ISOMORPHISMS IN A CATEGORY OF PROOFS

Greg Restall

Philosophy Department, The University of Melbourne
restall@unimelb.edu.au

MIT SLLEGR SEMINAR * 20 APRIL 2018

I aim to show how a category of propositional formulas and classical proofs can give rise to finely grained hyperintensional notions of sameness of content. One notion is very finely grained (distinguishing \( p \) and \( p \land p \)), others less so. I show that one notion amounts to equivalence in Richard Angell’s logic of analytic containment [1].

1 THE CATEGORY OF CLASSICAL PROOFS

Four different derivations, and two proofs.

\[
\begin{align*}
\frac{p > p}{p \land q > p} \quad \frac{p > p}{p \lor q > p} & \quad \frac{p \land q > q}{p \land q > p \lor q} \quad \frac{p \lor q > q}{p \lor q > p \land q} \\
\frac{p \land q > q}{p \land q > p \lor q} \quad \frac{p \lor q > q}{p \lor q > p \land q} & \quad \frac{p \lor q > q}{p \lor q > p \land q} \quad \frac{p \land q > q}{p \land q > p \lor q}
\end{align*}
\]

Motivating idea: Proof terms are an invariant for derivations under rule permutation. \( \delta_1 \) and \( \delta_2 \) have the same term iff some permutation sends \( \delta_1 \) to \( \delta_2 \).

More examples:

\[
\begin{align*}
(p \land q) \lor (p \land r) & \quad (p \lor q) \lor (p \lor r)
\end{align*}
\]

Links wholly internal to a premise or a conclusion are called caps (\(<\rightarrow\)) and ends (\(<\sim\)).

FACTS: Not every directed graph on occurrences of atoms in a sequent is a proof term. \( \forall \) They typecheck. [An occurrence of \( p \) is linked only with an occurrence of \( p \).] \( \forall \) They respect polarities. [Positive occurrences of atoms in premises and negative occurrences of atoms in conclusions are inputs. Negative occurrences of atoms in premises and positive occurrences of atoms in conclusions are outputs.] \( \forall \) They must satisfy an “enough connections” condition, amounting to a non-emptyness under every switching. [e.g. the obvious linking between premise \( p \lor q \) and conclusion \( p \land q \) is not connected enough to be a proof term.]

Cut is chaining of proof terms, composition of graphs.

\[
\begin{align*}
(p \land q) \lor (p \land r) & \quad (p \lor q) \lor (p \lor r)
\end{align*}
\]

Cut elimination is confluent and terminating. [So it can be understood as a kind of evaluation.] \( \forall \) Cut elimination for proof terms is local. [So it is easily made parallel.]

\( \mathcal{C} \) is the Category of Classical Proofs. objects: Formulas \( \rightarrow \) \( A \), \( B \), etc. Arrows: Cut-Free Proof Terms \( \rightarrow \) \( \pi : A \rightarrow B \). Composition: Composition of derivations with the elimination of Cut. If \( \pi : A \rightarrow B \) and \( \tau : B \rightarrow C \) then \( \tau \circ \pi : A \rightarrow C \). Identity: Canonical identity proofs \( \rightarrow \) \( \text{Id}(A) : A \rightarrow A \).

The category \( \mathcal{C} \) is symmetric monoidal and star autonomous, but not Cartesian, with structural monoids and comonoids, and is enriched in \( \text{SLat} \) (the category of semilattices) [9]. Being enriched in \( \text{SLat} \) means that proofs terms come ordered by \( \subseteq \), and compose under \( \lor \), and these interact sensibly with composition.

\[
\begin{align*}
\pi \subseteq \pi' & \Rightarrow \pi \circ \tau \subseteq \pi' \circ \tau' \\
\tau \subseteq \tau' & \Rightarrow \pi \circ \tau \subseteq \pi \circ \tau'
\end{align*}
\]

\( \pi \circ (\tau \cup \tau') = (\pi \circ \tau) \cup (\pi \circ \tau') \)

\( (\pi \circ \tau') \circ \tau = (\pi \circ \tau) \cup (\pi \circ \tau') \)

