5th European Congress of Mathematics - Amsterdam, July 14-18 2008

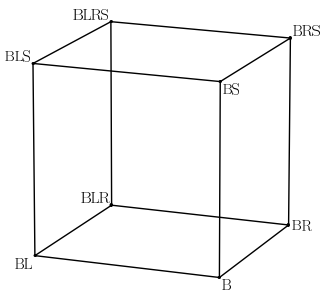
Sequent calculus and quantum parallelism

GIULIA BATTILOTTI
Department of Philosophy, University of Florence, ITALY

Challenge: find an explanation to the quantum computational speed up (due to superposition and entanglement) in terms of logical proofs.

The cube of logics

Basic logic **B** is a core for sequent calculus. Its rules for connectives are given through *metalinguistic links*. It is extended to calculi for well-known logics by the addition of structural rules. This is representable in the following cube:



B = Basic Logic
BL ∼ Linear Intuitionistic **BR** ∼ Dual Linear Intuitionistic
BS ∼ Paraconsistent Quantum
BLS ∼ Intuitionistic **BRS** ∼ Dual Intuitionistic
BLR ∼ Linear
BLRS ∼ Classical

In **B** and **BS** rules have *no context* near active formulae. In logics with "**L**" left contexts are allowed, in logics with "**R**" right contexts are allowed.

We look for a sequent calculus which describes quantum parallelism as a further extension of **B**

Connectives from metalinguistic links

In basic logic we consider the following metalinguistic links between assertions: *yield*, *and*, *forall*.

1. *yield* links two assertions at a different level, in a *sequential* way.
2. *and* links two assertions at the same level, in a *parallel* way.
3. *forall* links assertions with a variable in common. The variable is the reason of the link.

Let us represent assertions by sequents. Then logical connectives and their rules in sequent calculus are the result of importing the links into the object level. This is obtained solving the following definitory equations:

1. $\Gamma \vdash A \to B \quad \equiv \quad \Gamma, A \vdash B$
   $\Gamma, A \vdash B$ represents the sequential link between A and B, in presence of a left context Γ. Then implication $\to$ is a way to import sequentiality and this is possible only in logics with "**L**".
2. $\Gamma \vdash A\&B \quad \equiv \quad \Gamma \vdash A \quad \Gamma \vdash B$
   $\Gamma \vdash A \cdot B \quad \equiv \quad \Gamma \vdash A, B$
   The couple of sequents $\Gamma \vdash A \quad \Gamma \vdash B$ is the *additive* way to represent *and*; the comma in the sequent $\Gamma \vdash A, B$ is the *multiplicative* way to represent the parallel link between A and B.
   Then parallelism is imported in two ways: the additive (by the additive conjunction &) and the multiplicative (by the multiplicative disjunction, here denoted by $\cdot$).
3. $\Gamma \vdash (\forall x \in D)A(x) \quad \equiv \quad \Gamma, z \in D \vdash A(z)$, z not free in Γ
   $\Gamma, z \in D \vdash A(z)$ gathers all assertions $A(z)$ depending on a free variable on the domain D. This is imported by the quantifier $\forall$.
   Since Γ does not depend on z, $\forall$ inherits the features of the additive parallelism, enforced by the common variable.

(Equations corresponding to the additive disjunction $\oplus$, the multiplicative conjunction $\otimes$ and the existential quantifier $\exists$ can be obtained symmetrically).

Additive + multiplicative parallelism

Combining additive and multiplicative parallelism is allowed by the distributive law of multiplicative connectives w.r.t additive connectives. The distributive law $A \cdot (B\&C) = (A\&B) \cdot (A\&C)$ is provable in logics with "**R**". Distributivity is extended to the predicative case as follows:

$$(\forall x \in D_1)A(x) \cdot (\forall x \in D_2)B(x) = (\forall x \in D_1)(\forall y \in D_2)(A(x) \cdot B(y))$$

(classical distributivity).

This requires *independent* variables in A, B. Computational drawback: exponential increasing of complexity in the number of independent variables.

Distributivity with *dependent* variables:

$$(\forall x \in D)A(x) \cdot (\forall x \in D)B(x) = (\forall x \in D)(A(x) \cdot B(x))$$

fails. Reason: **it is false**!!! Computational advantage: no exponential increasing of complexity with dependent variables.

