Proc. QPL 2004, pp. 3–20

A categorical quantum logic

Samson Abramsky Ross Duncan

Oxford University Computing Laboratory

Abstract

We define a sequent calculus corresponding to the logic of strongly compact closed categories with biproducts. Based on this calculus, we define a proof-net syntax with a strongly normalising cut-elimination. This syntax encodes abstract qualitative and quantitative information about the behaviour of quantum processes.

1 Introduction

Recent work by Abramsky and Coecke [AC04] on compact closed categories with biproducts offers the first complete formalisation of finite dimensional quantum mechanics. Unlike earlier work, classical information flow is explicitly represented by the biproduct structure, while the compact closed structure models deterministic quantum behaviour: preparation, unitary evolution and projection. Mediating between the two levels is a semiring of scalars which represents the probability amplitudes in the abstract.

Compact closed categories are degenerate models of multiplicative linear logic in which the connectives, times and par, are identified. Similarly, the biproduct is a connective in which the additives of linear logic are combined. The system resulting from these identifications has a very different flavour to linear logic, indeed from any logic. Cyclic structures abound and every sequent is provable. These apparent perversities are, however, no cause for alarm: the resulting equations faithfully mirror calculations in quantum mechanics as shown in [AC04].

Beginning with a category $\mathcal{A}$ of basic types and maps between them we construct the free strongly compact closed category with biproducts $F\mathcal{A}$. We define a proof-net syntax for which this category is a faithful model. In the case without biproducts, we extend the work of Kelly and Laplaza [KL80] by showing that proof-net syntax is both faithful and fully complete with respect to $G\mathcal{A}$, the free compact closed category on $\mathcal{A}$. A morphism in $G\mathcal{A}$ represents one possible path of evolution for a quantum system; to each such morphism there is a corresponding proof-net. The biproduct structure, which encodes non-determinism of quantum measurement outcomes, is represented by slicing the proof-net. Each slice represents a different possible outcome of a quantum process.

Hence every proof-net corresponds to a physical network of quantum state preparations and measurements, and a compilation process to quantum circuits is easily defined. Cut-elimination reduces each such network to one without measurements and as such expresses the execution of a protocol or algorithm. Cut-elimination preserves denotational equality and hence serves as a correctness proof for the protocol encoded by the proof-net.

The models so constructed can be parameterised in two distinct fashions.

- The choice of the generating category $\mathcal{A}$ defines the possible preparations and projections.
- The semiring of scalars $I \rightarrow I$ gives rise to the “probabilities” of the different outcomes of a process.

By varying these parameters it is possible to explore what are the minimal requirements to achieve various “quantum” effects. For example it is known that the category **Rel** does not have enough scalars to represent the teleportation protocol. Another example: if $\mathcal{A}$ is a discrete category then the only possible preparations are maximally entangled pairs. This is sufficient for entanglement swapping, but not logic gate teleportation.

The cut-elimination procedure provides an easily implemented method for performing calculations about the structure of entangled states. Such a concrete implementation promises to be a useful tool for reasoning qualitatively about quantum protocols. Further: the system can be viewed as a step towards a quantum programming language equipped with an entanglement-aware type system.

In the next section we revise the basic structure of strongly compact closed categories with biproducts. In section 3 we define a sequent calculus system **LCCB** for the logic of compact closed categories with biproducts. We give the semantics for **LCCB**, both in one and two sided formulation and describe its cut-elimination. In section 4 we define the notion of CCB-net and give a sound strong normalisation procedure for it. We sketch the proofs of faithfulness, and full completeness for the compact closed case.

2 Strongly Compact Closed Categories with Biproducts

In this section we recall the definitions and key properties of strongly compact closed categories with biproducts. For a full treatment of the biproduct structure see [Mit65], for the monoidal and compact closed structure see [Mac97, KL80]. The application of these strongly compact closed categories with biproducts to quantum mechanics is developed in [AC04].

Definition 1 (Symmetric Monoidal Category). A *symmetric monoidal* category is a category $\mathcal{C}$ equipped with a bifunctor

$$- \otimes - : \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C},$$

a monoidal unit object I and certain natural isomorphisms

$$\lambda_A : A \simeq \mathrm{I} \otimes A \qquad\qquad \rho_A : A \simeq A \otimes \mathrm{I}$$

$$\alpha_{A,B,C} : A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$$

$$\sigma_{A,B} : A \otimes B \simeq B \otimes A$$

which satisfy certain coherence conditions [Mac97].

In any monoidal category $\mathcal{C}$, the endomorphisms $\mathcal{C}(I, I)$ form a commutative monoid [KL80]. We call these endomorphisms the *scalars* of $\mathcal{C}$. For each scalar $s : I \to I$ we can define a natural transformation

$$s_A : A \xrightarrow{\;\cong\;} I \otimes A \xrightarrow{\;s \otimes 1_A\;} I \otimes A \xrightarrow{\;\cong\;} A\,.$$

Hence, we can define *scalar multiplication* $s \bullet f := f \circ s_A = s_B \circ f$ for $f : A \to B$. Then we have

$$(s \bullet g) \circ (r \bullet f) = (s \circ r) \bullet (g \circ f)$$

for $r : I \to I$ and $g : B \to C$.

Definition 2 (Compact Closed Category). A symmetric monoidal category is *compact closed* if to each object A there is an assigned left adjoint $(A^*, \eta_A, \epsilon_A)$ such that the composites

$$A \cong A \otimes I \xrightarrow{1_A \otimes \eta_A} A \otimes (A^* \otimes A) \cong (A \otimes A^*) \otimes A \xrightarrow{\epsilon_A \otimes 1_A} I \otimes A \cong A$$
$$A^* \cong I \otimes A^* \xrightarrow{\eta_A \otimes 1_{A^*}} (A^* \otimes A) \otimes A^* \cong A^* \otimes (A \otimes A^*) \xrightarrow{1_{A^*} \otimes \epsilon_A} A^* \otimes I \cong A^*$$

are both identities.