\( \mathcal{C} \) is just classical propositional logic, in a categorical setting. (The sequent calculus plays no essential role here. You can define proof terms on other proof systems, e.g. natural deduction, Hilbert proofs, tableaux, resolution.)
2. ISOMORPHISMS

If $A \rightarrow B$ is an isomorphism in a category iff it has an inverse $g : B \rightarrow A$, where $g \circ f = id_A : A \rightarrow A$ and $f \circ g = id_B : B \rightarrow B$. (If $g'$ and $g''$ are inverses, $g = id_A \circ g = (g' \circ f) \circ g = g'' \circ (f \circ g) = g' \circ id_B = g'$, so any inverse is unique. We can call it $f^{-1}$.)

If A and B are isomorphic in a category $\mathcal{C}$, then what we can do with A (in $\mathcal{C}$) we can do with B, too.

If A and B are isomorphic in $\mathcal{C}$, then they agree not only on provability, but also, on proofs. The distinctions drawn when you analyse how something is proved (from premises), are not far from what you want to understand when you ask how something is made true.

Isomorphisms in $\mathcal{C}$:

$p \land q \equiv q \land p$; $\neg(p \land q) \equiv \neg p \lor \neg q$

$q \land p \equiv p \land q$; $\neg(p \land q) \equiv \neg q \lor \neg p$

Non-isomorphisms in $\mathcal{C}$: $p \lor (q \land \neg q) \not\equiv p \lor q \land \neg q$; $p \lor (q \land \neg q) \not\equiv (p \lor q) \land (p \lor \neg q)$; $p \lor (p \lor q) \not\equiv p \lor (p \lor q)$.

Proof Sketch (Došen and Petrič, 2012 [3]).

Let's look at relations like isomorphism, but which erase distinctions, up to HZ or Mx.

Let's say that $A$ and B HZ-match, when there are proofs $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$ where $\pi \circ \pi' = HZ(A)$ and $\pi' \circ \pi = HZ(B)$. We write $\approx_{HZ}$ for the HZ-matching relation, and we write $\approx_{HZ}(\pi, \pi') : A \approx_{HZ} B$ to say that $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$ define a HZ-match between A and B.

Let's say that $A$ and B Mx-match, when there are proofs $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$ where $\tau \circ \pi = Mx(A)$ and $\pi \circ \pi' = Mx(B)$. We write $\approx_{Mx}$ for the Mx-matching relation, and we write $\approx_{Mx}(\pi, \pi') : A \approx_{Mx} B$ to say that $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$ define a Mx-match between A and B.

Isomorphism $\subseteq$ HZ-Matching: If $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$, then consider $\pi' = HZ(B) \circ \pi \circ HZ(A)$ and $\tau' = HZ(A) \circ \pi^{-1} \circ HZ(B)$. These satisfy the HZ-matching criteria, $\tau' \circ \pi = HZ(A)$ and $\pi' \circ \tau' = HZ(B)$.

HZ-Matching $\subseteq$ Logical Equivalence: If $\pi : A \approx_{HZ} B$, then consider $\tau = Mx(B) \circ \pi \circ Mx(A)$ and $\tau' = Mx(A) \circ \pi^{-1} \circ Mx(B)$. These satisfy the Mx-matching criteria, $\tau' \circ \pi = Mx(A)$ and $\pi' \circ \tau' = Mx(B)$.

Mx-Matching $\subseteq$ Logical Equivalence: If $A \approx_{Mx} B$ then there are proofs $\pi : A \rightarrow B$ and $\pi' : B \rightarrow A$.

Matching Relations are Equivalences: reflexive $HZ(A), HZ(A)$: $A \approx_{HZ} A$. $Mx(A), Mx(A) : A \approx_{Mx} A$.

If $\pi, \pi' : A \approx_{HZ} B$, then $\pi', \tau : B \approx_{HZ} C$. If $\pi, \pi' : A \approx_{Mx} B$, then $\pi', \tau : B \approx_{Mx} C$. Transitive If $\pi', \pi : A \approx_{HZ} B$ and $\tau, \tau' : B \approx_{HZ} C$, then $(\tau \circ \pi), (\pi' \circ \tau') : A \approx_{HZ} C$. If $\pi, \pi' : A \approx_{Mx} B$ and $\tau, \tau' : B \approx_{Mx} C$, then $(\tau \circ \pi), (\pi' \circ \tau') : A \approx_{Mx} C$.

