Abstract Interpretation of Proofs: Classical Propositional Calculus

Martin Hyland

DPMMS, Centre for Mathematical Sciences,
University of Cambridge, England

Abstract. Representative abstract interpretations of the proof theory of the classical propositional calculus are described. These provide invariants for proofs in the sequent calculus. The results of calculations in simple cases are given and briefly discussed.

Keywords: classical propositional calculus, proof theory, category theory.

1 Introduction

1.1 Background

The Curry-Howard isomorphism suugests the connection between proofs in intuitionistic propositional logic, simply typed lambda calculus and cartesian closed categories. This set of ideas provides a context in which constructive proofs can be analysed in a direct fashion. For a treatment in which the category theoretic aspect does not dominate see [13]. By contrast analyses of classical proof theory tend to be indirect: typically one reduces to the contructive case via some form of double-negation translation. (Of course there is also work constructing measures of complexity of classical proofs, but that is not a structural analysis in the sense that there is one for constructive proofs.)

In [16], I sketched a proposal to analyse classical proofs in a direct fashion with the intention inter alia of providing some kind of Curry-Howard isomorphism for classical proof. This is currently the focus of an EPSRC project with principals Hyland (Cambridge), Pym (Bath) and Robinson (Queen Mary). Developments have been interesting. While we still lack natural mathematical semantics for an analysis along the lines of [16], the flaws in the detail proposed there are now ironed out (see [1]). The proof net proposal of Robinson [30] was a response to the difficulties of that approach; it has been considered in depth by Fürhmann and Pym [11]. This leads to more familiar semantics and we have a clear idea as to how this resulting semantics departs from the conception of proof embodied in the sequent calculus. But we are far from understanding the full picture.

One motivation for the project on classical proof was a desire for a systematic approach to the idea of invariants of proofs more flexible than that of complexity analyses. In this paper I try further to support this basic project by describing

J. Marcinkowski and A. Tarlecki (Eds.): CSL 2004, LNCS 3210, pp. 5–20, 2004.

two abstract interpretations of the classical propositional calculus. One should regard these as akin to the abstract interpretations used in strictness analysis. The point is to define and compute interesting invariants of proofs. The abstract interpretations considered here are intended to be degenerate in the same way that the (so-called) relational model is a degenerate model of Linear Logic. There the tensor and par of linear logic are identified; our abstract interpretations identify classical conjunction and disjunction. (The notion of degenerate model for Linear Logic is discussed at greater length in [19].)

In joint work with Power I have tried to put the theory of abstract interpretations on a sound footing. That involves categorical logic of a kind familiar to rather few, so here I leave that aside and simply consider some case studies in the hope of provoking interest. These cases studied can be regarded as representative: they arise from free constructions of two different kinds. I give some calculations (in a bit of a rush - I hope they are right) but do not take the analysis very far. A systematic study even of the interpretations given here would be a major undertaking; but the calculations complement those in [12] which are for special cases of the second class of interpretations considered here.

One should observe that in this paper I get nowhere near the complexities considered by Carbone in [4], [5] and [6]. Carbone's work can also be regarded as a study of abstract interpretations: it is nearest to being a precursor of the approach taken here.

I hope that by and large the notation of the paper will seem standard. However I follow some computer science communities by using diagrammatic motation for composition:

$$f : A \longrightarrow B \quad \text{and} \quad g : B \longrightarrow C$$

compose to give

$$f; g : A \longrightarrow C\,.$$

1.2 Abstract interpretations

We start with some general considerations concerning the semantics of proofs in the sequent calculus for the classical propositional calculus. The basic idea, which goes back to Szabo, is to take the CUT rule as giving the associative composition in some polycategory. If we simplify (essentially requiring representability of polymaps) along the Fürhmann-Pym-Robinson lines we get the following.

Definition 1. *A* model of classical propositional proof satisfying the Fürhmann-Pym-Robinson equations *consists of the following data.*

- *A $*$-autonomous category $\mathbb{C}$: here the tensor is the conjunction $\wedge$, and its unit is the true $\top$; dually the par is the disjunction $\vee$, and its unit is the false $\bot$.*
- *The equipment on each object A of $\mathbb{C}$ of the structure of a commutative comonoid with respect to tensor.*
- *The equipment on each object A of $\mathbb{C}$ of the structure of a commutative monoid with respect to par.*

One requires in addition

- *that the commutative comonoid structure is compatible with the tensor structure (so* $\top$ *has the expected comonoid structure and comonoid structure is closed under* $\wedge$*);*
- *that the commutative monoid structure is compatible with the par structure (so* $\perp$ *has the expected monoid structure and monoid structure is closed under* $\vee$*);*
- *and that the structures correspond under the duality (so that the previous two conditions are equivalent).*

There are further categorical nuances which we do not discuss here.

The interpretation of classical proofs in such a structure is a straightforward extension of the interpretation of multiplicative linear proofs in a $*$-autonomous category. The algebraic structure deals with the structural rules of the sequent calculus. The several requirements added are natural simplifying assumptions. They do not really have much proof theoretic justification as things stand.