For each morphism $f : A \to B$ in a compact closed category we can construct its *name*, $\ulcorner f \urcorner : I \to A^* \otimes B$, *coname*, $\llcorner f \lrcorner : A \otimes B^* \to I$, and *dual*, $f^* : B^* \to A^*$, by

$$\ulcorner f \urcorner = (1_{A^*} \otimes f) \circ \eta_A$$
$$\llcorner f \lrcorner = \epsilon_A \circ (g \otimes 1_{B^*}$$
$$f^* = \rho_{A^*} \circ (1_{A^*} \otimes \epsilon_B) \circ (1_{A^*} \otimes f \otimes 1_{B^*}) \circ (\eta_A \otimes 1_{B^*}) \circ \lambda_{B^*}^{-1}$$

In particular the map $f \mapsto f^*$ extends to a contravariant endofunctor with $A \cong A^{**}$.

Each compact closed category admits a categorical trace. That is, for every morphism $f : A \otimes C \to B \otimes C$ certain axioms [JSV96] are satisfied by $\mathrm{Tr}^C_{A,B}(f) : A \to B$, defined as the composite is defined by:

$$A \cong A \otimes I \xrightarrow{1_A \otimes \eta_{C^*}} A \otimes C \otimes C^* \xrightarrow{f \otimes 1_{C^*}} B \otimes C \otimes C^* \xrightarrow{1_B \otimes \epsilon_C} B \otimes I \cong B.$$

The following results are proved in [AC04].

Lemma 3. *Suppose we have maps* $E \xrightarrow{k} A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$*. Then*

1. $(1_{A^*} \otimes g) \circ \ulcorner f \urcorner = \ulcorner g \circ f \urcorner$ *(absorption)*
2. $(k^* \otimes 1_{A^*}) \circ \ulcorner f \urcorner = \ulcorner f \circ k \urcorner$. *(backward absorption)*
3. $\lambda_C^{-1} \circ (\llcorner f \lrcorner \otimes 1_C) \circ (1_A \otimes \ulcorner g \urcorner) \circ \rho_A = g \circ f$ *(compositionality)*
4. $(\rho_A^{-1} \otimes 1_{D^*}) \circ (1_{A^*} \otimes \llcorner g \lrcorner \otimes 1_D) \circ (\ulcorner f \urcorner \otimes \ulcorner h \urcorner) \circ \rho_I = \ulcorner h \circ g \circ f \urcorner$ *(compositional CUT)*

The obvious analogues of Lemma 3.1 and 3.2 for conames also hold.

Definition 4 (Strong Compact Closure). A compact closed category $\mathcal{C}$ is *strongly compact closed* if and $A = A^{**}$ and the assignment $A \mapsto A^*$ extends to a covariant involutive functor. Write f_* for the action of this functor on arrow f. Given $f : A \longrightarrow B$ in a strongly compact closed category we can define its *adjoint* $f^\dagger : B \longrightarrow A$ by $f^\dagger = (f_*)^* = (f^*)_*$.

Definition 5 (Zero Object). A zero object in $\mathcal{C}$ is both initial and terminal. If **0** is a zero object, there is an arrow $0_{A,B} : A \longrightarrow \mathbf{0} \longrightarrow B$ between any pair of objects A and B.

Definition 6 (Biproduct). A *biproduct* is a bifunctor $- \oplus - : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ which is both a product and coproduct.

If $\mathcal{C}$ has biproducts, then we can define an operation of addition on each hom-set $\mathcal{C}(A, B)$ by

$$f + g = \nabla \circ (f \oplus g) \circ \Delta$$

for $f, g : A \to B$, where $\Delta = \langle 1_A, 1_A \rangle$ and $\nabla = [1_B, 1_B]$. This operation is associative and commutative, with 0_{AB} as an identity. Moreover, composition is bilinear with respect to this additive structure.

If $\mathcal{C}$ has biproducts, we can choose projections p_1, p_2 and injections q_1, q_2 for each $A \oplus B$ satisfying:

$$p_i \circ q_j = \delta_{ij} \qquad q_1 \circ p_1 + q_2 \circ p_2 = 1_{A \oplus B}$$

where $\delta_{ii} = 1_I$, and $\delta_{ij} = 0_I$, $i \neq j$.

Proposition 7 (Distributivity of $\otimes$ over $\oplus$). *In monoidal closed categories there are natural isomorphisms*

$$d_{A,B,C} : A \otimes (B \oplus C) \cong (A \otimes B) \oplus (A \otimes C)$$

$$d_{A,\cdot,\cdot} = \langle 1_A \otimes p_1, 1_A \otimes p_2 \rangle \qquad d^{-1}_{A,\cdot,\cdot} = [1_A \otimes q_1, 1_A \otimes q_2] \,.$$

A left distributivity isomorphism can be defined similarly.

If $\mathcal{C}$ is strongly compact closed and has biproducts we require a compatibility condition, namely that the coproduct injections

$$q_i : A_i \to \bigoplus_{k=1}^{k=n} A_k$$

satisfy $q_j^\dagger \circ q_i = \delta_{ij}$. It then follows that we can require that the projections and injections additionally satisfy $(p_i)^\dagger = q_i$.

3 Sequent Calculus

We define a logic for strongly compact closed categories with biproducts. The formulae of the logic correspond to the objects of the category, while there is an inference rule corresponding to each of the canonical constructions of the compact closed and biproduct structure. Proofs in the logic denote arrows in the category. Rather than an arbitrary CCB, we consider only those freely generated from some base category. Let the free compact closed category with biproducts on $\mathcal{A}$ be $F\mathcal{A}$.

The logic of $F\mathcal{A}$ is parameterised by $\mathcal{A}$. The objects of $\mathcal{A}$ occur as the atoms of the syntax, while we introduce generalised axiom, cut and unit rules generated by the arrows of $\mathcal{A}$.

Definition 8. The *atoms* of the logic are the objects of $\mathcal{A}$. The *formulae* of the logic are built from the following grammar:

$$F ::== \ A \mid F^* \mid F \otimes F \mid F \oplus F$$

The following equations between formulae apply:

$$\begin{aligned} A^{**} &= A \\ (A \otimes B)^* &= A^* \otimes B^* \\ (A \oplus B)^* &= A^* \oplus B^*. \end{aligned}$$

As well as the objects of the category, we need some further information about the structure of the category.

Definition 9. The *loops* of $\mathcal{A}$ are equivalence classes of endomorphisms of $\mathcal{A}$; arrows are considered equivalent if they differ only by a cyclic permutation. For example, given $f : A \to B$ and $g : B \to A$, the endomorphisms $f \circ g : B \to B$ and $g \circ f : A \to A$ are equivalent.

