05. Rigorization and Proof

(*Reference*: Brown, J. (1999) *Philosophy of Mathematics*, Chap. 3.)

Topics
I. Formal System and Proof
II. Analytical Proofs
III. Picture Proofs

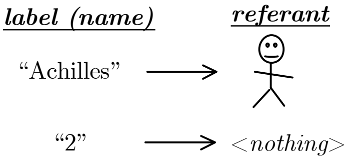
I. The Notion of a Proof in a Formal System

One way to view mathematics: mathematics as a formal game

The subject matter of mathematics = *meaningless symbols*
Mathematics itself = *symbol manipulation*

Chess analogy: What do chess pieces stand for? (What do they denote?)

"2" is *just* a name
- a symbol
- it doesn't refer to a real object



ASIDE: In philosophy of mathematics, this view of mathematics is known as "formalism". There are other ways of viewing mathematics. A "Platonist", for instance, believes the referants of mathematical symbols are real objects (numbers, sets, etc), and mathematicians "discover" things about them, as opposed to inventing new games to play.

How best to characterize such formal games? ***Answer****: The Notion of a Formal System:*

Formal System:
A formal system consists of a ***language*** (*symbols* and *grammar*) and a set of ***axioms*** and ***inference rules***. The axioms are basic statements in the language that are taken to be true. The inference rules tell you how to derive more complex statements, ***theorems***, from the axioms.

Example of a very simple formal system - call it "S"

***1. Symbols of S*:**

Individuals:	♣, ♥	*think of them as "Mr. ♣" and Mr. ♥"*
Properties:	♦, ♠	
Variables:	x, y, z, ...	*range over the individuals*
Connectives:	$\rightarrow$, &, $\vee$, $\sim$, $\leftrightarrow$	*"if then", "and", "or", "not", "if and only if"*
Quantifiers:	$\forall$, $\exists$	*universal and existential quantifiers*
Punctuation:	(,)	*right and left parentheses*

The alphabet of the language of S.

***2. Grammar of S*:**

Terms (subjects of statements)
All individuals and variables are terms.

Statements (make claims about subjects)
(i) If t is a term, then Pt is a statement, where P is a property.
(ii) If $\mathcal{A}$ and $\mathcal{B}$ are statements, then so are $(\mathcal{A} \rightarrow \mathcal{B})$, $(\mathcal{A}\ \&\ \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $\sim\mathcal{A}$, $(\mathcal{A} \leftrightarrow \mathcal{B})$, $(\forall x)\mathcal{A}$, $(\exists x)\mathcal{A}$.
(iii) Nothing else is a statement.

How to construct terms and statements out of the alphabet.

Examples of statements:

$♦♣$	*"Mr. ♣ has property ♦"*
$(♦♣ \to ♠♥)$	*"If Mr. ♣ has property ♦, then Mr. ♥ has property ♠"*
$(\forall x)♠x$	*"All individuals have property ♠"*
$(\exists x)♦x$	*"There exists an individual that has property ♦"*

3. Rules for Manipulating the Symbols:

Axioms of S:

(1) $(\forall x)(♦x \to ♠x)$ (*"For all individuals x, if x is a ♦, then x is a ♠."*)

(2) $(\exists x)♠x \to ♦♣$ (*"If there exists an individual x that is a ♠, then Mr. ♣ is a ♦"*)

(3) $♠♥$ (*"Mr. ♥ is a ♠"*)

Think of ***axioms*** *as basic claims about the individuals and properties of S.*

Inference Rules for S

Let $\mathcal{A}$, $\mathcal{B}$ be statements, and let P be a property:

(1) *Modus Ponens (MP)*
Given an *if-then* statement, and the "*if*"-part, you may infer the "*then*"-part.

$$\begin{array}{l} \mathcal{A} \to \mathcal{B} \\ \mathcal{A} \\ \hline \therefore\ \mathcal{B} \end{array}$$

(2) *Universal Instantiation (UI)*
From "All individuals have property P", you may infer "Individual a has property P".

$$\begin{array}{l} (\forall x)Px \\ \hline \therefore\ Pa \end{array}$$

(3) *Existential Generalization (EG)*
From "Individual a has property P", you may infer "There exists an individual that has property P".

