High Level Quantum Structures in Linguistics and Multi Agent Systems

Mehrnoosh Sadrzadeh
School of Electronics and Computer Science
University of Southampton
ms6@ecs.soton.ac.uk

Abstract

We present two applications to AI of recently introduced high level quantum structures. These structures are the categorical quantum logic of (Abramsky & Coecke 2004) and the quantale quantum logic of (Coecke, Moore, & Stubbe 2001). Firstly, we show how the diagrammatic toolkit of categorical quantum logic, when restricted to its pregroup fragment (Lambek 1999; 2001), simplifies analysis of sentence structure of different languages. Moreover, the quantitative values that arise in these diagrams signify different degrees of complexity of sentences, which turn out to vary for different languages. Secondly, we show how expanding the quantale quantum logic with epistemic modalities provides a powerful system to reason about information update in multi-agent systems. Finally, we indicate how the above two applications to non-quantum domains can themselves be 're-quantized', providing applications to quantum informatics of distributed systems.

Key words: Computational linguistics, Information update in multi-agent systems, High level quantum structures.

Introduction

Recently there have been intriguing results and developments in AI related fields that use methods originating in the study of quantum mechanics. The use of Hilbert space concepts such as Hermitian operators, trace and (Birkhoff & von Neumann 1936)-style quantum logics in *information retrieval* can be found in (van Rijsbergen 2004). In this context, the main benefit of the quantum mechanical structure is that it combines logic with vector space models and at the same time relaxes the distributive constraints of classical logic. Combining logical and quantitative methods turns out to be of importance in *natural language processing* (Gazdar 1996) where similar quantum mechanical concepts prove to be useful (Widdows 2004). A recent proposal in (Clark & Pulman 2006) makes particular use of the Hilbert space tensor product, which is the quantum mechanical description of compound quantum systems. The existence of a conference which focusses on applications of quantum mechanical methods in AI, at which this work will be presented, indicates the emergence of a new scientific community.

In this paper we present two 'non-quantum' applications of recently developed logics that govern behavior of quantum mechanisms. These applications are in the fields of:

- computational linguistics (Lambek 1999; 2001)
- information-update in multi-agent systems (Baltag, Coecke, & Sadrzadeh 2004; Sadrzadeh 2006a)

Moreover, while these applications live outside the quantum domain, we strongly feel that they 're-applied' within the field of quantum informatics.

The next section, in which we discuss the application to computational linguistics, makes use of the diagrammatic toolkit developed for the categorical quantum logic of (Abramsky & Coecke 2004). This logic, in contrast to other quantum logics, was developed to capture compound quantum systems. Hence it axiomatises the Hilbert space tensor product. Initially we only use the 'purely qualitative' pregroup fragment of this logic for the analysis of sentences in natural languages. Then we introduce 'quantities' which are meaningful when comparing different languages.

In the third section, we make use of the quantale quantum logic of (Coecke, Moore, & Stubbe 2001) to reason about information update. For this purpose, we need to enrich the quantale setting with operators whose adjoints stand for knowledge of agents. The dynamics is encodes in the same way as in the quantum case, that is as the weakest precondition of actions. The resulting family of adjunctions provide us with a strong deductive power: we need neither distributivity nor negation to reason about the classical scenarios of multi-agent systems.

In the fourth section, we discuss an interesting parallel between the development of mathematical models in computational linguistics and high level quantum structures. Finally, in the last section we show how our information update setting can be used to model quantum protocols by encoding and reasoning about a simplified version of Ekert'91 protocol (Ekert 1991). We end by discussing how the decision procedure of pregroups is useful in automating verification and derivation of quantum protocols.

Pregroup analysis of sentence structure

The first application is syntactical analysis of human languages using pregroups, a recent development of Lambek (Lambek 1999; 2001). Pregroups are replacements for

Lambek Calculus (Lambek 1958), widely used as type categorial grammars (Moortgat 1997) in computational linguistics. They have been applied to many languages, for example English (Lambek 2004), French (Bargelli & Lambek 2001b), Arabic (Bargelli & Lambek 2001a), Italian (Casadio & Lambek 2001), and recently by the author to Persian (Sadrzadeh 2006b). One advantage of this system, over type categorial grammars, is that the analysis is done linearly and in one dimension, rather than in 'page filling trees'.

Similar to type categorial grammars, the analysis starts by fixing some basic linguistic types and partial orders between them. We then freely generate a pregroup[1] of these types denoted as

$$(P, \leq, \cdot, (-)^l, (-)^r)$$

This is a partially ordered monoid where each type has a left and a right adjoint. That is, we have the following inequalities for a type $p \in P$ and its adjoints $p^l, p^r \in P$

$$p^l \cdot p \leq 1 \leq p \cdot p^l, \qquad p \cdot p^r \leq 1 \leq p^r \cdot p$$

The unit of juxtaposition, that is 1, is the empty type, which is self adjoint. So for $p \in P$ we have

$$1 \cdot p = p \cdot 1 = p, \qquad 1^l = 1^r = 1$$

Examples of the starting types are the following

- π for pronoun,
- s for declarative statement,
- q for yes-no question,
- i for infinitive of the verb,
- o for direct object.