Now we define the two-sided sequent calculus $\mathbf{LCCB}_2$.

Definition 10. An $\mathbf{LCCB}_2$ sequent is of the form

$$\Gamma \vdash \Delta; [L]$$

where Γ, Δ are lists of formulae and L is a multiset of loops.

The inclusion of the loops in the definition of sequent is slightly misleading: strictly the loop sets are a proof decoration rather than a property of the sequents themselves. For this reason two sequents are defined to be equal if they differ only by loops. This identification is forced since loops are not preserved by cut-elimination.

Definition 11. An $\mathbf{LCCB}_2$ proof is a tree of sequents joined by the inference rules show in in figures 1, 2 and 3. The inferences at the leaves of the tree must be axioms.

We will assume, without loss of generality, that axioms introduce only atomic formulae. Hence the rules for identity axiom and zero can be subsumed by the generalised axiom rule, even though $0_B^A : A \to B$ is not an arrow of the base category $\mathcal{A}$.

Example 12. Suppose we have $A \xrightarrow{f} B$ and $C \xrightarrow{g} D \xrightarrow{h} C$.

$$\dfrac{\dfrac{\dfrac{\dfrac{f}{B \vdash A; []} \quad \dfrac{}{A \vdash A; []}}{B \oplus A \vdash A; []} \quad \dfrac{g}{C \vdash D; []}}{B \oplus A, C \vdash A, D; []}}{B \oplus A \vdash A; []}\ (h\text{-cut})$$

Identity Group

$$\frac{}{A \vdash A\ ;\ []}\ \text{(axiom)} \qquad\qquad \frac{\Gamma, A \vdash A, \Delta\ ;\ [L]}{\Gamma \vdash \Delta\ ;\ [L]}\ \text{(cut)}$$

Structure Group

$$\frac{\Gamma \vdash \Delta\ ;\ [L]}{\tau(\Gamma) \vdash \sigma(\Delta)\ ;\ [L]}\ \text{(exchange)}$$

Multiplicative Group

$$\frac{\Gamma \vdash \Delta\ ;\ [L] \qquad \Gamma' \vdash \Delta'\ ;\ [L']}{\Gamma, \Gamma' \vdash \Delta, \Delta'\ ;\ [L, L']}\ \text{(mix)}$$

$$\frac{\Gamma, A, B \vdash \Delta\ ;\ [L]}{\Gamma, A \otimes B \vdash \Delta\ ;\ [L]}\ \text{(times-L)} \qquad\qquad \frac{\Gamma \vdash A, B, \Delta\ ;\ [L]}{\Gamma \vdash A \otimes B, \Delta\ ;\ [L]}\ \text{(times-R)}$$

Figure 1: MULTIPLICATIVE RULES FOR **LCCB**$_2$

$\mathcal{A}$-Generalised Identity Group

$$\frac{f}{A \vdash B\ ;\ []}\ (f\text{-axiom}) \qquad \text{where } f : A \to B \text{ is an arrow of } \mathcal{A}$$

$$\frac{\Gamma, A \vdash B, \Delta\ ;\ [L]}{\Gamma \vdash \Delta\ ;\ [L]}\ (g\text{-cut}) \qquad \text{where } g : B \to A \text{ is an arrow of } \mathcal{A}.$$

$$\frac{}{\vdash\ ;\ [h]}\ (h\text{-unit}) \qquad \text{where } h : A \to A \text{ is a loop of } \mathcal{A}.$$

Figure 2: GENERALISED AXIOM, CUT AND UNIT RULES FOR **LCCB**$_2$

Warning!. It is necessary to distinguish between occurrences of formulae in sequents, and throughout proofs, otherwise one can arrive at situations where it is impossible to see what is going on, such as the proof below.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A} \quad \dfrac{}{A \vdash A}}{A, A \vdash A, A}\ \text{(mix)} \qquad \dfrac{}{A \vdash A}}{A, A, A \vdash A, A, A}\ \text{(mix)}}{A, A, A \vdash A, A, A}\ \text{(exchange)}}{A, A \vdash A, A}\ \text{(cut)}$$

In the following it is tacitly assumed that all formulae occur uniquely.

Additive Group

$$\frac{\Gamma, A \vdash \Delta \; ; [L] \qquad \Gamma, B \vdash \Delta \; ; [L']}{\Gamma, A \oplus B \vdash \Delta \; ; [L, L']} \text{ (plus-2L)} \qquad \frac{\Gamma, A_i \vdash \Delta \; ; [L]}{\Gamma, A_1 \oplus A_2 \vdash \Delta \; ; [L]} \text{ (plus-1L)}$$

$$\text{for } i = 1, 2$$

$$\frac{\Gamma \vdash \Delta, A \; ; [L] \qquad \Gamma \vdash \Delta, B \; ; [L']}{\Gamma \vdash \Delta, A \oplus B \; ; [L, L']} \text{ (plus-2R)} \qquad \frac{\Gamma \vdash \Delta, A_i \; ; [L]}{\Gamma \vdash \Delta, A_1 \oplus A_2 \; ; [L]} \text{ (plus-1R)}$$

$$\frac{0^A_B}{A \vdash B \; ; []} \text{ (zero)} \qquad \frac{\Gamma, A \vdash B, \Delta \; ; [L]}{\Gamma \vdash \Delta \; ; [L]} \text{ (0-cut)}$$

$$\frac{\Gamma \vdash \Delta \; ; [L] \qquad \Gamma \vdash \Delta \; ; [L']}{\Gamma \vdash \Delta \; ; [L, L']} \text{ (sum)}$$

Figure 3: ADDITIVE RULES FOR **LCCB**$_2$

Discussion of the Rules

The Cut Rule The cut rule, as shown here, might be better described as a trace rule. Peeking ahead to the semantics it is indeed interpreted by the trace. By proposition 2.4 of [AHS02] we have

$$g \circ f = \mathrm{Tr}^B_{A,C}(\sigma_{B,C} \circ (f \otimes g))$$

for $f : A \to B, g : B \to C$. Hence our cut rule gives the usual idea of partial composition. We will write the traditional cut

$$\frac{\Gamma \vdash \Delta, A \qquad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \text{ (cut)}$$

as short hand for its **LCCB**$_2$ derivation, viz.

$$\cfrac{\cfrac{\Gamma \vdash \Delta, A \qquad A, \Gamma' \vdash \Delta'}{\Gamma, A, \Gamma' \vdash \Delta, A, \Delta'} \text{ (mix)}}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \text{ (cut)}$$

Generalised Axioms and Cuts The side condition on generalised axioms and cut rules – that they are generated by arrows of the base category $\mathcal{A}$ – implies that the formulae introduced by the axiom must be atomic; likewise the cut-formulae of a generalised cut are always atomic. There is no semantic reason for this restriction, and axioms and cuts derived from the arrows of $F\mathcal{A}$ are quite possible, however cut-elimination would be impossible. The effect of an "over-generalised cut" on some arrow g in $F\mathcal{A}$ can be simulated by constructing a proof corresponding to g and using two identity cuts.