Matching: $\neg \circ \neg \approx_{HZ} HZ(p \land q \land (q \lor r) \approx_{HZ} HZ(p \land q) \lor (p \land q)$.

Mx-Matching $\subseteq$ Logical Equivalence: If an atom $p$ occurs positively [negatively] in A but not in B, then A and B do not Mx-match.
PROOF: Mx(A) : A ⊢ A contains the link from [to] that occurrence of p in the premise A to [from] its corresponding occurrence in the conclusion A. ⁹ No proof from A to B contains a link from [to] that occurrence to anything in B (since there is no positive [negative] occurrence in B at all). ⁹ So, in the composition proof from A to A, there is no link from [to] the premise occurrence to [from] the conclusion occurrence. No proof from A to B and back can recreate Mx(A).

COROLLARY: p \not\equiv_{Mx} p \land (q \lor \neg q); p \land \neg p \not\equiv_{Mx} q \land \neg q.

Hz-matching \subset Mx-matching: (p \land \neg p) \land (q \lor \neg q) \equiv_{Mx} (p \lor \neg p) \land (q \lor \neg q).

However, (p \land \neg p) \land (q \lor \neg q) \not\equiv_{Hz} (p \lor \neg p) \land (q \lor \neg q). So:

Isomorphism \subset Hz-Matching \subset Mx-Matching \subset Logical Equivalence

4 MATCHING & LOGICS OF ANALYTIC CONTAINMENT

Angell's Logic of Analytic Containment: [ac1] A \equiv \neg \neg A [ac2] A \equiv \neg (A \land A) [ac3] A \equiv \neg (A \land B) [ac4] A \equiv (B \land A) \land C [ac5] A \equiv (B \land C) [ac6] A \equiv (B \land A) \land (A \lor C) \equiv (B \land A) \land (A \lor C) \equiv (B \land A) \land (A \lor C) \equiv (B \land A) \land (A \lor C) \equiv (B \land A) \land (A \lor C) Here, A \lor B is shorthand for \neg (\neg A \land \neg B). You can define A \rightarrow B as A \equiv (A \land B).

The first degree fragment of Parry's Logic of Analytic Containment is found by adding \neg (A \rightarrow (B \land B)) \rightarrow A to Angell's Logic. (Parry's logic still satisfies this relevance constraint: A \rightarrow B is provable only when the atoms in B are present in A.)

First Degree Entailment (FDE) is found by adding A \rightarrow (A \lor B) to Angell's Logic. 

FDE allows for a disjunctive (or conjunctive) normal form. The only difference from classical logic is that p \lor \neg p, and q \land \neg q are both non-trivial, and ineliminable. 

A simple translation encodes FDE inside classical logic. Choose, for each atom p, a fresh atom p', its shadow. For each FDE formula A, its translation is the formula A' found by replacing the negative occurrences of atoms p in A by their shadows. An argument is FDE valid iff its translation is classically valid.

Definition: Mx(A, B) is the set of all possible linkings which could occur in any proof from A to B. 

That is, it contains a link from positive atoms in A, negative atoms in B to matching (positive atoms in B, negative atoms in A).

Fact: Mx(A, B) is a proof iff there is some proof from A to B. 

(And if so, it is the maximal such proof)

Mx(p \lor \neg p, p \land q) is not a proof:

p \lor \neg p

\neg p \land q

Lemma: If A \equiv_{Mx} B, then Mx(A, B) and Mx(B, A) are proofs, and Mx(A, B), Mx[B, A] : A \equiv_{Mx} B.

Proof: If p, p' : A \equiv_{Mx} B, then p \equiv_{Mx} Mx(A, B) and p' \equiv_{Mx} Mx(B, A) are both proofs. Since p' \lor p = Mx(A), we have Mx(A) \equiv p' \lor p \equiv_{Mx} Mx(B, A) \equiv Mx(A, B) \equiv Mx(A), and similarly, Mx(B) = Mx(A, B) \equiv Mx(A, B), so Mx(A, B), Mx[B, A] : A \equiv_{Mx} B.