For when the person of the pronoun and tense of the verb matters, we also have $\pi_j, s_k, q_k \in P$ for j'th person pronoun and k'th tense sentence and question. We require the following partial orders

$$\pi_j \leq \pi \qquad s_k \leq s \qquad q_k \leq q$$

The adjoints and juxtapositions of these types are used to form the compound types. One assigns a type to each word in a sentence and then uses the monoid multiplication for juxtaposition of these types. The juxtaposition of adjacent adjoint types causes reduction to 1. This process is repeated until no more reduction is possible and a type is returned as the main type of the juxtaposition. If this type is the desired type (e.g. s for statement and q for question), the juxtaposition is a grammatical sentence. It has been shown in (Buszkowski 2001) that this procedure is decidable. Thus we obtain a decision procedure to determine if a given sentence of a language is grammatical or not.

For simplicity, we use an arrow → for ≤ and drop the · between juxtaposed types. For the sample sentence 'He likes her', we have the following type assignment

He	likes	her
π_3	$(\pi^r s o^l)$	o

Since $\pi_3 \to \pi$ and juxtaposition is order preserving, we obtain the following reduction

$$\pi_3(\pi^r s o^l)o \to \pi(\pi^r s o^l)o$$

Now by $\pi\pi^r \to 1$ and $o^l o \to 1$, we obtain

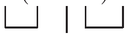
$$\pi(\pi^r s o^l)o \to 1s1 = s$$

The desired reduction for the whole sentence is as follows

$$\pi(\pi^r s o^l)o \to s$$

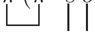
The reduction can be done diagrammatically by drawing a vertical line for each type and connecting the adjoint type that cancel each other by a horizontal line. For example, for the above reduction we have the following diagram

$$\pi\,(\pi^r\, s\, o^l)\, o$$



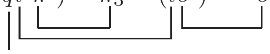
This diagram only has one vertical line of type s, so the sentence is of the type statement and grammatical. A non-grammatical example would be 'He likes' with the following diagram

$$\pi\,(\pi^r\, s\, o^l)$$



Here we have two vertical lines and thus the phrase is of type so^l and not a sentence. As another example consider the analysis of the yes-no question 'Does he like her?'. We assign the compound type (io^l) to the infinitive of the transitive verb and $(qi^l\pi^l)$ to the question word 'does' and get the following reduction

Does	he	like	her?	→	question
$(qi^l\pi^l)$	π_3	(io^l)	o	→	q

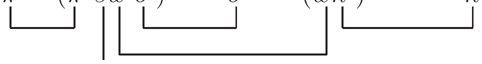


In these examples there are no ambiguities, but in more complex examples the diagram is of essential help in demonstrating the order of reductions. For more on pregroups see (Lambek 1999; 2001).

Comparing different languages. The same procedure is followed for analyzing the sentence structure of different languages. The reduction diagrams can be used for comparing their sentence structures. Based on (Sadrzadeh 2006b), we fix a sample sentence and reduce it in English, French, Arabic, Hebrew, Hindi, and Persian. The interesting observation is that languages that have the same roots follow the same reduction patterns.

Consider our previously fixed types and the sentence 'he bought a book from the bookshop'. Leaving out the person, tense, and details of determinate nouns, we get the following reduction for our sample sentence in English

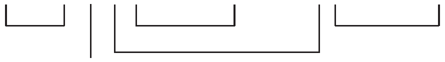
He	bought	a book	from	the bookshop.
π	$(\pi^r s w^l o^l)$	o	(wn^l)	n



A similar sentence in French has exactly the same reduction

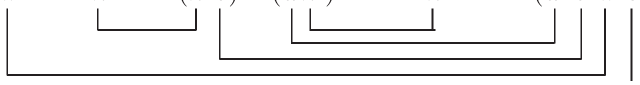
Il	a acheté	un livre	dans	la librairie.
π	$(\pi^r s\, w^l o^l)$	o	wn^l	n

[1] Instead of generating a residuated partially ordered monoid for a type categorial grammar.



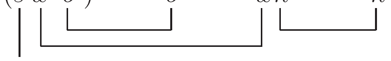
Persian has a very different pattern

he	the book		from	bookshop	bought
u	ketab	ra	az	ketabkhaneh	kharid
π	n	$(n^r o)$	(wn^l)	n	$(w^r o^r \pi^r s)$

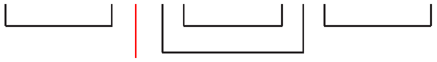


For the same sentence in Arabic the reduction is as follows

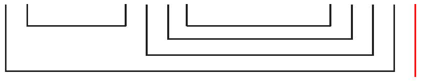
bought	the book	from	the shop
Yashtari	ketaban	men	alsogh.
$(s\, w^l\, o^l)$	o	wn^l	n



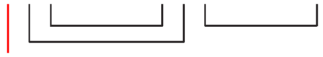
It turns out that the reduction patterns of Persian and Hindi are similar, where as Arabic is closer to Hebrew[2]. The reduction pattern of English and French sentences is



Compare this to the reduction pattern of the Persian and Hindi sentences



Arabic and Hebrew have yet a different reduction pattern



Degree of nesting. We introduce three numbers for the reduction pattern of a sentence. The first one is the number of times a map of the sort $pp^r \to 1$ or $p^l p \to 1$ is applied. It can easily be determined by counting the horizontal lines of the reduction diagram. For example this number for the above English and French sentences is 4, for the Persian sentence it is 5. The second number is less than or equal to the first one and stands for the maximum of the number of nestings of these maps. For instance, this number for our English, French, Arabic and Hebrew sample sentences is 2, and for Persian it is $max\{2,4\} = 4$. These degrees provide us a with a quantitative way of measuring the complexity of sentences and are connected to the *chunks of information* discussed in (Lambek 2004), that is, the number of unprocessed tokens while parsing a sentence. For a discussion about these chunks in English sentences, see (Lambek 2004). In my analysis of Persian grammar, I analyzed one of the Rubayyat of Omar Khayyam with a degree of nesting of 5. The most complicated sentence I could produce was a compound one with multiple subjects and objects and a compound verb; this had a degree of nesting of 9.

