Proofs—and what they're good for

GREG RESTALL • restall@unimelb.edu.au • SYDNEY PHILOSOPHY SEMINAR • 18 MAY 2016

My aim: To explain the nature of ***proof***, from the perspective of a ***normative pragmatic account of meaning***, using the tools of ***proof theory***.

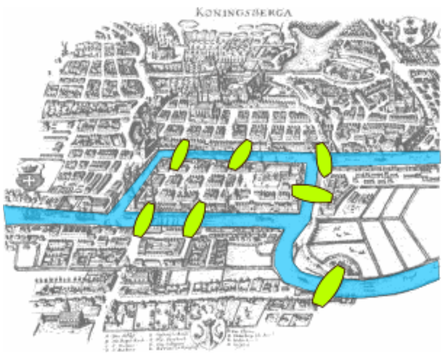
1. MOTIVATION

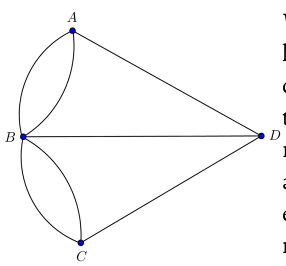
***Example proof* (1)**: Every *drink* (in our fridge) is either a *beer* or a *lemonade* $(\forall x)(Dx \rightarrow (Bx \vee Lx))$. So either every *drink* is a *beer*, or some *drink* is a *lemonade* $(\forall x)(Dx \rightarrow Bx) \vee (\exists x)(Dx \wedge Lx)$. *Why*? Take an arbitrary *drink*. If it's a *lemonade*, we have the conclusion that some *drink* is a *lemonade*. If we don't have that conclusion, then that arbitrary *drink* is a *beer*, and so, all the *drinks* are *beers*.

$$
\begin{prooftree}
\AxiomC{$Da \succ Da$}
\AxiomC{$Ba \succ Ba$}
\AxiomC{$La \succ La$}
\RightLabel{$\vee L$}
\BinaryInfC{$Ba \vee La \succ Ba, La$}
\RightLabel{$\supset L$}
\BinaryInfC{$Da \supset (Ba \vee La), Da \succ Ba, La$}
\RightLabel{$\forall L$}
\UnaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)), Da \succ Ba, La$}
\AxiomC{$Da \succ Da$}
\RightLabel{$\wedge R$}
\BinaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)), Da \succ Ba, Da \wedge La$}
\RightLabel{$\exists R$}
\UnaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)), Da \succ Ba, (\exists x)(Dx \wedge Lx)$}
\RightLabel{$\supset R$}
\UnaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)) \succ Da \supset Ba, (\exists x)(Dx \wedge Lx)$}
\RightLabel{$\forall R$}
\UnaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)) \succ (\forall x)(Dx \supset Bx), (\exists x)(Dx \wedge Lx)$}
\RightLabel{$\vee R$}
\UnaryInfC{$(\forall x)(Dx \supset (Bx \vee Lx)) \succ (\forall x)(Dx \supset Bx) \vee (\exists x)(Dx \wedge Lx)$}
\end{prooftree}
$$

***Example proof* (2)**: Consider the bridges in Königsberg (depicted below).

It is not possible to walk a circuit through Königsberg, *crossing each bridge exactly once*.





Why? Any bridge takes you from one landmass (A,B,C,D) to another. In any circut, you must *leave* a landmass as many times as you *arrive*. So if you are not to repeat a bridge, each landmass must have an even number of bridges entering and exiting it. Here, each landmass has an *odd* number of bridges, so a circuit is impossible.

Our focus will be on *categorical* proofs from premises to a conclusion. In particular, my focus today will be on categorical proofs of a very special kind—proofs in *first order predicate logic*, where the central concepts used are the logical notions of conjunction, disjunction, negation, the (material) conditional, the quantifiers, and identity. But what I say here will apply to proof using the features of other concepts.

Puzzles about proof: How can proofs expand our knowledge, when the conclusion is already present (implicitly) in the premises? ¶ How can we be ignorant of a conclusion which actually already follows from what we already know? ¶ What grounds the necessity in the connection between premises and conclusion?

2. BACKGROUND

Positions collect together *assertions* and *denials* $[X : Y]$.

Assertions and *denials* are moves in a communicative pracitce.
I can *deny* what you *assert*. We can assert or deny the same thing. We can also *retract* assertions and denials. I can *try on* assertion or denial hypothetically (suppose *p* — then *q*…)

Asserting or denying involves *taking a stand* on some matter.

Assertion and denial ***clash***.