Fact: If A is classically equivalent to B, and all atoms occurring positively [negatively] in A also occur positively [negatively] in B, and vice versa, then A and B Mx-match—and conversely.

Proof: If A is logically equivalent to B, then Mx(A, B) and Mx(B, A) are both proofs. 

It suffices to show that Mx(A, B) \equiv Mx(A, B) = Mx(A) (and similarly for B). To show this, we need to show that each positive [negative] occurrence of an atom in A is linked to any positive [negative] occurrence of that atom in A by way of some link in Mx(A, B) composed with a link in Mx(B, A). But since that atom occurs positively [negatively] also in B at least once, the links to accomplish this occur in Mx(A, B) and Mx(B, A) . 

Conversely, if A \equiv_{Mx} B, we have already seen that A and B must be equivalent, and no atom occurs positively [negatively] in A but not B.

This is not Equivalence in Parry's Logic. A is equivalent to B in Parry's logic of analytic containment iff A is classically equivalent to B and the atoms present in A are present in B and vice versa. 

(p \land \neg p) \land q \not\equiv_{Mx} (p \lor \neg p) \land q, but this pair satisfies Parry's variable sharing criterion.

Question: Does the equivalence relation of Mx-matching occur elsewhere in the literature?

Definition: Hz(A, B) is the set of all possible linkings which could occur in any proof from A to B, excluding caps and cups. 

That is, it contains a link from positive atoms in A to corresponding positive atoms in B and negative atoms in A to corresponding negative atoms in B.

Hz(p \land \neg p, q \lor \neg q) contains no links. Hz(p \land \neg p, p \lor \neg p) is a proof, but not the maximal one:

p \land \neg p

\neg p \lor p

Fact: Hz(A, B) is a proof iff A entails B in FDE.


From the Hz-proof Hz(A, B) to FDE-validity: Notice that no negative occurrences of atoms in A or B are linked to any positive occurrences of atoms in A or B. So, there is another Hz-proof Hz(A', B') for the FDE translations for A and B.

Lemma: If A \equiv_{Hz} B, then Hz(A, B) and Hz(B, A) are proofs, and Hz(A, B), Hz(B, A) : A \equiv_{Hz} B.

Proof: If p, p' : A \equiv_{Hz} B, then since p' \lor p = Hz(A) and p \lor p' = Hz(B), p and p' are cap- and cup-free, so p \subset Hz(A, B) and p' \subset Hz(B, A), so Hz(A, B) and Hz(B, A) are both proofs. 

Since p' \lor p = Hz(A), we have Mx(A) = p' \lor p \subset Hz(A, B) \subset Hz(A), and similarly, Hz(B) = Hz(A, B) \subset Hz(A), so Hz(A, B), Hz(B, A) : A \equiv_{Mx} B.

Fact: If A is FDE-equivalent to B, and all atoms occurring positively [negatively] in A also occur positively [negatively] in B, and vice versa, then A and B Hz-match—and conversely.

Proof: If A is FDE-equivalent to B, then Hz(A, B) and Hz(B, A) are both proofs. 

It suffices to show that Hz(A, B) \equiv Hz(A, B) = Hz(A) (and similarly for B). To show this, we need to show that each positive [negative] occurrence of an atom in A is linked to any positive [negative] occurrence of that atom in A by way of some link in Hz(A, B) composed with a link in Hz(B, A). 

But since that atom occurs positively [negatively] also in B at least once, the links to accomplish this occur in Hz(A, B) and Hz(B, A) . 

Conversely, if A \equiv_{Hz} B, we have already seen that
A and B must be fde-equivalent, and no atom occurs positively [negatively] in A but not B.

FACT: [Ferguson 2016 [4]; Fine 2016 [5]] A is equivalent to B in Angell’s logic of analytic containment iff A is fde equivalent to B, and any atom occurs positively [negatively] in A iff it occurs positively [negatively] in B.