It would be proved by the following parallel rule:

$$\frac{\Gamma, z \in D \vdash A(z), B(z)}{\Gamma \vdash (\forall x \in D)A(x), (\forall x \in D)B(x)} \ \forall\|$$

which fails due to restriction on variables on the right, necessary when formulae can pass from right to left. This does not hold in **B**. So adopting the above rule as such in **B** would be possible, but would cause inconsistency in its extensions.

A new predicative connective

Idea: good = computationally convenient
(in a paraconsistent framework)

To obtain a better $\forall\|$ rule: consider a common variable as a further link.
In $\Gamma \vdash A(z), B(z)$ the comma says also "there is a variable in common, or there used to be a variable in common above in the derivation". So we write $,_z$ for it, and put the definitory equation:

$$\Gamma \vdash A \bowtie B \quad \equiv \quad \Gamma \vdash A,_z B$$

The common link $,_z$ allows the parallel application of the $\forall$-rule:

$$\frac{\Gamma, z \in D \vdash A(z),_z B(z)}{\Gamma \vdash (\forall x \in D)A(x),_z (\forall x \in D)B(x)} \ \forall\|$$

It allows to prove distributivity in the following form:

$$(\forall x \in D)A(x) \bowtie (\forall x \in D)B(x) = (\forall x \in D)(A(x) \bowtie B(x))$$

(Bell's distributivity).

This creates a unique multiplicative-additive quantifier

$$\bowtie_{x \in D} (A(x); B(x))$$

corresponding to $(\forall x \in D)A(x) \bowtie (\forall x \in D)B(x)$ or to $(\forall x \in D)(\forall x \in D)A(x)) \bowtie B(x)$ equivalently.

$\bowtie$ exploits dependent variables and is defined by the equation:

$$\Gamma \vdash \bowtie_{x \in D} (A(x); B(x)) \quad \equiv \quad \Gamma, z \in D \vdash A(z),_z B(z)$$

Substitution of the variable z by a closed term t destroys the $,_z$-link. $\Gamma \vdash A(z),_z B(z)$ becomes $\Gamma \vdash A(t), B(t)$ where the comma is the usual comma of sequent calculus.

Quantum Computational Speed Up

Quantum computational speed up is due to the so called massive quantum parallelism, that is the parallel computation created by the peculiar quantum features of information, namely quantum superposition and quantum entanglement. Quantum superposition is the co-existence, in the same particle, of different states, one of which will be measured.
A quantum unit of information (qubit) is represented by the vector $|q\rangle = a|0\rangle \oplus b|1\rangle$ where a, b are complex numbers (probability amplitudes) s.t. $|a|^2 + |b|^2 = 1$ and $|0\rangle$, $|1\rangle$ are two orthogonal unitary vectors. $|q\rangle$ is then the superposition of the two states $|0\rangle$, $|1\rangle$, where $|0\rangle$ will be measured with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$.
Two qubits are maximally entangled when they are represented by one of the following four states (Bell's states)

$$|q_1 q_2\rangle = 1/\sqrt{2}|00\rangle \pm 1/\sqrt{2}|11\rangle \qquad |q_1 q_2\rangle = 1/\sqrt{2}|01\rangle \pm 1/\sqrt{2}|10\rangle$$

This means that the two states $|0\rangle$ and $|1\rangle$ are equally probable after measurement, and that the measurement of one of the two is determined by the measurement of the other.

Quantum superposition by quantifiers

In probability theory an *experiment* is a random variable Z with an associated probability measure p_Z.

Let $\mathcal{A}$ be a quantum system. A quantum measurement on $\mathcal{A}$ is an experiment, considering the possible outcomes as a random variable. The set of possible outcomes is an orthonormal basis B of the Hilbert space of $\mathcal{A}$. Let $D = D(Z, p_Z) = \{(z, p\{Z = z\} : z \in B\}$ such set. Let Γ a set of hypothesis of the experiment. Of course, they cannot depend on the outcome of the experiment.

The assertion $\Gamma\ z \in D \vdash A(z)$ is "*forall* possible outcomes z in D, in the hyporthesis Γ, the possible result of the measurement of $\mathcal{A}$ is z". Since Γ does not depend on z, we put the equivalence of the definitory equation of *forall*: $\Gamma \vdash (\forall x \in D)A(x) \equiv \Gamma\ z \in D \vdash A(z)$
Then the proposition $(\forall x \in D)A(x)$ represents quantum superposition.