$$\begin{array}{l} Pa \\ \hline \therefore\ (\exists x)Px \end{array}$$

Think of ***inference rules*** *as rules that let you deduce more complex claims ("theorems") about individuals and properties from the basic claims (axioms).*

Example of a theorem and its proof:

Theorem: $♣♠$ (*"Mr. ♣ is a ♠."*)

Proof:

(1)	$♠♥$	Axiom 3
(2)	$(\exists x)♠x$	*EG* 1
(3)	$(\exists x)♠x \to ♦♣$	Axiom 2
(4)	$♦♣$	*MP* 3, 2
(5)	$(\forall x)(♦x \to ♠x)$	Axiom 1
(6)	$♦♣ \to ♠♣$	*UI* 5
(7)	$♠♣$	*MP* 4, 6

Features of the proof:

(i) Consists of a sequence of statements.

(ii) The last statement is the theorem we're trying to prove.

(iii) All prior statements are either basic claims (axioms), or follow from previous statements by means of the inference rules.

This establishes the truth of the theorem:

If the axioms are true, and we accept the rules of inference as legitimate rules of deduction, then the theorem *must* also be true.

Definition of a Proof in S:

A ***proof in S*** is a sequence of S-statements such that any member is either an axiom of S or follows from previous members by the rules of inference of S.

Note: Of course our formal game S is very primitive, even when compared to very simple branches of mathematics (like arithmetic, as we'll see). But the general notion of a proof remains the same. In most proofs in mathematics, not all the steps will be made as *explicit* as they are above.

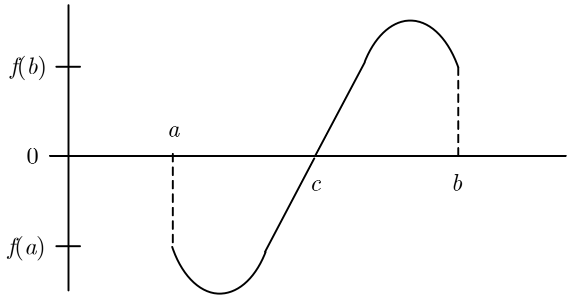
ASIDE: This idea of a proof in a formal system was only made explicit in the early 20th century in the field of logic. But the general idea is much older. Intuitively, what Cauchy and Riemann, among others, did for the calculus was to take the somewhat vague notion of an infinitesimal and make it rigorous by (implicitly) embedding it in a formal system with axioms and inference rules.

II. Analytical Proofs

The above is a formal definition of an "analytical" proof. Here's a more concrete example from Calculus:

Intermediate Zero Theorem (Bolzano 1817)

Claim: If f is a continuous function on the interval $[a, b]$ and f changes sign from negative to positive (or *vice versa*), then there is a c between a and b such that $f(c) = 0$.



Kinda obvious!
But how to show this ***explicitly*** *and* ***formally****?*

Proof: Let $f(a) < 0 < f(b)$.

Consider the set $S = \{$all x such that $a \leq x \leq b$ and $f(x) < 0\}$.

S is non-empty (at least a is a member), and it is *bounded above* by b.

So: S has a *least upper bound*, call it c.

This means: For all $x \in S$, $x < c$, and there's no d such that $x < d < c$.

Then: Either $f(c) < 0$, or $f(c) > 0$, or $f(c) = 0$.

Suppose: $f(c) < 0$.

Then: There's an open interval $(c - \delta, c + \delta)$ around c in which $f(x) < 0$. But this allows there to be x such that $f(x) < 0$ (hence $x \in S$), but $x > c$. But we assumed c was an *upper* bound of S.

Suppose: $f(c) > 0$.

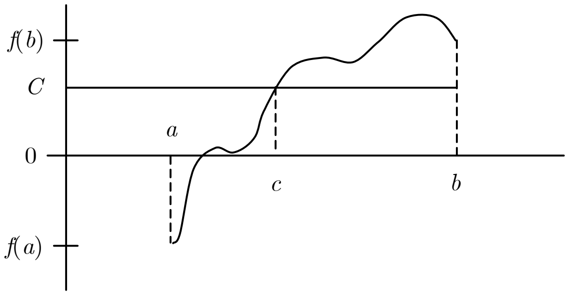
Then: There is an open interval $(c - \delta, c + \delta)$ around c in which $f(x) > 0$. But this allows there to be a d such that $d < c$ and $f(d) > 0$. This entails that for any x in S, $x < d$. So for any x in S, $x < d < c$. But we assumed c was a *least* upper bound of S.