Information-update in multi-agent systems.

The second application is modeling information flow in interactive multi agent systems where agents communicate and as a result their information gets updated. We present the model developed in (Baltag, Coecke, & Sadrzadeh 2004; Sadrzadeh 2006a), which is the first algebraic semantics in the area, and is moreover equipped with a complete sequent calculus. Our model is more general by being non-Boolean and non-distributive, and subsumes the usual relational models (Fagin *et al.* 1995; Baltag, Moss, & Solecki 1999) . The reasoning power is compensated by a logic of actions and the epistemic and dynamic modalities that arise via adjunction. This simple setting solves complicated multi-agent scenarios that involve updates by higher order reflective announcements, such as the muddy children puzzle. The proofs of these scenarios are much simpler than in the relational Kripke structure models of knowledge.

Our mathematical structure is a pair (M, Q) consisting of a quantale $(Q, \bigvee, \bullet, 1)$ of communication actions and its right module $(M, \bigvee)$ of propositions. The join and multiplication of the quantale stand for non-deterministic choice and sequential composition of actions. The join in the module stands for logical disjunction. Both are endowed with a family of join preserving endomorphisms $f_A = (f_A^M, f_A^Q)$, indexed over the set of agents $A \in \mathcal{A}$. Each such map encodes appearance of an agent about actions f_A^Q and propositions f_A^M. For the latter we have

> $f_A^M(m)$ stands for all the propositions that agent A considers possible whenever m holds in the 'real world'.

Two extreme cases are

- $f_A^M(m) = \top$ corresponding to absence of any information.
- $f_A^M(m) = m$ corresponding to correct information.

We can also model incorrect information, e.g. when $m \leq m'$ but $f_A(m) \not\leq m'$ or the other way around. If for $m, m' \in M$ we have $f_A^M(m) < f_A^M(m')$ then agent A possesses strictly more information on m than on m'. A similar interpretation holds for the actions.

> $f_A^Q(q)$ stands for all the actions that agent A considers as happening, when in reality action q is happening.

The appearance maps allow to accommodate misinformation actions such as the following

- Information hiding or encryption by $q < f_A^Q(q)$,
- Lying, cheating and deceit by $q \not\leq f_A^Q(q)$.

The right Galois adjoints to these maps $(\Box_A^M, \Box_A^Q)$ encode knowledge or information of agents, the adjunction is denoted as

$$(f_A^M, f_A^Q) \dashv (\Box_A^M, \Box_A^Q)$$

for which we have the following

$$f_A^M(m) \leq m' \quad \leftrightarrow \quad m \leq \Box_A^M m'$$
$$f_A^Q(q) \leq q' \quad \leftrightarrow \quad q \leq \Box_A^Q q'$$

[2] No publication on pregroup analysis has been reported for Hindi and Hebrew. The similarity is deduced from working out examples.

From this it follows that the box modality is monotone and preserves all meets. That is, we have the following for $\Box_A^M$ and similar ones for $\Box_A^Q$.

$$\begin{array}{c} m \leq m' \text{ implies } \Box_A^M m \leq \Box_A^M m' \\ \Box_A^M \bigwedge_i m_i = \bigwedge_i \Box_A^M m_i \\ \Box_A^M \top = \top \end{array}$$

These are the properties of a normal modality (Fagin *et al.* 1995) and thus we interpret $\Box_A$ as our **knowledge modality** with the following reading

- $\Box_A^M m$: agent A knows/believes that proposition m is true.
- $\Box_A^Q q$: agent A knows/believes that action q is happening.

This covers both knowledge and belief: in contexts where no wrong belief is allowed, we read it as knowledge or *justified true belief*, and otherwise, as *justified belief*.

Information update is modeled by the action of quantale on the module

$$- \cdot - : M \times Q \to M$$

for which we have join preservation on both arguments and the following axioms

$$\begin{array}{rcl} m \cdot 1 & = & m \\ (m \cdot q_1) \cdot q_2 & = & m \cdot (q_1 \bullet q_2) \end{array}$$

The right Galois adjoint to update is $[q]m$, for which we have

$$m \cdot q \leq m' \leftrightarrow m \leq [q]m'$$

This stands for the **dynamic modality** of PDL (Harel, Kozen, & Tiuryn 2000) and the **weakest precondition** of Hoare Logic (Hoare & Jifeng 1987).

