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 (∀x)(Dx → (Bx v Lx)). So either every drink is a beer, or some drink is a lemonade (∀x)(Dx → Bx) ∨ (∃x)(Dx ∧ 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.

Da > Ba, La > La
Da > Da
Ba ∨ La > Ba, La
Da > Ba, Da ∨ La
(∀x)(Dx ⊃ (Bx v Lx)), Da > Ba, (∃x)(Dx ∧ Lx)

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.

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 practice. I can deny what you assert. We can assert or deny the same thing. We can also retract assertions and denials. I can try to assert or deny 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 it could be added to one’s vocabulary, giving rules for interpreting assertions and denials involving that concept.

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

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

X, A ∧ B ⊨ Y iff X, A, B ⊨ Y
X ∧ A ⊨ B, Y iff X, A ⊨ B, Y
X, ¬A ⊨ Y iff X ⊨ A, Y
X, A ⊨ B, Y iff X ⊨ A, B, Y
X ⊨ (∀x)Fx, Y iff X ⊨ 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 "⊃", then we have

\[ A \supset B \equiv A \supset B \iff A \supset B, A \vdash B. \]

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 such 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 \( A, B \vdash C \) 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 inappropriately 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 possess 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 \( X \vdash A \), then 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 \( X \vdash A \), 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 there is no reason to believe, that this ticket will not win, but we also have reason to believe that some ticket will win.

\[ ([\exists x] (Wx \land \neg Wx), \forall x ([T x \equiv x = t_1 \lor x = t_2 \lor \ldots \lor x = t_{2000000} \land \neg Wt_{2000000}]) \]

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 \( j \) in a way that deviates from its defining rule.

“…”