Identity Group

$$\frac{}{1_A : A \to A}\text{(axiom)} \qquad \frac{f : \Gamma \otimes A \to A \otimes \Delta}{\mathrm{Tr}^A_{\Gamma,\Delta}(\sigma_{A,\Delta} \circ f) : \Gamma \to \Delta}\text{(cut)}$$

Structure Group

$$\frac{f : \Gamma \to \Delta}{\sigma \circ f \circ \tau^{-1} : \tau(\Gamma) \to \sigma(\Delta)}\text{(exchange)}$$

Multiplicative Group

$$\frac{f : \Gamma \to \Delta \qquad g : \Gamma' \to \Delta'}{(f \otimes g) : \Gamma \otimes \Gamma' \to \Delta \otimes \Delta'}\text{(mix)}$$

$$\frac{f : (\Gamma \otimes A) \otimes B \to \Delta}{f \circ \alpha^{-1}_{\Gamma,A,B} : \Gamma \otimes (A \otimes B) \to \Delta}\text{(times-L)}$$

$$\frac{f : \Gamma \to A \otimes B \otimes \Delta}{\alpha_{\Gamma,A,B} \circ f : \Gamma \to (A \otimes B) \otimes \Delta}\text{(times-R)}$$

Figure 4: SEMANTICS FOR THE MULTIPLICATIVE RULES OF **LCCB**$_2$

Zero Rules For similar reasons the axiom and cut rules for zero are introduced; without them certain bad cuts are impossible to remove. It has been noted that the logic of biproducts is inconsistent: every sequent is provable. By including the zero axiom we embrace this inconsistency. A more computational point of view is that every type is inhabited, at least by the divergent program, or in the quantum setting, the evolution with zero probability.

Loops By adding the loops to the syntax we make a minor technical improvement on [Shi96]: all cuts can be eliminated, so there is no need for an auxiliary notion of normal form. More importantly, the loops are syntactic representatives for the scalars $I \to I$; separating them out opens the door to an additional rewriting system to compute the "probabilities" of different paths of the computation. Unfortunately the sequent presentation flattens too much of the branching structure to permit this, but it can be reclaimed via the proof-nets introduced in the next section.

Definition 13. The rules of **LCCB**$_2$ are in one to one correspondence with the constructions on arrows shown in figures 4, 5 and 6. Hence every proof π of $\Gamma \vdash \Delta$ in **LCCB**$_2$, defines an arrow of $F\mathcal{A}$, $[\![\pi]\!] : \bigotimes \Gamma \to \bigotimes \Delta$, by its construction.

LCCB$_2$ encodes the categorical structure very naturally. However the large number of rules make it rather cumbersome. Operating in the one-sided calculus **LCCB**$_1$ reduces the workload while losing nothing essential. Proofs in **LCCB**$_2$ can be easily translated into **LCCB**$_1$, and have isomorphic denotations. The rules of **LCCB**$_1$ are shown in figure 7.

$\mathcal{A}$-Generalised Identity Group

$$\frac{}{f : A \to B}\ (f\text{-axiom}) \qquad \text{where } f : A \to B \text{ is an arrow of } \mathcal{A}$$

$$\frac{f : \Gamma \otimes A \to B \otimes \Delta}{\mathrm{Tr}^{A\otimes B}_{\Gamma,\Delta}(\sigma \circ (f \otimes g) : \Gamma \to \Delta}\ (g\text{-cut}) \qquad \text{where } g : B \to A \text{ is an arrow of } \mathcal{A}.$$

$$\frac{}{\epsilon_A \circ \ulcorner h \urcorner : I \to I}\ (h\text{-unit}) \qquad \text{where } h : A \to A \text{ is a loop of } \mathcal{A}.$$

Figure 5: SEMANTICS FOR THE GENERALISED AXIOM, CUT AND UNIT RULES OF **LCCB**$_2$

Additive Group

$$\frac{f : \Gamma \otimes A \to \Delta \qquad g : \Gamma \otimes B \to \Delta}{[f, g] \circ d : \Gamma \otimes (A \oplus B) \to \Delta}\ (\text{plus-2L})$$

$$\frac{f : \Gamma \otimes A_i \to \Delta}{f \circ (1_\Gamma \otimes p_i) : \Gamma \otimes (A_1 \oplus A_2) \to \Delta}\ (\text{plus-1L})$$

$$\frac{f : \Gamma \to \Delta \otimes A \qquad g : \Gamma \to \Delta \otimes B}{d^{-1} \circ \langle f, g \rangle : \Gamma \to \Delta \otimes (A \oplus B)}\ (\text{plus-2R})$$

for $i = 1, 2$

$$\frac{f : \Gamma \to \Delta \otimes A_i}{(1_\Delta \otimes q_i) \circ f : \Gamma \to \Delta \otimes (A_1 \oplus A_2)}\ (\text{plus-1R})$$

$$\frac{0^A_B}{0^A_B : A \to B}\ (\text{zero}) \qquad \frac{f : \Gamma, A \to B, \Delta}{\mathrm{Tr}^{A\otimes B}_{\Gamma,\Delta}(\sigma \circ (f \otimes 0^B_A) : \Gamma \to \Delta}\ (0\text{-cut})$$

$$\frac{f : \Gamma \to \Delta \qquad g : \Gamma \to \Delta}{f + g : \Gamma \to \Delta}\ (\text{sum})$$