The combination of epistemic and dynamic modalities is used to model *learning* of agents after actions, by deriving propositions of the following form

$$[q]\Box_A m$$

We read this as after action q agent A knows that proposition m holds. In order to derive such propositions from our assumptions, we need the following *suspicion* inequalities

$$\begin{array}{rcl} 1 & \leq & f_A^Q(1) \\ f_A^Q(q \bullet q') & \leq & f_A^Q(q) \bullet f_A^Q(q') \\ f_A^M(m \cdot q) & \leq & f_A^M(m) \cdot f_A^Q(q) \end{array}$$

The first inequality enables us to accommodate suspicions: even when nothing is happening one could still suspect that something hidden might be happening, for example we can have $f_A^Q(1) = 1 \vee q$. Suspicions are important for applications to protocol security, see ch. 5 of (Sadrzadeh 2006a)for details. The other two inequalities ask for a rationality condition on appearance of sequential composition and update. Their laxity is imposed by the first inequality as follows

$$f_A^Q(q \bullet 1) = f_A^Q(q) = f_A^Q(q) \bullet 1 \leq f_A^Q(q) \bullet f_A^Q(1)\,.$$

$$f_A^M(m \cdot 1) = f_A^M(m) = f_A^M(m) \cdot 1 \leq f_A^M(m) \cdot f_A^Q(1)\,,$$

The triple $(M, Q, \{f_A\}_{A \in \mathcal{A}})$ together with suspicion axioms is called an *epistemic system*, for details see (Baltag, Coecke, & Sadrzadeh 2004; Sadrzadeh 2006a).

Concrete examples. The actions of our multi-agent scenarios are partial actions, that is, they have preconditions and thus cannot be applied to all the propositions. Whenever $m \cdot q = \bot$ we say q cannot be applied to m. To represent these, we define a *kernel* for each action $q \in Q$ as follows

$$Ker(q) := \{m \in M \mid m \cdot q = \bot\},$$

This is the weakest proposition to which the action cannot be applied, that is $Ker(q) = [q]\bot$.

Examples are public and private refutations of propositions. A public refutation of the proposition $m \in M$ is an action $q \in Q$ with $f_A^Q(q) = q$ for all $A \in \mathcal{A}$ and for which $Ker(q) = \downarrow m$. A private refutation to a subgroup is another action that privately refutes m to the subgroup β of agents. In this case $Ker(q)$ is the same as above and $f_A^Q(q) = q$ for $A \in \beta$ and $f_A^Q(q) = 1$ otherwise.

In each scenario, we have a non-epistemic part, referred to as *facts*. These are propositions that are stable under any epistemic action: if they are true before running q, they will remain true afterwards. These are defined as the *stabilizer* of Q

$$Stab(Q) := \{\phi \in M \mid \forall q \in Q\,, \phi \cdot q \leq \phi\}.$$

The muddy children puzzle with honest children is a paradigmatic example in the standard epistemic logic literature, e.g. (Fagin *et al.* 1995). We encode and solve it using the setting of an epistemic system. The puzzle goes like this: n children are playing in the mud and $k \leq 1$ of them have dirty foreheads. Their father announces: 'at least one of you has a dirty forehead', and then starts asking 'do you know that it is you who has a dirty forehead?'. The children think and if they are honest and $k > 1$, they all reply at the same time 'no!', the rounds of no answers repeat until the dirty ones know that they are dirty. We show that for honest children, after $k - 1$ rounds of refutations, child j for $1 \leq j \leq k$ knows that he is dirty.

However, if the children are not honest and cheat or lie in their replies, other interesting properties can be proven. These cases have not been considered, and cannot be formally dealt with, in the standard approaches to epistemic logic. The more recent dynamic epistemic logic of (Baltag, Moss, & Solecki 1999) offers formal proofs of these cases in a Boolean setting. Our algebra proves these in a much simpler axiomatic way in its non-boolean and non-distributive setting.

We encode the puzzle in an epistemic system as follows. The set of agents $\mathcal{A}$ includes the children $C_1, \cdots, C_n$ where the first k, for $1 \leq k \leq n$, are dirty. The module M includes all possible initial propositions s_β where $\beta \subseteq \mathcal{A}$ and its elements are those children who have mud on their foreheads. So $s_{C_1, \cdots, C_k}$ is the "real state" in which $C_1, \cdots, C_k$ are dirty and $C_{k+1}, \cdots, C_n$ are clean. Since the children cannot see their own foreheads (which might either be dirty or not) we have

$$f_{C_i}^M(s_\beta) = s_{\beta \setminus \{C_i\}} \vee s_{\beta \cup \{C_i\}}\,.$$

We also need the following facts

- $D_\emptyset$ for the fact that no child has a dirty forehead

- D_i for the fact that the i'th child has a dirty forehead
- $\bar{D}_i$ for the fact that the i'th child has a clean forehead

Hence we have:

$$\{D_\emptyset\} \cup \{D_i, \bar{D}_i \in M \mid C_i \in \mathcal{A}\} \subseteq Stab(Q)\,.$$

For the propositions and facts we have $s_\beta \leq D_i$ for all $C_i \in \beta$, $s_\beta \leq \bar{D}_i$ for all $C_i \notin \beta$, and $s_\emptyset \leq D_\emptyset$, which sets that each proposition satisfies the corresponding fact. A round of all children's "no" answers is a public refutation q with

$$Ker(q) = \downarrow \bigvee_{i=1}^{i=n} \Box_{C_i} D_i$$

Father's first announcement is a public refutation q_0 with

$$Ker(q_0) = \downarrow D_\emptyset$$

A cheating action, for example between children 2 to k, is a private refutation π with

$$Ker(\pi) = \downarrow \bigvee_{i=1}^{k} \bar{D}_i$$

A lying actions, for example of child 1 lying to the rest about him knowing that he is dirty, is an action $\bar{q}$ with

$$Ker(\bar{q}) = \downarrow (\Box_{C_1} \bar{D}_1 \vee \bigvee_{i=2}^{n} \Box_{C_i} D_i)$$

The lier child knows that he is lying, that is $f^Q_{C_1}(\bar{q}) = \bar{q}$. But all the others $2 \leq i \leq n$ think he is telling the truth, that is $f^Q_{C_i}(\bar{q}) = q$. One can similarly, encode actions of mixed rounds of yes and no answers. We denote by q' a round of yes answers of children 2 to k and no answers of the rest.

