[9] A K Pati and Braunstein S L. Impossibility of deleting an unknown quantum state. *Nature*, 404:164, 2000. arXiv: quant-ph/9911090.

[10] G Birkhoff and J von Neumann. The logic of quantum mechanics. *Ann. of Math. (2)*, 37(4):823–843, 1936.

[11] J S Bell. *Speakable and unspeakable in quantum mechanics.* Cambridge University Press, Cambridge, 1987. Collected papers on quantum philosophy.

[12] D M Greenberger, M A Horne, A Shimony, and A Zeilinger. Bell's theorem without inequalities. *Amer. J. Phys.*, 58(12):1131–1143, 1990.

[13] P Zizzi. The Liar paradox in Basic logic. to appear.