Figure 6: SEMANTICS FOR THE ADDITIVE RULES OF **LCCB**$_2$

$$\frac{}{\vdash A^*, A \; ; []}\ \text{(axiom)} \qquad \frac{\vdash \Gamma, A, A^* \; ; [L]}{\Gamma \vdash \Delta \; ; [L]}\ \text{(cut)}$$

$$\frac{f}{\vdash A^*, B \; ; []}\ \text{(f-axiom)} \qquad \frac{\vdash \Gamma, A^*, B, \Delta \; ; [L]}{\Gamma \vdash \Delta \; ; [L]}\ \text{(g-cut)}$$

$$\frac{}{\vdash \; ; [h]}\ \text{(h-unit)} \qquad \frac{\vdash \Gamma \; ; [L]}{\vdash \sigma(\Gamma) \; ; [L]}\ \text{(exchange)}$$

$$\frac{\vdash \Gamma \; ; [L] \qquad \vdash \Delta \; ; [L']}{\vdash \Gamma, \Delta \; ; [L, L']}\ \text{(mix)} \qquad \frac{\vdash \Gamma, A, B \; ; [L]}{\vdash \Gamma, A \otimes B \; ; [L]}\ \text{(times)}$$

$$\frac{\vdash \Gamma, A_i \; ; [L]}{\vdash \Gamma, A_1 \oplus A_2 \; ; [L]}\ \text{(plus-1)} \quad \text{for } i = 1, 2 \quad \frac{\vdash \Gamma, A \; ; [L] \qquad \vdash \Gamma, B \; ; [L']}{\vdash \Gamma, A \oplus B \; ; [L, L']}\ \text{(plus-2)}$$

$$\frac{0^A_B}{\vdash A^*, B \; ; []}\ \text{(zero)} \qquad \frac{\vdash \Gamma, A^* B \; ; [L]}{\vdash \Gamma \; ; [L]}\ \text{(0-cut)}$$

$$\frac{\vdash \Gamma \; ; [L] \qquad \vdash \Gamma \; ; [L']}{\vdash \Gamma \; ; [L, L']}\ \text{(sum)}$$

Figure 7: SEQUENT RULES FOR **LCCB**$_1$

Definition 14. Given an **LCCB**$_2$ proof π of the sequent $\Gamma \vdash \Delta \; ; [L]$ we can define an **LCCB**$_1$ proof π^* of $\vdash \Gamma^*, \Delta \; ; [L]$ by a direct rule for rule translation of π. Since the connectives are self dual, left and right rules for the connectives are both translated by the same rule in the one sided system.

Proposition 15. *Let π be an **LCCB**$_2$ proof and π^* its **LCCB**$_1$ translation. Then:*

$$[\![\pi^*]\!] = \ulcorner [\![\pi]\!] \urcorner.$$

From here on we'll work exclusively with **LCCB**$_1$.

Theorem 16 (Cut-Elimination). *Every **LCCB**$_1$ proof can be transformed into cut-free proof of the same sequent.*

Proof. Standard techniques largely suffice. The self-duality of $\oplus$ permits "bad cuts" which cannot be eliminated by decomposing and reordering inferences; judicious application of the 0-cut and sum rules solves the problem. The only novelties are the rules of the $\mathcal{A}$-generalised group. Let $A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathcal{A}$, and consider the proof shown below.

$$\frac{\dfrac{f}{\vdash A*, B \; ; []} \qquad \dfrac{\vdots}{\vdash C^*, \Gamma \; ; [L]}}{\vdash A^*, \Gamma \; ; [L]}\ \text{(g-cut)}$$

Since C is atomic the formula C^* must be introduced by an axiom, hence we can permute the cut up the right hand subproof until we reach this axiom. Hence we have:

$$\dfrac{\dfrac{f}{\vdash A*, B \ ;\ []} \qquad \dfrac{h}{\vdash C^*, D \ ;\ []}}{\vdash A^*, D \ ;\ []}\ (g\text{-cut})$$

which reduces to

$$\dfrac{f \circ g \circ h}{\vdash A^*, D \ ;\ []}.$$

Of course if both f and g were identities then the cut could just have been erased at the starting point.

Now suppose $A \xrightarrow{f} B \xrightarrow{g} A$. The proof

$$\dfrac{\dfrac{f}{\vdash A^*, B \ ;\ []}\ (\text{axiom})}{\vdash}\ (g\text{-cut})$$

represents what has been called "incestuous self-plugging" [Gir95]. In the degenerate world of compact closed categories, such things are quite acceptable. The proof reduces to

$$\dfrac{}{\vdash [f \circ g]}.\ ((f \circ g)\text{-unit})$$

The remaining cases are either handled as in linear logic [Gir87] or Shirahata's CMLL [Shi96]. □

Theorem 17 (Soundness of Cut-Elimination). *If π reduces to π' by some number of cut elimination steps, then $[\![\pi]\!] = [\![\pi']\!]$.*

Remark. The soundness proof refers to the "natural" cut-elimination procedure, hinted at above. It's worth noting that there are possible cut elimination procedures, equally good at producing valid proofs, which are not sound. As a simple example, we note that in any cut-free proof of the sequent

$$\vdash \Gamma \ ;\ [h]$$

the loop h must be introduced by an application of the h-unit rule, and the mix rule. Omitting these inferences yields a perfectly serviceable cut-free proof of $\vdash \Gamma$, however its denotation will not coincide with that of the original.

The sequent calculus presentation is the most natural way to define the semantics of the logic, however it is far from perfect. As is usual for sequent calculi, the cut elimination procedure is not confluent, so a proof can have many denotationally equivalent normal forms. Almost as bad, the branching structure induced by the biproduct is completely hidden. To remedy these defects, in the next section we define a proof-net which captures more precisely the structure of the category and simulates more directly the behaviour of quantum systems.

4 CCB-nets

CCB-nets provide a proof-net like syntax encoding the structure of a compact closed category with biproducts. The additive structure is encoded by dividing the proof into *slices*.

Definition 18 (CCB-slice). A *CCB-slice* is a finite oriented graph with edges labelled by formulae. The graph is constructed by composing the following nodes[1] respecting the labelling on the incoming and outgoing edges.

Axiom No incoming edges; two out-going edges. To each arrow[2] $f : A \to B$ of $\mathcal{A}$ we have an axiom link, one outgoing edge with A^* and the other with B.