As indicated above we take a notion of abstract interpretation which arises by the identification of the conjunction $\wedge$ and disjunction $\vee$.

Definition 2. *By an* abstract interpretation of classical proof *we mean a compact closed category in which each object* A *is equipped with*

- *the structure* $t : A \to I, d : A \to A \otimes A$ *of a commutative comonoid,*
- *the structure* $e : I \to A, m : A \otimes A \to A$ *of a commutative monoid,*

with the structures

- *compatible with the monoidal structure* $(I, \otimes)$*, and*
- *and interchanged under the duality* $(-)^*$*.*

One should note that the optical graphs of Carbone [4] are in effect abstract interpretations, but in a more general sense than that considered here.

We gloss the definition a little. According to it, each object is equipped with commutative monoid structure to model the structural rules for $\vee$ and with commutative comonoid structure to model the structural rules for $\wedge$. Naturally we expect the structural rules to be interchanged by the duality $(-)^*$. Modulo natural identifications we have

$$(t_A)^* = e_{A^*} : I \to A^* \,, \qquad (e_A)^* = t_{A^*} : A^* \to I \,,$$
$$(d_A)^* = m_{A^*} : A^* \otimes A^* \to A^* \,, \; (m_A)^* = d_{A^*} : A^* \to A^* \otimes A^* \,.$$

In addition we ask that the structure be compatible with the monoidal structure. This means first that I should have the expected structure

$$t_I = \mathrm{id}_I : I \to I \,, \; d_I = \tilde{l}_I = \tilde{r}_I : I \to I \otimes I \,,$$
$$e_I = \mathrm{id}_I : I \to I \,, m_I = l_I = r_I : I \otimes I \to I \,,$$

derived from the unit structure

$$l_A : I \otimes A \to A \; r_A : A \otimes I \to A$$
$$\tilde{l}_A : A \to I \otimes A \; \tilde{r}_A : A \to A \otimes I$$

for the tensor unit I. In addition it means that the structures are preserved by tensor: that is, modulo associativities we have

$$d_{A\otimes B} = d_A \otimes d_B; \mathrm{id}_A \otimes c_{A,B} \otimes \mathrm{id}_B : A \otimes B \to A \otimes B \otimes A \otimes B\,,$$
$$m_{A\otimes B} = \mathrm{id}_A \otimes c_{A,B} \otimes \mathrm{id}_B; m_A \otimes m_B : A \otimes B \otimes A \otimes B \to A \otimes B\,.$$

For the moment it is best to regard these requirements as being justified by the models which we are able to give.

1.3 Strictness

Any honest consideration of categorical structure should address questions of strictness. In particular one has the distinction between functors preserving structure on the nose and functors preserving structure up to (coherent) natural isomorphism. A setting in which such issues can be dealt with precisely is laid out in [2]. The only issue which need concern us here is that of the strictness of the structure in our definition of abstract interpretation.

We shall largely deal with structures freely generated by some data. So it will be simplest for us to take the monoidal structure to be strictly associative. Similarly we shall be able to take the duality to be strictly involutive so that

$$(f : A \to B)^{**} = (f : A \to B)$$

and to respect the monoidal structure, so that on objects

$$I^* = I \quad \text{and} \quad (A \otimes B)^* = B^* \otimes A^*$$

on the nose, and similarly for maps. Note further that duality in a compact closed category provides adjunctions for all the 1-cells of the corresponding one object bicategory. That is very much choice of structure: so for us every object A is equipped with a left (say) dual A^* with explicit unit and counit

$$I \longrightarrow A \otimes A^* \quad \text{and} \quad A^* \otimes A \longrightarrow I\ .$$

This is all as explained in [21]. But one should go further: in general there should be natural coherence diagrams connecting the adjunction for $A \otimes B$ with the adjunctions for A and B. (In a sense these conditions parallel the assumption that the comonoid and monoid structures are preserved under tensor product. The relevent coherence theorem extending [21] is not in principle hard, but we do not need it here.)

For the purposes of this paper one can take the definition of abstract interpretation in the strict sense indicated. But not much depends on that: the critical issue for the background theory is simply that the notion is given by algebraic structure over Cat in the sense of [22]. A reader to whom all this is foreign should still understand the examples.

1.4 Miscellaneous examples

Before turning to the interpretations which are our chief concern, we give a few natural examples of abstract interpretations. For this section we ignore strictness issues.

1. Consider the category **Rel** of sets and relations equipped with the set theoretic product $\times$ as tensor product. **Rel** is compact closed; it is contained in the compact closed core of **SupLat** the category of complete lattices and sup-preserving maps. The duality is

$$(-)^* \quad : (A \xrightarrow{F} B) \longrightarrow (B \xrightarrow{F^{op}} A)$$

in particular is the identity on objects. For each object $A \in$ **Rel** there is a natural choice of commutative comonoid structure arising from product in **Set**. By duality that gives a choice of commutative monoid structure on all objects, and by definition the structures are interchanged by the duality. This gives a simple abstract interpretation.