The ***bounds*** on positions:

– ***Identity***: $[A : A]$ is out of bounds.

– ***Weakening***: If $[X : Y]$ is out of bounds so are $[X, A : Y]$ and $[X : A, Y]$

– ***Cut***: If $[X, A : Y]$ and $[X : A, Y]$ are out of bounds, so is $[X : Y]$

A position that is *out of bounds* does not succeed in taking a stand.

Definitions come in a number of flavours. One is obvious:

Explicit Definition: Define a concept by showing how you can compose this concept out of more primitive concepts.

(x is a square $=_{df}$ x is a rectangle $\wedge$ all sides of x are equal in length)

Concepts given an explicit definition are *sharply delimited* (contingent on accepting the definition, of course). Logical concepts like conjunction, disjunction, negation, the (material) conditional, the quantifiers, and identity are similarly sharply delimited, but they *cannot* be given explicit definition. (They are *used* in giving explicit definitions.)

Definition through a rule for use: Define a concept by showing it could be added to one's vocabulary, giving rules for interpreting assertions and denials involving that concept.

$[X, A \wedge B : Y]$ is out of bounds if and only if $[X, A, B : Y]$ is out of bounds.

$X, A \wedge B \vdash Y$ *iff* $X, A, B \vdash Y$ $\qquad$ $X \vdash A \supset B, Y$ *iff* $X, A \vdash B, Y$

$X, \neg A \vdash Y$ *iff* $X \vdash A, Y$ $\qquad$ $X \vdash A \vee B, Y$ *iff* $X \vdash A, B, Y$

$X \vdash (\forall x)Fx, Y$ *iff* $X \vdash Fa, Y$ (where a is not present in X, Y)

The concepts introduced in this way are *uniquely defined* (if you and I follow the same rule, our usages are intertranslatable) and they *conservatively extend* the original vocabulary (if a position was safe before we added the concept, it's still safe afterwards).

They play useful dialogical roles. (e.g. Once we have conjunction, I can disagree with your assertion of A and B without disagreeing with A or disagreeing with B). They are subject-matter-neutral. To use Brandom's terms, the new concepts *make explicit* some of what was previously merely implicit.

3. WHAT PROOFS ARE

Consider a *tiny* proof, consisting of a single step of *modus ponens:*

If it's Wednesday, I'm in Sydney. It's Wednesday. Therefore, I'm in Sydney.

Here, we have two assertions (the premises), a connecting *therefore* and another assertion (the conclusion).

This proof crucially uses the *conditional*. If we mean "$\supset$", then we have $A \supset B \vdash A \supset B$ *iff* $A \supset B, A \vdash B$.

And hence, a position in which I assert "If it's Wednesday, I'm in Sydney" and "It's Wednesday" but I deny "I'm in Sydney" is out of bounds. So, "I'm in Sydney" is undeniable, and the assertion makes explicit what was previously implicit.

A *proof* of $X \vdash Y$ shows that the position $[X : Y]$ is out of bounds, by way of the defining rules of the concepts used in X and Y.

In this sense, proofs are *analytic*.

(*Proofs can be solely assertions, or they could mix assertions and denials.*)

A *proof* of $A, B \vdash C, D$ can be understood as a *proof* of C from the position $[A, B : D]$, or a *refutation* of A, from the position $[B : C, D]$.

4. HOW PROOFS WORK

Proofs make explicit the positions that are out of bounds.

Observation 1: Our ability to *specify* consequence far outstrips our ability to *recognise* it. We have *no idea* if the position

[*Peano Arithmetic* : *Goldbach's Conjecture*]

is out of bounds or not. This is not a *bug*—it is a *feature*. The logical concepts are *expressive*. They give us the means to *say* things (think things, explore things) whose significance we continue to work out.

It is straightforward to verify whether a putative proof is a proof. It is not straightforward to find a proof of something that *has* a proof.

Are we logically omniscient?

Suppose $PA \vdash GC$ and we know PA. Do we *know* GC?

In a very weak sense, *yes*. It is a logical consequence of what we know. It is *implicitly present* in what we know. Denying GC is inconsistent (with PA). But this inconsistency is not transparent to us.

In another sense, the answer is *no*. Even if I believe GC (for inconclusive reasons), that may not count as knowledge if that belief is acquired in the wrong way. (By testimony, by misunderstanding, by inappropraite generalisation, by my mistaken proof.) Different accounts of knowledge will assess this case differently, but if the *ground* (or *source*) of the epistemic state plays some role in whether it counts as knowledge, then this is a place where logical omniscience can break down.