Using the above encoding, we prove the following inequalities for $1 \leq j \leq k$ and $k+1 \leq j' \leq n$. The first inequality is for the case when the children are honest, the second and third ones are for the cases when children 2 to k cheat and secretly tell each other that they are dirty. and the last one covers the case when child 1 lies in his reply.

Propositions.

$$\begin{aligned}
s_{\{C_1,\cdots,C_k\}} &\leq [q_0\,(\bullet q)^{(k-1)}]\Box_{C_j} D_j && (1)\\
s_{C_1,\ldots,C_k} &\leq [q_0(\bullet q)^{k-2} \bullet \pi \bullet q']\Box_1 \bar{D}_1 && (2)\\
s_{C_1,\ldots,C_k} &\leq [q_0(\bullet q)^{k-2} \bullet \pi \bullet q']\Box_{j'} \bot && (3)\\
s_{\{C_1\}} &\leq [q_0 \bullet \bar{q}]\Box_{C_j} D_j && (4)
\end{aligned}$$

where $(\bullet q)^{(k-1)}$ denotes $q \bullet \cdots \bullet q$ with $k-1$ occurrences of q.

Proofs. All the proofs are done by by induction on the number k of dirty children. They all start by moving the dynamic modalities from the right hand side to the left had side by adjunction. For example the first inequality is equivalent to the following by the dynamic adjunction

$$s_{\{C_1,\cdots,C_k\}} \cdot q_0\,(\cdot\, q)^{(k-1)} \leq \Box_{C_j} D_j$$

This is equivalent to the following by the epistemic adjunction

$$f_{C_j}\left(s_{\{C_1,\cdots,C_k\}} \cdot q_0\,(\cdot\, q)^{(k-1)}\right) \leq D_j$$

Now distribute the f_{C_j}, replace it with its assumed values, and apply the suspicion inequality. It then suffices to prove the following two case

$$\begin{cases} s_{\{C_1,\cdots,C_k\}} \cdot q_0\,(\cdot\, q)^{(k-1)} \leq D_j \\ s_{\{C_1,\cdots,C_k\}\setminus\{C_j\}} \cdot q_0\,(\cdot\, q)^{(k-1)} \leq D_j\,. \end{cases}$$

To show that the first case holds for all k, we update both sides of our assumption $s_{\{c_1,\cdots,c_k\}} \leq D_j$ by $q_0\,(\cdot\, q)^{(k-1)}$ and get

$$s_{\{C_1,\cdots,C_k\}} \cdot q_0\,(\cdot\, q)^{(k-1)} \leq D_j \cdot q_0\,(\cdot\, q)^{(k-1)}$$

What we want follows since we have $D_j \cdot q_0\,(\cdot\, q)^{(k-1)} \leq D_j$ by $D_j \in Stab(Q)$. The second case is proven by proceeding the induction. The cheating and lying inequalities are proven similarly. We refer the reader for details of these proofs to (Baltag, Coecke, & Sadrzadeh 2004; Sadrzadeh 2006a).

In the curious case of the third inequality, the clean children will believe in the falsum, since what they see and hear are contradictory. They see k dirty children, but hear their yes answer in round $k-1$, as opposed to round k. They can be saved from their confusion, by either making them suspect the cheating action, that is assume $f^Q_{j'}(\pi) = \pi \vee 1$ to start with. Another option would be to axiomatize a *revision* operator in the setting and let the agents *revise* their beliefs after such situations. The latter option has been pursued in a joint paper of the author with A. Baltag (Baltag & Sadrzadeh 2006).

Pregroups, quantales and quantum logic

Quantales were initially introduced by Mulvey as a *quantum* (i.e. *non-commutative*) counterpart to locales, which are complete Heyting algebras or indeed intuitionistic logics[3]. Later quantales were used as a dynamic counterpart to the 'static' Birkhoff-von Neumann style quantum logic by Coecke et al. (Coecke, Moore, & Stubbe 2001). Their setting is based on a pair consisting of a quantale and its right module (M, Q). The non-distributive M is the lattice of closed subspaces of a Hilbert space and stands for properties of a quantum system. The quantale Q contains quantum actions such as measurements and unitaries. The binary operation of Q on M is the update of the property of a system by a quantum action. Given that the property $b \in M$ is true after applying projector $P_a \in Q$, the possible initial states which the system had before applying P_a, can be computed using the right Galois adjoint P^*_a to action of projector defined as

$$P^*_a(b) := \bigvee \{c \in M \mid P_a(c) \leq b\}$$

The adjunction $P_a \dashv P^*_a$ provides a **causal duality** and P^*_a stands for the **weakest causes** with respect to the projector

[3] For locales and localic topology see (Johnstone 1982). The reason why one would prefer generalized localic topology rather that point-set topology is because it brings the logical properties of a topological space to the forefront.

action. That is the join of all the initial states on which applying P_a will guarantee b to be true. $P_a^*(b)$ is also referred to as the **Sasaki hook**, for which we can set

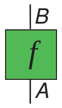
$$a \Rightarrow_S b := P_a^*(b)$$

Although this new setting brought dynamics and operationalism to quantum logic, it suffered from a usual draw back: dealing with combined systems.