2. We can extend the above example to one fundamental to Winskel's Domain Theory for Concurrency (see [27] for example). Following [27] write **Lin** (after Linear Logic) for the category with objects preordered sets and maps profunctors between them. We can regard this also as being within the compact closed core of **SupLatt**. We equip the preordered set $\mathbb{P}$ with comonoid structure via the counit

$$t_{\mathbb{P}} : \mathbb{P} \longrightarrow 1 \qquad t_{\mathbb{P}}(a, \star) = \text{true}$$

and the comultiplication

$$d_{\mathbb{P}} : \mathbb{P} \longrightarrow \mathbb{P} \times \mathbb{P} \qquad d_{\mathbb{P}}(a, (b, c)) = a \geq b \text{ and } a \geq c\,,$$

extending the definition for **Rel**. The duality is

$$(-)^* : (\mathbb{P} \xrightarrow{F} \mathbb{Q}) \longrightarrow (\mathbb{Q}^{op} \xrightarrow{F^{op}} \mathbb{P}^{op})$$

and this is no longer the identity on objects. The duality induces the monoid structure from the comonoid structure so the structures are automatically interchanged by duality.

3. Let **FVec** be the category of finite dimensional k-vector spaces (and k-linear maps) for a field k. A *commutative bialgebra* is an object A of **FVec** equipped with the structure

$$t : A \to I, \quad d : A \to A \otimes A$$

of a commutative comonoid and the structure

$$e : I \to A, m : A \otimes A \to A$$

of a commutative monoid, satisfying the equations

$$
\begin{aligned}
e_A; t_A &= \mathrm{id}_I \\
m_A; t_A &= t_A \otimes t_A; m_I \\
e_A; d_A &= d_I; e_A \otimes e_A \\
m_A; d_A &= d_A \otimes d_A; \mathrm{id}_A \otimes c_{A,A} \otimes \mathrm{id}_A; m_A \otimes m_A
\end{aligned}
$$

(Hopf algebras (that is, bialgebras with antipode) are amongst the staples of representation theory. There is a plentiful supply of such: the standard group algebra kG of a finite group G is a Hopf algebra.) If we take the category whose objects are bialgebras, with maps linear maps of the underlying vector spaces, we get an abstract interpretation in our sense.

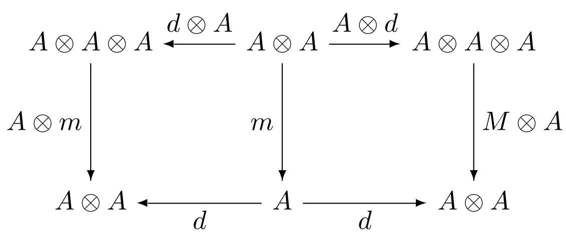
2 Frobenius Algebras

2.1 Frobenius abstract interpretations

Definition 3. *A* commutative Frobenius algebra *in a symmetric monoidal category is an object A equipped with the structure $A, t : A \to I, d : A \to A \otimes A$ of a commutative comonoid and the structure $A, e : I \to A, m : A \otimes A \to A$ of a commutative monoid, satisfying the equation*

$$A \otimes d; m \otimes A = m; d = d \otimes A; A \otimes m\,.$$

Note that an algebra is a module over itself (on the left and on the right), and a coalgebra a comodule over itself (again on both sides). We can write the Frobenius equations in diagrams as



and we see that they say that d is a map of right and left modules. Equivalently (and by symmetry) they say that m is a map of right and left comodules.

In mathematics algebras with a Frobenius structure have played a role in representation theory for a century, certainly since Frobenius [10]. The condition is explicitly identified in work of T. Nakayama and C. Nesbitt from the late 1930s. Sources for this early history are mentioned in [23]. An important conceptual understanding of the Frobenius condition or structure was suggested by Lawvere [24].

Definition 4. *We say that an abstract interpretation is* Frobenius *if all the comonoid and monoid structures satisfy the equations of a Frobenius algebra.*

We note that for an object A in **Rel** one readily calculates that

$$A \otimes d; m \otimes A = m; d = d \otimes A; A \otimes m$$

is the relation $A \times A \to A \times A$ identifying equal elements of the diagonal. So **Rel** is a Frobenius abstract interpretation. In view of remarks below, one could regard this as explaining why the objects in **Rel** are self-dual! One the other hand it is easy to see that the Frobenius condition fails for **Lin**. This is related to the fact that we do not generally have $\mathbb{P}^{op} \cong \mathbb{P}$ for posets $\mathbb{P}$.