In this (hypothetical) case, there *is* evidence, in the sense of a proof from PA to GC, but if we do not posess it, and use it to ground our belief in GC, this proof is epistemically inert.

Observation 2: *Proofs preserve truth*. The definition of proof does not involve *truth*. However, given plausible (minimal) assumptions about the nature of truth, it follows that if there is a proof for $X \vdash A, Y$ then if each member of X is true and each member of Y is not true, then A is true.

Observation 3: *Proofs transfer warrant*. The definition of proof does not involve *warrant*. However, given plausible (less minimal) assumptions about the nature of warrant, it follows that if there is a proof for $X \vdash A, Y$ then given (conclusive) warrant *for* each member of X and (conclusive) warrant *against* each member of Y, we have (conclusive) warrant for A.

Caveat: matters are subtle when it comes to defeasible warrant. Consider the lottery paradox, where for any ticket we have defeasible reason to believe, that this ticket will not win, but we also have reason to believe that some ticket will win.

$$[(\exists x)(Tx \wedge Wx), (\forall x)(Tx \equiv x = t_1 \vee x = t_2 \vee \cdots \vee x = t_{1\,000\,000}) \\ : Wt_1, Wt_2, Wt_3, \ldots, Wt_{1\,000\,000}]$$

This position is out of bounds, but each particular component of the position is *highly likely*.

Observation 4: *Achilles and the Tortoise*. Consider the exchange between Achilles and the Tortoise.

We have $A, B \vdash Z$. This does *not* mean that anyone who accepts A and B must accept Z.

But Z *is* undeniable in any context where A and B are asserted. To *deny* it Z to use *if* in a way that deviates from its defining rule.

"Well, now, let's take a little bit of the argument in that First Proposition—just *two* steps, and the conclusion drawn from them. Kindly enter them in your note-book. And in order to refer to them conveniently, let's call them A, B, and Z:—

(A) Things that are equal to the same are equal to each other.
(B) The two sides of this Triangle are things that are equal to the same.
(Z) The two sides of this Triangle are equal to each other.

Readers of Euclid will grant, I suppose, that Z follows logically from A and B, so that any one who accepts A and B as true, *must* accept Z as true?"

"Undoubtedly! The youngest child in a High School—as soon as High Schools are invented, which will not be till some two thousand years later—will grant *that*."

"And if some reader had *not* yet accepted A and B as true, he might still accept the *sequence* as a *valid* one, I suppose?"

"No doubt such a reader might exist. He might say 'I accept as true the Hypothetical Proposition that, *if* A and B be true, Z must be true; but, I *don't* accept A and B as true.' Such a reader would do wisely in abandoning Euclid, and taking to football."

"And might there not *also* be some reader who would say 'I accept A and B as true, but I *don't* accept the Hypothetical'?"

"Certainly there might. *He*, also, had better take to football."

"And *neither* of these readers," the Tortoise continued, "is *as yet* under any logical necessity to accept Z as true?"

"Quite so," Achilles assented.

"Well, now, I want you to consider *me* as a reader of the *second* kind, and to force me, logically, to accept Z as true."

"A tortoise playing football would be—" Achilles was beginning

"—an anomaly, of course," the Tortoise hastily interrupted. "Don't wander from the point. Let's have Z first, and football afterwards!"

"I'm to force you to accept Z, am I?" Achilles said musingly. "And your present position is that you accept A and B, but you *don't* accept the Hypothetical—"

"Let's call it C," said the Tortoise.

"—but you *don't* accept

(C) If A and B are true, Z must be true."

"That is my present position," said the Tortoise.

"Then I must ask you to accept C."

"I'll do so," said the Tortoise, "as soon as you've entered it in that note-book of yours. What else have you got in it?"

"Only a few memoranda," said Achilles, nervously fluttering the leaves: "a few memoranda of—of the battles in which I have distinguished myself!"

"Plenty of blank leaves, I see!" the Tortoise cheerily remarked. "We shall need them *all*!" (Achilles shuddered.) "Now write as I dictate:—

(A) Things that are equal to the same are equal to each other.
(B) The two sides of this Triangle are things that are equal to the same.
(C) If A and B are true, Z must be true.
(Z) The two sides of this Triangle are equal to each other."

"You should call it D, not Z," said Achilles. "It comes *next* to the other three. If you accept A and B and C, you *must* accept Z."

"And why *must* I?"

Lewis Caroll "What the Tortoise Said to Achilles," *Mind* 4:14 (1895), 278–280