In particular, the derivable sequent $(\forall x \in D)A(x), z \in D \vdash A(z)$ says that the particle described by the proposition $(\forall x \in D)A(x)$ can be found in state z for any z. Substituting z by a *closed* term t, one has that the superposition $(\forall x \in D)A(x)$ is converted into $A(t)$, t corresponding to a fixed element of the orthonormal basis. The other possibilities are lost. This describes a collapse. *Substitution destroys superposition.*

Example: $\mathcal{A}$ a particle, the domain D_Z given by the measurement of the spin of $\mathcal{A}$ along the z axis. D_Z has got two elements: $|\uparrow\rangle$ and $|\downarrow\rangle$ (the two directions of the spin). $(\forall x \in D_Z)A(x)$ represents the superposed state of the two directions of the spin along the z-axis. $(\forall x \in D_Z)A(x) \vdash A(|\uparrow\rangle)$ says that $\mathcal{A}$ is found in the "up" direction along the z-axis.

Quantum entanglement

Let $\mathcal{A}$ and $\mathcal{B}$ be two entangled particles, for example two electrons with opposite spin. The possible result of a measurement of the spin along the z axis, performed on $\mathcal{A}$ or on $\mathcal{B}$, is equally described by the assertion $\Gamma, z \in D_Z \vdash A(z),_z B(z)$.

The corresponding state is then described by the proposition

$$\bowtie_{x \in D_Z} (A(x); B(x)).$$

and we have Bell's ditributivity for entangled particles.
As above, a substitution by a closed term destroys the superposition, hence the entanglement.

Let $\mathcal{C}$ and $\mathcal{D}$ be two separated particles. A possible measurement of $\mathcal{C}$ is described simply by $\Gamma, z \in D_Z \vdash C(z)$. Measurements on both particles are also possible and described by $\Gamma, z \in D, y \in D_Z \vdash C(z), D(y)$, where z and y are independent variables. Measurements on both particles and on different axix (e.g. the z-axis for $\mathcal{C}$ and the y-axis for $\mathcal{D}$) are also possibles and described by $\Gamma, z \in D_Z, y \in D_Y \vdash C(z), D(y)$ (different domains). In both cases, one has classical distributivity with exponential growth of complexity.

Conclusion: entanglement creates Bell's distributivity and inhibits classical distributivity.
From this the quantum computational speed-up.

Alan Turing wrote:

"...if a machine is expected to be infallible, it cannot be also intelligent. There are several theorems [Goedel's incompleteness theorems] which say almost exactly that. But these theorems say nothing about how much intelligence may be displayed if a machine makes no pretence at infallibility."

References

[1] Battilotti, G.: Basic logic and quantum computing: logical judgements by an insider observer, Int. J. of Quantum Information **3**,1 (2005) 105-109. arXiv: quant-ph/0407057.

[2] Battilotti, G., Faggian, C. (2002) Quantum Logic and the cube of Logics, in Handbook of Philosophical Logic, new edition, vol. 6, D. Gabbay and F. Guenthner eds., Kluwer.

[3] Dalla Chiara M.L., Giuntini R., Leporini R., (2003) Quantum Computational Logics: a survey. in V. F. Hendricks, J. Malinowski (eds.), Trends in Logic: **50** Years of Studia Logica, Kluwer Academic Publishers, 213–255

[4] Dalla Chiara M.L., Giuntini R., Leporini R., (2006) Compositional and Holistic Quantum Computational Semantics, Natural Computing.

[5] Girard, J. Y.: Linear Logic, Theoretical Computer Science **50**(1987) 1-102.

[6] Maietti, M.E., Sambin, G.: Toward a minimalist foundation for constructive mathematics, in: From Sets and Types to Topology and Analysis: Towards Practicable Foundations for Constructive Mathematics" (L. Crosilla, P. Schuster, eds.), Oxford UP, to appear.

[7] Sambin, G., Battilotti, G. and Faggian, C. (2000) Basic Logic: Reflection, Symmetry, Visibility, The Journal of Symbolic Logic **65**, 979–1013.