Since the comonoid structure of a Frobenius algebra is not natural with respect to the monoid structure (and dually not vice-versa either), we are not dealing with a commutative sketch in the sense of [17]: rather one needs the more general theory of [18]. As a consequence the identification of the free Frobenius algebra, given in the next section, is non-trivial. However a simplifying feature of Frobenius algebras is that they carry their own duality with them. In fact Frobenius algebras are self dual: one has the unit

$$I \xrightarrow{e_A} A \xrightarrow{d_A} A \otimes A\,,$$

and the counit

$$A \otimes A \xrightarrow{m_A} A \xrightarrow{t_A} I\,.$$

By straightforward calculation one has

$$\begin{aligned}(e_A; d_A) \otimes \mathrm{id}_A; \mathrm{id}_A \otimes (m_A; t_A) &= e \otimes \mathrm{id}_A; d \otimes \mathrm{id}_A; \mathrm{id}_A \otimes m; \mathrm{id}_A \otimes t\\ &= e \otimes \mathrm{id}_A; m; d; \mathrm{id}_A \otimes t\\ &= \mathrm{id}_A; \mathrm{id}_A = \mathrm{id}_A\end{aligned}$$

giving one of the triangle identities; And symmetrically one has

$$\mathrm{id}_A \otimes (e_A; d_A); (m_A; t_A) \otimes \mathrm{id}_A$$

which is the other. This shows that in any symmetric monoidal closed category the Frobenius objects live in the compact closed core. Moreover it is easy to see that the intrinsic duality interchanges the comonoid and monoid structures on a Frobenius algebra. So the abstract interpretation aspect is also automatic. So overall to give abstract interpretations it suffices to find Frobenius algebras in some symmetric monoidal closed category.

2.2 The free Frobenius algebra

In recent times the study of Frobenius algebras has become compelling following the identification of 2-dimensional Topological Quantum Field Theories (TQFT) with commutative Frobenius algebras [9]. A readable intuitive explanation is given in [23]. In essence this arises from an identification of the free symmetric monoidal category generated by a Frobenius algebra. We state this in the customary rough and ready way: though we make some of the ideas more precise in a moment, there is a limit to what it is useful to do here.

Proposition 1. *The free symmetric monoidal category generated by a Frobenius algebra can be described in the following equivalent ways.*
1. It is the category of topological Riemann Surfaces. Objects are finite disjoint sums of the circle and maps (from n circles to m circles) are homeomorphism classes of surfaces with boundary consisting of $n+m$ marked circles.
2. It is the category of one dimensional finitary topology up to homology. The objects are finite discrete sets of points and the maps from n points to m points are homology classes of one dimensional simplicial complexes with $n+m$ marked points as boundary.

To make things more precise, we might as well engage at once with the strict version of the above. In that view the free symmetric monoidal category generated by a Frobenius algebra has objects

$$0,\ 1,\ 2,\ \dots,n,\ \dots$$

which should be regarded as representatives of finite sets. The maps from n to m are determined by an equivalence relation on $n+m$, which one can think of as giving connected components topologically, together with an association to each of these connected components of a natural number (the genus).

Dijkgraaf's identification of two-dimensional TQFT has been independentally established more or less precisely by a number of people. I not unnaturally like the account in Carmody [7] which already stresses the wiring diagrams in the sense of [17] and [18], as well as rewriting in the style of the identification of the simplicial category by generators and relations [26]. We shall show that the TQFT aspect of Frobenius algebras runs parallel to a simple topological idea of abstract interpretation.

2.3 Representative Calculations

We consider here the obvious interpretation of classical proofs in the symmetric monoidal category generated by a Frobenius algebra. In this interpretation all atomic propositions are interpreted by the generating Frobenius algebra, so are not distinguished. Also the interpretation is not sensitive to negation. Despite that the intrepretation does detect some structural features of proofs. We already explained the data for a map in the free symmetric monoidal category generated by a Frobenius algebra: it consists of a collection of connected components and a genus attached to each. A proof π in classical propositional logic gives rise to its interpretation $V(\pi)$ which is thus a map of this kind. One loses just a lttle information if one considers only the invariants given by the homology

$$H_0(\pi) = H_0(V(\pi), \mathbb{Q}) \quad \text{and} \quad H_1(\pi) = H_1(V(\pi), \mathbb{Q})$$

of a proof π. We set

$$h_0(\pi) = \dim H_0(\pi) \quad \text{and} \quad h_1(\pi) = \dim H_1(\pi)\,.$$

Usually we ensure there will be just one connected component so that one loses no information in passing to homology: the invariant reduces to the genus usually written $g = h_1(\pi)$.

1. **Proofs in MLL** The Frobenius algebra interpretation of proofs in Multiplicative Linear Logic should be regarded as one of the fundamentals of the subject. For simplicity we follow [14] in dealing with a one-sided sequent calculus.
   - For an axiom
   $$A \vdash^{\alpha} A$$
   we have
   $$h_0(\alpha) = 1 \quad \text{and} \quad h_1(\alpha) = 0\,.$$
   - For the $\wedge$-R rule
   $$\frac{\vdash^{\pi_1} \Gamma, A \quad \vdash^{\pi_2} \Delta, B}{\vdash^{\pi} \Gamma, \Delta, A \wedge B}$$
   we have
   $$h_0(\pi) = h_0(\pi_1) + h_0(\pi_2) + 1 \quad \text{and} \quad h_1(\pi) = h_1(\pi_1) + h_1(\pi_2)\,.$$
   - For the $\vee$-L rule
   $$\frac{\vdash^{\pi'} \Gamma, A, B}{\vdash^{\pi} \Gamma, A \vee B}$$
   we have
   $$h_0(\pi) = h_0(\pi') \quad \text{and} \quad h_1(\pi) = h_1(\pi') + 1\,.$$