Cut Two incoming edges ; no outgoing edges. There are three subcases:

- Identity cuts: incoming edges are labelled by any pair of dual formulae, A, A^*;
- g-cuts: to each arrow $g : B \to A$ in $\mathcal{A}$ we have a cut rule, the incoming edges are labelled B and A^*;
- Zero cuts: incoming edges labelled by any formulae A, B.

Times Two incoming edges labelled A and B ; one outgoing edge labelled $A \otimes B$.

Plus 1 One incoming edge labelled A ; one outgoing edge labelled $A \oplus B$.

Plus 2 One incoming edge labelled B ; one outgoing edge labelled $A \oplus B$.

The orientation is such that edges enter the node from the top, and exit from the bottom. The *conclusions* of the slice are those labels on outgoing edges of links which are left unconnected. The order of the conclusions is significant.

Definition 19 (CCB-net). A *CCB-net* is a finite multiset of CCB-slices where each slice has the same conclusions.

Remark. This permissive syntax has a very lax notion of correctness: essentially anything goes. There is no requirement for the resulting graphs to be acyclic, nor need they be connected. Unlike proof-nets for linear logic, CCB-nets have no correctness criteria [DR89, HvG03] to pick out the sequentialisable structures since there is no external notion of correctness for CCB-nets. Although we will not prove it here, every CCB-net can be translated back into an equivalent sequent proof in $\mathbf{LCCB}_1$.

Definition 20 (Translation into CCB-nets). Given an $\mathbf{LCCB}_1$ proof π, we define a CCB-structure $N\pi$ by recursion over the structure of π.

- If proof π is just an axiom, let $N\pi$ be the single slice containing just the corresponding axiom link.
- If proof π is a just an application of the h-unit rule for some $h : A \to A$, let $N\pi$ be the single slice containing an axiom link for h with an identity cut link between its conclusions.

[1] which for historical reasons are usually called *links*.

[2] We again include $0_B^A : A \to B$ among the axioms for all A, B in $\mathcal{A}$

- If π arises from π' by an application of the cut rule for arrow g (including zero, and the identity on compound formulae) form $N\pi$ adding, in every slice, the cut link corresponding to g between the conclusions of $N\pi'$ corresponding to the active formulae of the cut rule.

- Suppose π arises from subproofs π_1 and π_2 by the mix rule. Suppose the sub-proofs have $N\pi_1 = \{S_i^1 | i = 1..n\}$ and $N\pi_2 = \{T_j | j = 1..m\}$. Then let $N\pi = \{R_{ij} | i = 1..n, j = 1..m\}$ where R_{ij} is the slice formed by combining S_i and T_j.

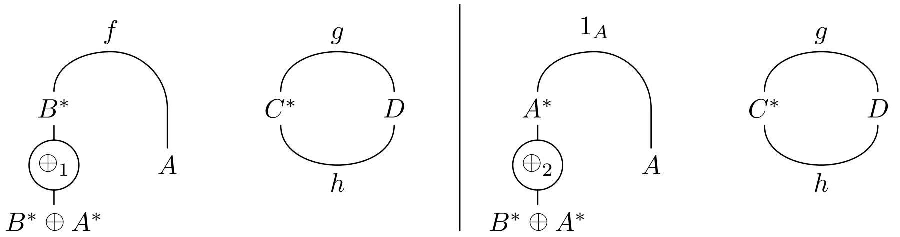
- If π arises from π' by an application of the times rule, form $N\pi$ adding, in every slice, a $\otimes$-link between the conclusions of $N\pi'$ corresponding to the active formulae of the times rule.

- If π arises from π' by an application of the unary plus rule with the premise on the left (right), form $N\pi$ by adding a $\oplus_1$-link (resp. $\oplus_2$-link) to the conclusion corresponding to the active formula in every slice of $N\pi'$.

- Suppose π arises via an application of the binary rule for plus : to each slice of $N\pi_1$ add a $\oplus_1$-link ; to each slice of $N\pi_2$ add a $\oplus_2$-link ; form $N\pi$ by the union of the these two sets of slices.

- If π arises via an application of the sum rule then $N\pi$ is the union of the $N\pi_1$ and $N\pi_2$.

Example 21. This CCB-net is the translation of Example 12.



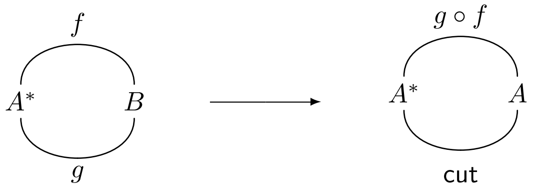
Definition 22 (Normal Forms). A CCB-slice is *normal* if every connected component either has no cut links, or is a closed loop formed by one axiom link and an identity cut. A CCB-net is normal if every slice is normal.

Theorem 23 (Cut Elimination). *Every CCB-net can be reduced to a normal CCB-net with the same conclusions. Further, the procedure is confluent and strongly normalising.*

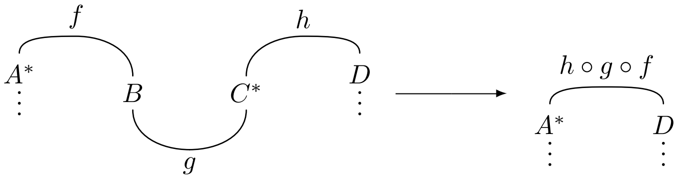
Proof. The procedure is to normalise each slice in parallel. To reduce a slice to normal form, apply these rewriting rules everywhere possible:

1. g-cut against an axiom. Due to the side-condition on generalised cuts, both incoming formulae must be atomic. Hence the cut links two formulae coming from axiom links.