So, Hz-matching = Angellic Equivalence.

5 MATCHING AS ISOMORPHISM

Hz(A) and Mx(A) are Idempotents: Hz(A) ⊗ Hz(A) = Hz(A), Mx(A) ⊗ Mx(A) = Mx(A).

For any category C, if tA is an idempotent for each object A, we can form a new category C(t) with the same objects as C, and with arrows tA ⊗ f ◦ tA : A → B. In this new category, the idempotents tA are the new identity arrows. So, C(tA) and C(tB) are the new identity arrows.

Hz-matching is isomorphism in C(tA).

Mx-matching is isomorphism in C(tA).

C(tA) and C(tB) are nontrivial, nonetheless.

These are each different proofs in C(tA) and C(tB).

6 IN CONCLUSION

These results allow for genuinely hyperintensional distinctions to be drawn, using tools that are native to classical proof theory. Proof theoretical resources indigenous to classical logic provide tools for fine-grained hyperintensional distinctions, and some of these tools slice at exactly the same joints as have been discerned using very different techniques. It is encouraging to see how non-classical logics like fde and Angell’s logic of analytic containment arise out of proof theoretical considerations in classical logic. (This is not unprecedented. In Chapter 1.3 of Proof Theory and Logical Complexity, Girard shows how the sequent calculus, under another guise, gives rise to Kleene’s 3-valued logic [6].)

Extending these results to include the units ⊤ and ⊥ are not difficult. (They were left out only to ease the presentation). In short, we allow for degenerate edges for proofs involving the units. For ⊤ we have a link with ⊤ as the target, but with no source. There are no links with ⊤ as a source. So, in the identity arrow from ⊤ to ⊤, there is a degenerate link into the conclusion ⊤, and nothing leaving the premise. The situation is reversed for ⊥. For ⊥ we have a link from ⊥ going nowhere. This link features in the identity proof for ⊥ → ⊥.

As for isomorphisms in the calculus with ⊤ and ⊥, it turns out that A ⊨ A ⊨ ⊤ ∧ ⊤, ¬¬ ⊨ ⊤, and ¬¬ ⊨ ⊤. However, A ⊨ A, in general, since this would violate the variable occurrence condition (which still holds). Nonetheless, ⊤ ∧ ⊤ ⊨ ⊤ and ⊤ ⊨ ⊤ ⊨ ⊤ and ⊤ ∧ ⊤ ⊨ ⊤.

One open question is how to relate these results to models of logics of content. Is there a way to move from the family of different proofs for A (from different premises) to situations making A true in any rich sense? An immediate issue to be confronted is that proofs—and proof terms—wear their premises and their conclusions on their face. A proof from A to B is not also a proof from a different C to a different D. Even though proof terms abstract away from some of the syntactic details of derivations or proofs, they don’t abstract away the premise and the conclusion.

Situations, even though they can be more local and discriminating than possible worlds (or models assigning a truth value to every formula in the language), generally make more than one thing true. To construct situations from proof terms, we must bridge this gap in some way or other.

Another step to consider is whether we can expand these results to first order logic. Some recent work of Dominic Hughes on unification nets for first order multiplicative linear logic [8] brings to light an important distinction for different approaches to proof terms for predicate logic. It is clear that these two derivations here correspond to the one natural deduction proof, and should have the same proof term:

But what about two different derivations going through two different intermediate terms, t1 and t2? Girard’s proof nets for first order MLL take these to be different [7]. There is one clear sense, proof theoretically, that the information flows from ∀xFx to ∃xFx in the same way regardless of which term used, so Hughes’ unification nets (which abstract away from the identity of the particular unifiers used) seem well motivated on proof theoretic grounds.

However, when it comes to the metaphysics of grounding and subject matter, it seems that there is good reason allow each object that makes ∃xFx true contribute in its own, individual, way. This much seems clear. Different objects witness quantifiers in different ways, and this should be reflected in the detail of truth-makers. However, the logic of such distinctions is yet to be understood clearly. Perhaps tools from proof theory will be able to help clarify some of the options to further explore.

REFERENCES