   The final claims need to be justified inductively using the fact that we always have one connected component, that is, we always have $h_0 = 1$.
   We deduce from the above that for a proof π, in multiplicative linear logic, the genus counts the number of pars (that is for us occurences of $\vee$) in the conclusions. Thus the Frobenius algebra interpretation points towards the Danos-Regnier correctness criterion. (My student Richard Garner has given a full analysis along these lines.)
2. **Distributive law** Perhaps the simplest interesting non-linear proofs are those of the distributive laws. Consider first the proof
   $$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, B \vdash A \wedge B} \quad \dfrac{A \vdash A \quad C \vdash C}{A, C \vdash A \wedge C}}{A, A, B \vee C \vdash A \wedge B, A \wedge C}}{A, B \vee C \vdash A \wedge B, A \wedge C}}{A \wedge (B \vee C \vdash (A \wedge B) \vee (A \wedge C)\,.}$$

   From the proof net one readily sees that one has $h_0 = 1$, that is one has one connected component, and that $h_1 = 3$. There are just two occurences of $\vee$, so a linear proof would have $h_1 = 2$. Thus the invariant does detect the non-linearity.
   I do not give here the most natural proof of the converse distributive law: $(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C)$. It seems necessarily more complex, in that the most obvious proof has $h_0 = 1$ but $g = h_1 = 8$. The proof does not just reverse.

3. **The Natural Numbers** Recall that (up to $\beta\eta$-equivalence) the constructive proofs of $(A \Rightarrow A) \Rightarrow (A \Rightarrow A)$ correspond to the Church numerals in the lambda calculus. (Implicitly we should rewrite $(A \Rightarrow A) \Rightarrow (A \Rightarrow A)$ as $(A \wedge \neg A) \vee (\neg A \vee A)$; but there are obvious corresponding proofs.) Let π_n be the proof given by the nth Church numeral $\lambda f, x. f^n(x)$. We compute the invariants for these proofs π_n. With just one conclusion we have forced $h_0(\pi_n) = 1$, so we just look at the genus. The proof net picture immediately show us that $h_1(\pi_n) = n + 1$. So the invariant readily distingushes these proofs.
   Now consider what it is to compose proofs π_n and π_m with the proof $\mu = \lambda a, b, f.\, a(b(f))$ of

$$(A \Rightarrow A) \Rightarrow (A \Rightarrow A)\,,\, (A \Rightarrow A) \Rightarrow (A \Rightarrow A) \vdash (A \Rightarrow A) \Rightarrow (A \Rightarrow A)$$

   corresponding to multiplication on the Church numerals. This gives a proof $\mu|\pi_n|\pi_m$ with cuts. We compute the invariants for the interpretation $V(\mu|\pi_n|\pi_m)$ in our model. This is just an exercise in counting holes. Generally we find that

$$h_0(\mu|\pi_n|\pi_m) = 1 \quad \text{and} \quad h_1(\mu|\pi_n|\pi_m) = n + m\,.$$

   However the case $n = m = 0$ is special. We get

$$h_0(\mu|\pi_0|\pi_0) = 2 \quad \text{and} \quad h_1(\mu|\pi_0|\pi_0) = 1\,.$$

   (Note that the Euler characteristic is consistent!)
   Of course if we reduce $\mu|\pi_n|\pi_m$ to normal form we get π_{nm} with

$$h_0(\pi_{nm}) = 1 \quad \text{and} \quad h_1(\pi_{nm}) = nm + 1\,.$$

   So the interpretation distinguishes proofs from their normal forms. The need to think this way about classical proof was stressed in [16].

3 Traced monoidal categories

3.1 Background

With our Frobenius Algebra interpretation we got the compact closed aspect of our abstract interpretation for free. For our second example we exploit a general method for contructing compact closed categories from traced monoidal categories. We recall the basic facts concerning traced monoidal categories. We do not need the subtleties of the braided case explained in the basic reference [20]. So for us a *traced monoidal category* is a symmetric monoidal category equipped with a trace operation

$$\frac{f : A \otimes U \to B \otimes U}{\mathrm{tr}(f) : A \to B}$$

satisfying elementary properties of feedback. A useful perspective and diagrams without the braidings in [20] is provided by Hasegawa [15]. It is a commonplace amongst workers in Linear Logic that traced monoidal categories provide a backdrop to Girard's Geometry of Interaction.

If $\mathbf{C}$ is a traced monoidal category, then its integral completion $\mathrm{Int}(\mathbf{C})$ is defined as follows.