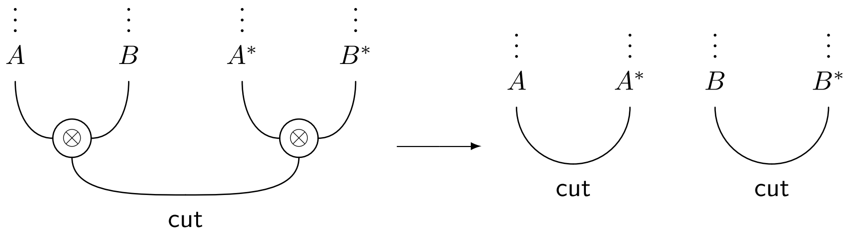
(a) If both formulae belong to the same axiom (say f):



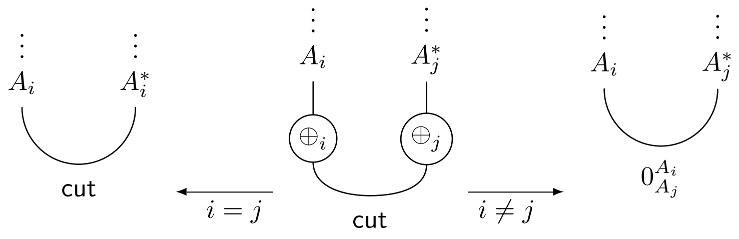
(b) If the cut formulae are conclusions of different axioms, say f and h:



2. Cut between two tensor products:



3. Cut between two biproducts:



The first rewriting rule either eliminates a cut, or reduces it to normal form. The other two rules reduce complex cuts to simpler cuts. Hence when no more rewrites can be done the slice is in normal form.

Each reduction step is purely local – no rewrite can affect any other – hence the process is confluent. Since each step reduces the complexity of the net, there is no infinite reduction sequence, and hence every CCB-net is strongly normalising. □

Definition 24 (Semantics for CCB-nets). Let ν be a CCB-slice with conclusions Γ. Define an arrow of $F\mathcal{A}$, $\llbracket \nu \rrbracket : I \to \bigotimes \Gamma$, by recursion on the structure of ν.

- If ν is just an axiom link corresponding to the arrow $F : A \to B$, then $\llbracket \nu \rrbracket := \ulcorner f \urcorner : I \to A^* \otimes B$.
- If ν has several disconnected components $\nu_1, \ldots, \nu_n$ then let $\iota : I \xrightarrow{\cong} \bigotimes_{i=1}^{n} I$ be the canonical isomorphism of the compact closed structure. The define $\llbracket \nu \rrbracket = (\bigotimes_{i=1}^{n} \nu_i) \circ \iota$.
- If ν is built by applying a g-cut between conclusions A and B^* of from ν', suppose that $\llbracket \nu' \rrbracket : I \to \Gamma \otimes (A \otimes B^*) \otimes \Delta$ then let $\llbracket \nu \rrbracket = (1_\Gamma \otimes \llcorner g \lrcorner \otimes 1_\Delta) \circ \llbracket \nu' \rrbracket$.
- If ν is built by applying a $\otimes$-link between conclusions A and B of ν', suppose that $\llbracket \nu' \rrbracket : I \to (\Gamma \otimes A) \otimes (B \otimes \Delta)$ then let $\llbracket \nu \rrbracket = a \circ \llbracket \nu' \rrbracket$, where $a : (\Gamma \otimes A) \otimes (B \otimes \Delta) \xrightarrow{\cong} \Gamma \otimes (A \otimes B^*) \otimes \Delta$.
- If ν is built by applying a $\oplus_i$ link to conclusion A of ν', suppose that $\llbracket \nu' \rrbracket : I \to \Gamma \otimes A \otimes \Delta$ then let $\llbracket \nu \rrbracket = (1_\Gamma \otimes q_i \otimes 1_\Delta) \circ \llbracket \nu' \rrbracket$.

All these constructions commute wherever the required compositions are defined due to the functoriality of the tensor, hence $\llbracket \nu \rrbracket$ is well defined.

Theorem 25 (Soundness). *If a CCB-net ν reduces to ν' by one or more steps of the cut-elimination procedure of Theorem 23 then $\llbracket \nu \rrbracket = \llbracket \nu' \rrbracket$.*

Proof. Each of the rewrite rules of the cut elimination procedure preserves denotation. For each rewrite rule we show the corresponding equation.

1. Suppose we have arrows $e : B \to A$ and $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ then

   (a) We have

   $$\begin{aligned} \llcorner e \lrcorner \circ \ulcorner f \urcorner &= \epsilon_{A^*} \circ (1_{A^*} \otimes g) \circ (1_{A^*} \otimes f) \circ \eta_A \\ &= \epsilon_{A^*} \circ (1_{A^*} \otimes (g \circ f) \circ \eta_A \\ &= \epsilon_{A^*} \circ \ulcorner (\urcorner g \circ f) \end{aligned}$$

   directly from the definition of the name and coname.

   (b) The required equation

   $$(1_{A^*} \otimes \llcorner g \lrcorner \otimes 1_D) \circ (\ulcorner f \urcorner \otimes \ulcorner h \urcorner) = \ulcorner h \circ g \circ f \urcorner$$

   is lemma 3.4 verbatim.

2. The case for tensor follows from $\epsilon_{A \otimes B} = \sigma \circ (\epsilon_A \otimes \epsilon_B)$.

3. By using forwards and backwards absorption (lemmas 3.1,3.2) we have

$$\epsilon_{A \oplus B} \circ (q_i \otimes q_j) = \llcorner p_j \circ 1_{A \oplus B} \circ q_i \lrcorner = \begin{cases} \epsilon_A & \text{if } i = j \\ \llcorner 0_B^A \lrcorner & \text{if } i = 1, j = 2 \\ \llcorner 0_A^B \lrcorner & \text{if } i = 2, j = 1 \end{cases}$$

The result follows by the functoriality of the tensor. □

Proposition 26. *Let π be a proof in* ***LCCB**$_1$*. *Then $[\![\pi]\!] = [\![N\pi]\!]$.*

Proof. Each step of the translation from **LCCB**$_1$ to CCB-nets preserves denotation. The less obvious steps are: the translation of the mix rule, which relies on the distributivity of $\otimes$ over $\oplus$; and the binary plus rule, which is based on the equation $\langle 1_A, 1_B\rangle = q_1 + q_2$. □

Now we show that the CCB-net syntax is a faithful model of the category $F\mathcal{A}$. The analysis largely mirrors that carried out for multiplicative linear logic in [Dun04] so the details will be suppressed.

Definition 27. An S-labelled involution on the set $\{1, \ldots, n\}$ is an involutive permutation such that to each transposition is associated a label from some set of labels S.