The coincidence is that quantales were also the structures considered by Lambek, even before the name quantale was coined, for analyzing the structure of natural languages (Lambek 1958). In his early work, Lambek used a partially ordered residuated monoid $(M, \leq, \bullet, \rightarrow, \leftarrow)$ with two adjoint binary operations, rather than the two unary ones in a pregroup. This led to the widely studied Lambek Calculus and type categorial grammars and has also been the precursor of Linear Logic (Girard 1987), a resource-sensitive logic much used and favored in Computer Science.

In a surprising turn of events, both of the above mentioned parties, that is Coecke and Lambek, independently abandoned the quantale logic for an even more intriguing mathematical structure, namely *compact closed categories*. This structure overcomes the weakness of other quantum logics by introducing a *tensor logic* and picture calculus to reason about combined systems in a categorical framework (Abramsky & Coecke 2004; Abramsky & Duncan 2006). In linguistics, this logic[4] is known and studied as *compact bilinear logic* (Buszkowski 2001)[5].

In a nutshell, in the tensor logic formulas are types of quantum systems $A, B, \cdots$ and proofs are operations performed on these systems $f, g, \cdots$. The notation $A \xrightarrow{f} B$, depicted in picture calculus as



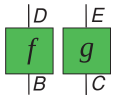
reads as 'B is derivable from A by performing the operation f'. The logic has a binary logical connective for the tensor product of two systems $A \otimes B$ that extends to proofs. So if we obtain systems D and E by, respectively, doing f and g on B and C, that is

$$B \xrightarrow{f} D \qquad C \xrightarrow{g} E$$

then we can combine B and C and do f and g in parallel to obtain the combination of D and E, that is

$$B \otimes C \xrightarrow{f \otimes g} D \otimes E$$

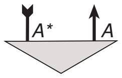
depicted as

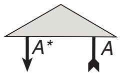


There is also a unary connective $(-)^*$ that represents the adjoint or dual of a type. This satisfies the following axioms

$$\eta \colon 1 \rightarrow A^* \otimes A \qquad \epsilon \colon A^* \otimes A \rightarrow 1$$

and is depicted as





The constant 1 is the unit of tensor, that is

$$1 \otimes A \cong A \otimes 1 \cong A$$

A pregroup is a compact closed category with a non-commutative tensor in an obvious way: formulas (objects) are the linguistic types and proofs (morphisms) are partial orders, so no explicit proof is provided for the derivations. Non-commutativity of tensor requires having left and right ϵ and η maps, one for each adjoint. For example for a pregroup P and $p \in P$ we have the following ϵ maps

$$\epsilon_r \colon p \otimes p^r \rightarrow 1, \qquad \epsilon_l \colon p^l \otimes p \rightarrow 1$$

The linguistic reduction diagrams are special cases of the diagrams of (Abramsky & Coecke 2004) that only use the ϵ triangles.

Re-application to quantum informatics

Agents in quantum protocols. Our *epistemic systems* can be used to reasoning about quantum informatic protocols. Given an epistemic system $(M, Q, \{f_A\}_{A \in \mathcal{A}})$, we assume the non-distributive lattice M contains properties of (finitely many) quantum systems and the quantale Q contains quantum actions. The dynamic and the epistemic modalities, respectively, stands for the weakest precondition and knowledge of agent involved in a quantum protocol. Our notation is an extension of measurement calculus (Danos, Kashefi, & Panangaden 2005) with agent contexts.

We model and reason about a simplified non-probabilistic version of the Ekert'91 protocol (Ekert 1991)[6]. It goes like this: A and B share a Bell pair on qubits 1 and 2. They randomly choose a basis Z or X by, for example, flipping a coin. Then, they send their measurement basis to each other over a safe classical channel. If the received basis is the same as their chosen basis, they share a secret, namely, the result of the measurement; otherwise they start over again.

We denote the action of agents A and B share a Bell pair on qubits 1 and 2 by $B_{1,2}^{A,B}$. The action of agent A measuring bit i in basis $j \in \{Z, X\}$ is denoted by $M_i^{j,A}$. The result of such a measurement is expressed in the fact R_i^j. So we have

$$B_{1,2}^{A,B}, M_i^{j,A}, M_i^{j,B} \in Q, \qquad R_i^j \in Stab(Q)$$

We impose a *Bell axiom* as follows

$$\top \leq [B_{1,2}^{A,B}.M_1^{j,A}.M_2^{j,B}](R_1^j \wedge R_2^j)$$

This says that after the sharing and measuring actions on the same basis, the results will hold. When A and B share a Bell pair, they are aware of it, that is

$$f_A(B_{1,2}^{A,B}) = f_B(B_{1,2}^{A,B}) = B_{1,2}^{A,B}$$

[4] That is without the dagger operation of (Abramsky & Coecke 2004) that yields a strongly compact closed category.

[5] This is a special case of Linear Logic where tensor and par coincide.