- The objects of $\mathrm{Int}(\mathbf{C})$ are pairs (A_0, A_1) of objects of $\mathbf{C}$.
- Maps $(A_0, A_1) \to (B_0, B_1)$ in $\mathrm{Int}(\mathbf{C})$ are maps $A_0 \otimes B_1 \to B_0 \otimes A_1$ of $\mathbf{C}$.
- Composition of $f : (A_0, A_1) \to (B_0, B_1)$ and $g : (B_0, B_1) \to (C_0, C_1)$ is given by taking the trace $\mathrm{tr}(\sigma; f \otimes g; \tau)$ of the composite of $f \otimes g$ with the obvious symmetries
$$A_0 \otimes C_1 \otimes B_0 \otimes B_1 \xrightarrow{\sigma} A_0 \otimes B_1 \otimes B_0 \otimes C_1\,,$$
and
$$B_0 \otimes A_1 \otimes C_0 \otimes B_1 \xrightarrow{\tau} C_0 \otimes A_1 \otimes B_0 \otimes B_1\,.$$
- Identities $(A_0, A_1) \to (A_0, A_1)$ are given by the identity $A_0 \otimes A_1 \to A_0 \otimes A_1$.

The basic result from [20] is the following.

Theorem 1. *(i) Suppose that* $\mathbf{C}$ *is a traced monoidal category. Then* $\mathrm{Int}(\mathbf{C})$ *is a compact closed category.*
(ii) Int *extends to a* 2*-functor left biadjoint to the forgetful* 2*-functor from compact closed categories to traced monoidal categories.*

3.2 Abstract Interpretations via traces

Suppose that we have a traced monoidal category $\mathbf{C}$ in which every object A is equipped with the structure of a commutative comonoid
$$I \xleftarrow{w} A \xrightarrow{d} A \otimes A$$
and of a commutative monoid
$$I \xrightarrow{e} A \xleftarrow{m} A \otimes A\,.$$
Consider the compact closed category $\mathrm{Int}(\mathbf{C})$. Given an object (A_0, A_1), we have maps
$$(A_0, A_1) \longrightarrow (I, I) \quad \text{given by} \quad A_0 \otimes I \xrightarrow{w \otimes e} I \otimes A_1$$
$$(A_0, A_1) \longrightarrow (A_0 \otimes A_0, A_1 \otimes A_1) \quad \text{given by} \quad A_0 \otimes A_1 \otimes A_1 \xrightarrow{d \otimes m} A_0 \otimes A_0 \otimes A_1$$
which clearly equip it with the structure of a commutative comonoid; and dually we have maps
$$(I, I) \longrightarrow (A_0, A_1) \quad \text{given by} \quad I \otimes A_1 \xrightarrow{e \otimes w} A_0 \otimes I$$
$$(A_0 \otimes A_0, A_1 \otimes A_1) \longrightarrow (A_0, A_1) \quad \text{given by} \quad A_0 \otimes A_0 \otimes A_1 \xrightarrow{m \otimes d} A_0 \otimes A_1 \otimes A_1$$

which equip it with the structure of a commutative monoid. These structures are manifestly interchanged (on the nose) by the duality. Thus such situations will always lead to abstract interpretations.

3.3 Traced Categories with biproducts

We consider the special case where the tensor product in a traced monoidal category is a biproduct (see for example [25]). Under these circumstances one has a canonical choice of commutative comonoid and monoid structure, and so a natural abstract interpretation.

We recall that a category $\mathcal{C}$ with biproducts is enriched in commutative monoids. More concretely each hom-set $\mathcal{C}(A, B)$ is equipped with the structure of a commutative monoid (which we write additively) and composition is bilinear in that structure. It follows that for each object A its endomorphisms $\mathrm{End}_{\mathcal{C}}(A) = \mathcal{C}(A, A)$ has the structure of what is now called a rig, that is to say a (commutative) ring without negatives. One can explain in these terms what it is to equip a category with biproducts with a trace. Here we concentrate on the one object case, which is the only case considered in the main reference [3].

We recall the notion of Conway Algebra (essentially in Conway [8]) as articulated in [3]

Definition 5. *A Conway Algebra is a rig A equipped with a unary operation*

$$(-)^* : A \longrightarrow B\,;\, a \to a^*$$

satisfying the two equations

$$(ab)^* = 1 + a(ba)^* b$$
$$(a + b)^* = (a^* b)^* a^*$$

It is immediate that in a traced monoidal category $\mathbf{C}$ whose tensor product is a biproduct each $\mathrm{End}_{\mathbf{C}}(A)$ is a Conway Algebra, the operation $(-)^*$ being given by

$$a^* = \mathrm{tr} \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} .$$

In the case of a category generated by a single object U, the requirement that $\mathrm{End}_{\mathbf{C}}(U)$ be a Conway algebra is in fact sufficient. Generally one takes the trace of a map $A \oplus C \longrightarrow B \oplus C$ given by the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a \in \mathcal{C}(A, B)$, $b \in \mathcal{C}(C, B)$, $c \in \mathcal{C}(A, C)$ $d \in \mathcal{C}(C, C)$ using the natural formula

$$\mathrm{tr} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + bd^* c$$

So to identify the free traced monoidal category with biproducts on an object U it suffices to identify the free Conway algebra on no generators.