Theorem 28 (Faithfulness). *Two CCB-nets ν, ν' with the same conclusions Γ are equal iff $[\![\nu]\!] = [\![\nu']\!]$.*

Proof. In order to specify a normal CCB-slice uniquely four data are required:

1. The list of conclusions Γ;
2. An involution θ, labelled by the union of the set arrows of $\mathcal{A}$ and the set $\{0^A_B | A, B \in \mathrm{Obj}_{\mathcal{A}}\}$.
3. A list of booleans B, indicating, for each occurrence of the connective $\oplus$ in Γ, whether the left or right subformula was the premise of the link which introduced it.
4. A multiset L of loops in $\mathcal{A}$.

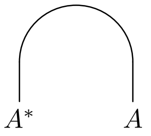
Suppose that f in $\mathcal{A}$ is the denotation of some CCB-slice. By definition 24 it must have the following structure:

$$I \xrightarrow{\cong} \bigotimes_{i=1}^{n} I \xrightarrow{\ulcorner f_1 \urcorner \otimes \cdots \otimes \ulcorner f_n \urcorner} \bigotimes_{i=1}^{n} (A^*_{2i-1} \otimes A_{2i}) \xrightarrow{\sigma} \bigotimes_{i=1}^{2n} A_{\sigma(i)} \xrightarrow{\kappa} \Gamma$$

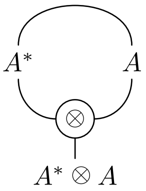
where σ is a permutation, and κ is a tensor product of identities and injections. Given the order of the names $\ulcorner f_i \urcorner$ the data Γ, θ and B suffice to specify σ and κ uniquely. Each loop in L picks out a scalar: to complete the construction of f we multiply by each of these scalars.

Since the denotation of a CB-net ν is just the sum of the denotation of its slices and ν and ν' are equal iff they have the same multisets of slices; so by the above reasoning the set of summands in their denotations must be equal. □

It should be noted that the faithfulness result required the conclusions of the CCB-nets to specified. In fact the syntax is not truly injective onto the arrows of $F\mathcal{A}$. For example, the CCB-nets



and



both denote the map η_A.

Theorem 29 (Kelly-Laplaza). *Each arrow $f : A \to B$ of the free compact closed category on a category $\mathcal{A}$ are completely described by the following data:*

1. *An involution θ on the atoms of $A^* \otimes B$;*
2. *A functor $p : \theta \to \mathcal{A}$ agreeing with θ on objects (i.e. a labelling of θ with arrows of $\mathcal{A}$.);*
3. *A multiset L of loops from $\mathcal{A}$.*

Proof. See [KL80]. □

Definition 30. Let $\mathbf{LCC}_2$ be the sequent calculus defined by the rules on figures 1 and 2 – that is, those rules corresponding to the compact closed structure only. Using the translation given in definition 20, any such proof can be transformed into a one slice CCB-net, where neither plus nor zero link occur. Call such a net a *CC-net*.

Theorem 31 (Full Completeness for the Compact Closed Fragment). *Let $f : \bigotimes_i A_i \to \bigotimes_j B_j$ be an arrow of the free compact closed category on $\mathcal{A}$. Then there is a CC-net ν such that $\ulcorner f \urcorner = [\![\nu]\!]$.*

Proof. By Kelly-Laplaza $f \approx (\theta, p, L)$. The involution θ specifies an axiom links, labelled as per the functor p. For each loop $h : A \to A$ in L, an h-axiom link is added; the loop is closed up with an identity cut. Since $\ulcorner s \bullet f \urcorner = s \bullet \ulcorner f \urcorner$ this suffices. □

5 Further Work

The full completeness result for the $\mathbf{LCC}_1$ subsystem specifies a CCB-slice for each classical branch of a quantum evolution. It seems that that a full completeness result linking the entire compact closed and biproduct structures to $\mathbf{LCCB}_1$ is within reach [Sol87, Del91], but unfortunately not ready for inclusion in this article.

While making use of its equational properties in various proofs, $\mathbf{LCCB}_2$ has no syntax for the strong part of strongly compact closed category with biproducts. In [AC04] this structure is used to define – among other things – the inner product. An inference rule for $(\cdot)^\dagger$ could be a powerful addition to the system.

Finally, although the CCB-net syntax holds out the possibility of a rewrite system for calculating the probabilities weighting the different slices this has not yet been explored. Even at the semantic level the full influence of the structure of the semi-ring of scalars upon the free generated category $F\mathcal{A}$ is unknown.

References

[AC04] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. To appear in LiCS 2004; preprint: arXiv quant-ph/0402130, 2004.

[AHS02] Samson Abramsky, Esfandir Haghverdi, and Philip Scott. Geometry of interaction and linear combinatory algebras. *Mathematical Structures in Computer Science*, 12:625–665, 2002.

[Del91] Pierre Deligne. Catégories tannakiennes. In *Grothendieck Festschrift*, volume 2, pages 111–194. Birkhauser, 1991.

[DR89] Vincent Danos and Laurent Regnier. The structure of multiplicatives. *Arch. Math. Logic*, 28(3):181–203, 1989.

[Dun04] Ross Duncan. Believe it or not, Bell states are a model of multiplicative linear logic. (Available from http://web.comlab.ox.ac.uk/oucl/work/ross.duncan/), 2004.

[Gir87] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1), 1987.

[Gir95] Jean-Yves Girard. Linear logic: its synatx and semantics. In *Advances in Linear Logic*. 1995.

[HvG03] Dominic Hughes and Rob van Glabbeek. Proof nets for unit-free multiplicative-additive linear logic. In *Proc. Logic in Computer Science 2003*. IEEE, 2003.

[JSV96] André Joyal, Ross Street, and Dominic Verity. Traced monoidal categories. *Math. Proc. Camb. Phil. Soc.*, 119:447–468, 1996.

[KL80] G.M. Kelly and M.L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980.

[Mac97] Saunders MacLane. *Categories for the Working Mathematician*. Springer-Verlag, 1997.

[Mit65] B. Mitchell. *Theory of Categories*. Academic Press, 1965.

[Shi96] Masaru Shirahata. A sequent calculus for compact closed categories, 1996.

[Sol87] S. V. Soloviev. On natural transformations of distinguished functors and their superpositions in certain closed categories. *Journal of Pure and Applied Algebra*, 47, 1987.