[6] An earlier attempt has been presented in (Sadrzadeh 2005)

Similarly, each agent is aware of the measurements he makes, but he is not aware of the measurements made by other agents. For example we have the following for A

$$f_A(M_i^{j,A}) = M_i^{j,A}, \qquad f_A(M_i^{j,B}) \neq M_i^{j,B}$$

The non-deterministic choice of basis is encoded in the following appearance maps for each agent

$$f_A(M_2^{j,B}) = M_2^{Z,B} \vee M_2^{X,B},\ f_B(M_1^{j,A}) = M_1^{Z,A} \vee M_1^{X,A}$$

We use a private announcements $j!_{A,B} \in Q$ to encode the action of communicating the basis. A run of the protocol is the following sequential composition α

$$B_{1,2}^{A,B} \bullet (M_1^{Z,A} \vee M_1^{X,A}) \bullet (M_2^{Z,B} \vee M_2^{X,B}) \bullet (Z!_{A,B} \vee X!_{A,B})$$

It is easy to show that A and B share a secret after a successful run of the protocol: by proving the following two inequalities for A and two similar ones for B. The first one says that agent A knows the result of his measurement, and the second one that he learns the result of B's measurement after communication.

Proposition.

$$\top \;\leq\; [\alpha]\Box_A R_1^Z \vee \Box_A R_1^X \qquad (5)$$
$$\top \;\leq\; [\alpha]\Box_A R_2^Z \vee \Box_A R_2^X \qquad (6)$$

Proof. We provide proof of the second inequality, which is more interesting. After applying the dynamic adjunction, distributing the joins, discarding the unsuccessful and impossible runs, we need to show the following two cases for each basis

$$\top . B_{1,2}^{A,B} . M_1^{Z,A} . M_2^{Z,B} . Z!_{A,B} \;\leq\; \Box_A R_2^Z$$
$$\top . B_{1,2}^{A,B} . M_1^{X,A} . M_2^{X,B} . X!_{A,B} \;\leq\; \Box_A R_2^X$$

Both cases are proven similarly. Consider the first one, after applying the epistemic adjunction and by the suspicion inequality it is enough to show the following

$$f_A(\top) . f_A(B_{1,2}^{A,B}) . f_A(M_1^{Z,A}) . f_A(M_2^{Z,B}) . f_A(Z!_{A,B}) \leq R_2^Z$$

Since $f_A(\top) \leq \top$ and by our assumptions, it is enough to show the following

$$\top . B_{1,2}^{A,B} . M_1^{Z,A} . (M_2^{Z,B} \vee M_2^{X,B}) . Z!_{A,B} \leq R_2^Z$$

We need to show both cases of the disjunction, proven similarly. For example consider the first case, we start from the Bell axiom

$$\top . B_{1,2}^{A,B} . M_1^{Z,A} . M_2^{Z,B} \leq R_2^Z$$

and update both sides with $Z!_{A,B}$

$$\top . B_{1,2}^{A,B} . M_1^{Z,A} . M_2^{Z,B} . Z!_{A,B} \leq R_2^Z . Z!_{A,B}$$

since the result of measurement is a fact, these updates have no effect on it, that is

$$\top . B_{1,2}^{A,B} . M_1^{Z,A} . M_2^{Z,B} . Z!_{A,B} \leq R_2^Z . Z!_{A,B} \leq R_2^Z$$

and we are done.

Secrecy is derived by proving that the above inequalities do not hold for an intruder agent I. That is, the following holds for A's qubit and we have a similar one for B's qubit. Proofs are similar to the above.

Proposition.

$$\top \not\leq [\alpha]\Box_I R_1^Z \vee \Box_I R_1^X$$

We can also reason about the usual attack to this protocol. This happens when agents A and B think that they share a Bell pair, but in reality it is the intruder I that shares the Bell pair with B. So the real action $B_{1,2}^{B,I}$ appears as $B_{1,2}^{A,B}$ to A and B. That is,

$$f_A(B_{1,2}^{B,I}) = f_B(B_{1,2}^{B,I}) = B_{1,2}^{A,B}$$

In this case after the protocol α', agents A and B think that they share a secret, but they are wrong! We can show the following inequality for A and a similar one for B

Proposition.

$$\top \leq [\alpha'] \Box_A R_2^Z \vee \Box_A R_2^X$$

where α' is as follows

$$B_{1,2}^{B,I} \bullet (M_1^{Z,A} \vee M_1^{X,A}) \bullet (M_2^{Z,B} \vee M_2^{X,B}) \bullet (Z!_{A,B} \vee X!_{A,B})$$

But this is wrong, since in reality we only have the following inequality

$$\top . B_{1,2}^{B,I} . M_1^{j,B} . M_2^{j,I} \leq R_1^j \wedge R_2^j$$

where as A's knowledge is based on the following

$$\top . B_{1,2}^{A,B} . M_1^{j,A} . M_2^{j,B} \leq R_1^j \wedge R_2^j$$

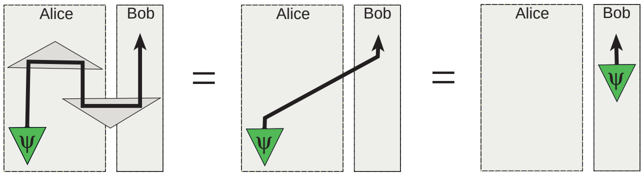
Decision procedures. In the pregroup analysis, we assign to each sentence the juxtaposition of its types α. Our aim is to show that the sentence is grammatical by showing that α reduces to the desired type x of the sentence. This is done by verifying that the chain of reductions

$$\downarrow\!\alpha \;:=\; \alpha \to \cdots \to \gamma$$

returns a type equal to x. One can look at each language phrase as a pair (α, x), and say that the phrase is grammatical if and only if $\downarrow\!\alpha = x$. Pictorially and for example for deciding if the sentence 'He likes her' is grammatical, we have to check the following equality

$$\sqcup \;\mid\; \sqcup \;\;=\;\; \mid$$

The existence of a decision procedure ensures that this procedure always terminates. The analogy to quantum information is established by looking at a protocol as a pair, consisting of its full description as a composition of operations, and its desired functionality. For instance, for the correctness of the teleportation protocol with input state ψ, we have to verify the following equality



According to this picture, the protocol pair is (α, ψ) with

$$\alpha := (\epsilon \otimes 1) \circ (1 \otimes \eta) \circ \psi$$

In the quantum case, the decision procedure becomes worth investigating since the category is not thin, as it is the case for a pregroup. The problem also becomes more intriguing in the recent setting of (Coecke & Pavlovic 2006) where classical information flow is also axiomatized as a refinement of quantum information flow. An interesting question arises: can the decision procedure be reversed? If yes, can it be used to derive new quantum protocols?