Fortunately that is already known. In [8] Conway effectively identifies the elements of the free Conway algebra on no generators: the distinct elements are those of the form

$$\{n \mid n \geq 0\} \cup \{n(1^*)^m \mid n, m \geq 1\} \cup \{1^{**}\}.$$

The algebraic structure can be deduced from the following absorbtion rules.

$$\begin{gathered} 1 + (1^*)^n = (1^*)^n \\ (1^*)^n + 1^{**} = 1^{**} + 1^{**} = 1^{**} \\ n.1^{**} = 1^*.1^{**} = 1^{**}.1^{**} = 1^{**} \\ 1^{***} = 2^* = 1^{**} \end{gathered}$$

3.4 Representative Calculations

The objects in the free traced monoidal category with biproducts generated by a single object are (as we had earlier)

$$0,\ 1,\ 2,\ \ldots, n,\ \ldots$$

representatives of finite sets. But now the maps from n to m are given by $m \times n$ matrices with entries in the free Conway algebra just described.

Taking Int gives us objects of the form (n, m) with n and m finite cardinals. We consider the interpretation which arises when each atomic proposition A is interpreted by the object $(1, 0)$ with $\neg A$ therefore interpreted by $(0, 1)$. Proofs π will have interpretations $V(\pi)$ which will be suitably sized matrices as above.

1. **Proofs in MLL** The data in an interepretation of a proof in multiplicative linear logic is familiar. Again we follow [14] by considering only one sided sequents. Suppose we have $\vdash^{\pi} \Gamma$. There will be some number, n say, of occurences of atomic propositions (literals) and the same number of the corresponding negations. So Γ will be interpreted by the object (n, n), and π by an $n \times n$ matrix. For MLL this matrix will always be a permutation matrix giving the information of the axiom links in π. (Of course the permutation is just a construct of the order in which the literals and their negations are taken.)
2. **Distributive laws** For simple proofs like those of the distributive laws the interpretation continues just to give information akin to that of axiom links. Consider first the proof of

$$A \wedge (B \vee C \vdash (A \wedge B) \vee (A \wedge C)$$

which we gave earlier. The interpretation is a map from $(3, 0$ to $(4, 0)$, and so is given by a 4×3 matrix: it is

$$\begin{pmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 1\,0\,0 \\ 0\,0\,1 \end{pmatrix}.$$

The natural proof of the converse distributive law,

$$(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C)\,,$$

may seem more complicated, but our current interpretation does not notice that. One gets

$$\begin{pmatrix} 1\,0\,1\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \end{pmatrix}\,,$$

which is just the transpose of the previous matrix.

3. **Natural Numbers** The interpretation of $(A \Rightarrow A) \Rightarrow (A \Rightarrow A)$ is $(2, 2)$ so the natural number proofs π_n are interpreted as 2×2 matrices. We get

$$V(\pi_0) = \begin{pmatrix} 0\,0 \\ 0\,1 \end{pmatrix}\,, \qquad V(\pi_{n+1}) = \begin{pmatrix} n\,1 \\ 1\,0 \end{pmatrix}\,.$$

As before we consider what it is to compose proofs π_n and π_m with the proof $\mu = \lambda a, b, f.\, a(b(f))$ of multiplication. This is interpreted by the (obvious permutation) matrix

$$\begin{pmatrix} 0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1 \\ 1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,0\,0 \end{pmatrix}$$

where the first two rows and columns come from the codomain. Essentially we have to compose and take a trace. At first sight this is not very exciting and things seem much as before. We find

$$V(\mu|\pi_{n+1}|\pi_{m+1}) = \begin{pmatrix} n+m & 1 \\ 1 & 0 \end{pmatrix}\,.$$

But the connectivity of π_0 introduces an unexpected nuance. To compute $V(\mu|\pi_0|\pi_{m+1})$, we can compose one way to get the matrix

$$\begin{pmatrix} 0\,0\,0\,0 & 0 & 0 \\ 0\,0\,0\,0 & 1 & 0 \\ 1\,0\,0\,0 & 0 & 0 \\ 0\,0\,0\,0 & m & 1 \\ 0\,0\,0\,1 & 0 & 0 \\ 0\,1\,0\,0 & 0 & 0 \end{pmatrix}$$

and then we need to take a not so obvious trace. We end up with

$$V(\mu|\pi_0|\pi_{m+1}) = \begin{pmatrix} 0 & 0 \\ 0 & m^* \end{pmatrix}\,.$$

For $V(\mu|\pi_0|\pi_0)$, the calculations are marginally simpler and we end up with

$$V(\mu|\pi_0|\pi_0) = \begin{pmatrix} 0 & 0 \\ 0 & 1^* \end{pmatrix} .$$

One sees that even simple cuts can produce cycles in a proof of a serious kind, and these are detected by our second interpretation.

4 Summary

In this paper I hope to have presented evidence that there are mathematical interpretations of classical proof which produce what can be regarded as invariants of proofs. Clearly there are many more possibilities than those touched on here. It seems worth making a couple of concluding comments.

First while the interpretations given do handle classical proofs, they do not appear to detect any particular properties of them. All examples given concern (very simple) familiar constructive proofs. There would have been no special interest for example in treating Pierce's Law.

Secondly, these interpretations are sensitive to cut elimination. This appears to be a necessary feature of any mathematical theory of classical proof respecting the symmetries. Even for constructive prrofs it suggests a quite different criterion for the identity of proofs than that given by equality of normal form. This criterion would have the merit of being sensitive inter alia to the use of Lemmas in mathematical practice.

References

1. G. Bellin and M. Hyland and E. Robinson and C. Urban. Proof Theory of Classical Logic. In preparation.
2. R. Blackwell and G. M. Kelly and A. J. Power. Two-dimensional monad theory. *Journal of Pure and Applied Algebra* **59** (1989), 1–41.
3. S. L. Bloom and Z. Esik. *Iteration Theories.* Springer-Verlag, 1993.
4. A. Carbone. Duplication of directed graphs and exponential blow up of proofs. *Annals of Pure and Applied Logic* **100** (1999), 1–67.
5. A. Carbone. Asymptotic cyclic expansion and bridge groups of formal proofs. *Journal of Algebra*, 109–145, 2001.
6. A.Carbone, Streams and strings in formal proofs. *Theoretical Computer Science*, 288(1):45–83, 2002.
7. S. Carmody. *Cobordism Categories.* PhD Dissertation, University of Cambridge, 1995.
8. J. H. Conway. *Regular algebra and finite machines.* Chapman and Hall, 1971.
9. R. Dijkgraaf. *A geometric approach to two dimensional conformal field theory.* Ph.D. Thesis, Univeristy of Utrecht, 1989.
10. G. Frobenius. Theorie der hyperkomplexen Grössen. *Sitzungsbereich K. Preuss Akad. Wis.* **24** 1903, 503–537, 634–645.
11. C. Führmann and D. Pym. Order-enriched Categorical Models of the Classical Sequent Calculus. Submitted.

12. C. Führmann and D. Pym. On the Geometry of Interaction for Classical Logic (Extended Abstract). To appear in Proceedings LICS 04, IEEE Computer Society Press, 2004.
13. J.-Y. Girard. *Proofs and Types.* Cambridge University Press, 1989.
14. J.-Y. Girard. Linear Logic. *Theoretical Computer Science* **50**, (1987), 1–102.
15. M. Hasegawa. *Models of sharing graphs. (A categorical semantics for* Let *and* Letrec.*)* Distinguished Dissertation in Computer Science, Springer-Verlag, 1999.
16. J. M. E. Hyland. Proof Theory in the Abstract. *Annals of Pure and Applied Logic* **114** (2002), 43–78.
17. M. Hyland and J. Power. Symmetric monoidal sketches. *Proceedings of PPDP 2000*, ACM Press (2000), 280–288.
18. M. Hyland and J. Power. Symmetric monoidal skecthes and categories of wiring diagrams. *Proceedings of CMCIM 2003*, to appear.
19. M. Hyland and A. Schalk. Glueing and Orthogonality for Models of Linear Logic. *Theoretical Computer Science* **294** (2003) 183–231.
20. A. Joyal and R. Street and D. Verity. Traced monoidal categories. *Math. Proc Camb Phil. Soc.* **119** (1996), 425–446.
21. G. M. Kelly and M. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra* **19** (1980), 193–213.
22. G. M. Kelly and A. J. Power. Adjunctions whose counits are equalizers, and presentations of finitary enriched monads. *Journal of Pure and Applied Algebra* **89** (1993), 163–179.
23. J. Kock. *Frobenius Algebras and 2D Topological Quantum Field Theories.* Cambridge University Press, 2003.
24. F. W. Lawvere. Ordinal sums and equational doctrines. In *Seminar on Triples and Categorical Homology Theory*, LNM **80** (1969), 141–155.
25. S. Mac Lane. *Categories for the working mathematician.* Graduate Texts in Mathematics **5**. Springer (1971).
26. J. P. May. *Simplicial objects in algebraic topology.* Van Nostrand, Princeton. 1967.
27. M. Nygaard and G. Winskel. Domain Theory for Concurrency. *Theoretical Computer Science*, to appear.
28. A. J. Power and E. P. Robinsons. A characterization of PIE limits. *Math. Proc. Camb. Phil. Soc.* **110**, (1991), 33–47
29. D. Prawitz. Ideas and results in proof theory. In *Proceedings of the Second Scandinavian Logic Symposium.* J.-E. Fenstad (ed), North-Holland 1971, 237–309.
30. E. P. Robinson. Proof Nets for Classical Logic. *Journal of Logic and Computation.* **13**, 2003, 777–797.
31. M. E. Szabo. Polycategories. *Comm. Alg.* **3** (1997), 663–689.