Acknowledgments

I would like to thank B. Coecke, J. Lambek, and E. D'hondt for valuable discussions and comments, and P. Panangaden and S. Abramsky for their help in analysis of the Hindi and Hebrew sample sentences.

References

Abramsky, S., and Coecke, B. 2004. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Science Press. arXiv:quant-ph/0402130.

Abramsky, S., and Duncan, R. 2006. A categorical quantum logic. *Mathematical Structures in Computer Science (to appear)*.

Baltag, A., and Sadrzadeh, M. 2006. The algebra of multi-agent dynamic belief revision. *Electronic Notes in Theoretical Computer Science* 157.

Baltag, A.; Coecke, B.; and Sadrzadeh, M. 2004. Epistemic actions as resources. *Journal of Logic and Computation (to appear)*. accessible from http://www.ecs.soton.ac.uk/∼ms6/JLC.pdf.

Baltag, A.; Moss, L.; and Solecki, S. 1999. The logic of public announcements, common knowledge and private suspicions. Technical report, CWI.

Bargelli, D., and Lambek, J. 2001a. An algebraic appraoch to arabic sentence structure. *Linguistic Analysis* 31.

Bargelli, D., and Lambek, J. 2001b. An algebraic approach to french sentence structure. *Logical Aspects of Computational Linguistics*.

Birkhoff, G., and von Neumann, J. 1936. The logic of quantum mechanics. *Annals of Mathematics* 37:823–843.

Buszkowski, W. 2001. Lambek grammars based on pregroups. *Logical Aspects of Computational Linguistics*.

Casadio, C., and Lambek, J. 2001. An algebraic analysis of clitic pronouns in italian. *Logical Aspects of Computational Linguistics*.

Clark, S., and Pulman, S. 2006. Combining symbolic and distributional models of meaning. Accepted for the AAAI Spring Symposium on Quantum Interaction.

Coecke, B., and Pavlovic, D. 2006. Quantum measurements without sums. In Chen, G.; Kauffman, L.; and Lamonaco, S., eds., *Mathematics of Quantum Computing and Technology*. Taylor and Francis. arXiv:quant-ph/0608035.

Coecke, B.; Moore, D. J.; and Stubbe, I. 2001. Quantaloids describing causation and propagation of physical properties. *Foundations of Physics Letters* 14.

Danos, V.; Kashefi, E.; and Panangaden, P. 2005. The measurement calculus. *Quantum Physics Archives*. arXiv: quant-ph/0412135.

Ekert, A. 1991. Quantum cryptography based on bell's theorem. *Physical Review Letters* 67.

Fagin, R.; Halpern, J. Y.; Moses, Y.; and Vardi, M. Y. 1995. *Reasoning about Knowledge*. MIT Press.

Gazdar, G. 1996. Paradigm merger in natural language processing. In Milner, R., and Wand, I., eds., *Computing Tomorrow: Future Research Directions in Computer Science*. Cambridge University Press. 88–109.

Girard, J.-Y. 1987. Linear logic. *Theoretical Computer Science* 50.

Harel, D.; Kozen, D.; and Tiuryn, J. 2000. *Dynamic Logic*. MIT Press.

Hoare, C. A. R., and Jifeng, H. 1987. The weakest prespecification. *Information Processing Letters* 24.

Johnstone, P. T. 1982. *Stone Spaces*. Cambridge University Press.

Lambek, J. 1958. The mathematics of sentence structure. *American Mathematics Monthly* 65.

Lambek, J. 1999. Type grammar revisited. *Logical Aspects of Computational Linguistics* 1582.

Lambek, J. 2001. Type grammars as pregroups. *Grammar* 4.

Lambek, J. 2004. A computational algebraic approach to english grammar. *Syntax* 7:2.

Moortgat, M. 1997. Categorical type logics. In van Benthem, J., and ter Meulen, A., eds., *Handbook of Logic and Language*. Elsevier.

Sadrzadeh, M. 2005. Staying safe with Bell. In *Q-day II Workshop organized by B. Coecke and V. Danos*. Institute Henri Pincaré, Université Paris VII.

Sadrzadeh, M. 2006a. *Actions and Resources in Epistemic Logic*. Ph.D. Dissertation, Université du Québec À Montréal. http://www.ecs.soton.ac.uk/∼ms6/all.pdf.

Sadrzadeh, M. 2006b. Pregroup analysis of persian sentences. unpublished paper, accessible from http://www.ecs.soton.ac.uk/∼ms6/PersPreGroup.pdf.

van Rijsbergen, C. J. 2004. *The Geometry of Information Retrieval*. Cambridge University Press.

Widdows, D. 2004. *Geometry and Meaning*. Center for the Study of Language and Information/SRI.