So: It must be the case that $f(c) = 0$.

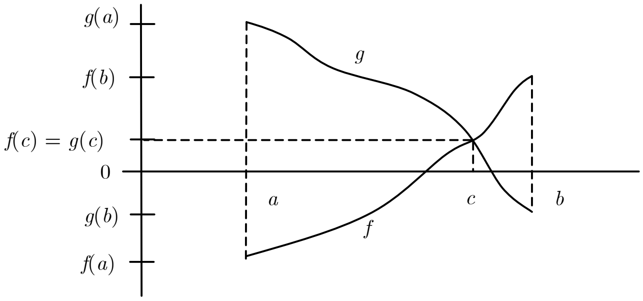
Similar proofs can be given for the following:

Intermediate Value Theorem

Claim: If f is a continuous function on the interval $[a, b]$ and there is a C between $f(a)$ and $f(b)$, then there is a c between a and b such that $f(c) = C$.



Claim: If f and g are continuous functions on the interval $[a, b]$ such that $f(a) < g(a)$ and $f(b) > g(b)$, then there is a c between a and b such that $f(c) = g(c)$.



III. Picture Proofs

If you take mathematics to be about *formal systems*, then *analytical proofs* will probably appeal to you.
BUT: If you take mathematics to be about other things, then other concepts of proof may appeal.

Alternative View of Mathematics:

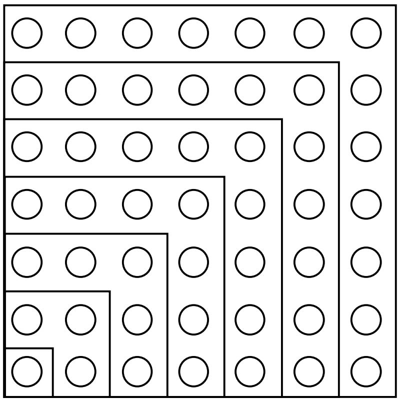
Mathematics is about *real abstract objects* and their properties (numbers, sets, functions, *etc*).
Mathematicians discover *truths* about these objects.
Many ways to do this, including *rigorous proof construction*, *intuition*, *etc.*

A ***picture proof*** is a diagram that allows you to "grasp" the truth of a theorem without deriving it from first principles.

Examples:

1. *Claim*: $1 + 3 + 5 + \ldots + (2n - 1) = n^2$

Picture Proof:



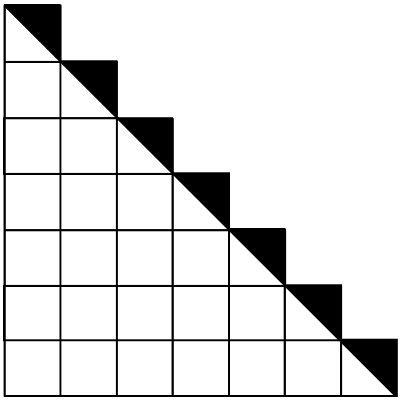
$n = 7$

ASIDE: Here's the analytical proof (by mathematical induction).
Base Step: Show the property holds for $n = 1$.
$((2 \times 1) - 1) = 1 \overset{\checkmark}{=} 1^2$.
Induction Step: Show that, if the property holds for any $n > 1$, then it holds for $n + 1$.
Suppose $1 + 3 + \ldots + (2n - 1) = n^2$ holds for some $n > 1$.
Now check for $n + 1$:

$$\begin{aligned} &\{1 + 3 + \ldots + (2n - 1)\} + (2(n + 1) - 1) \\ &= \{1 + 3 + \ldots + (2n - 1)\} + (2n + 1) \\ &= n^2 + (2n + 1) \\ &\overset{\checkmark}{=} (n + 1)^2 \end{aligned}$$

2. *Claim*: $1 + 2 + 3 + \ldots + n = \dfrac{n^2}{2} + \dfrac{n}{2}$

Picture Proof:



$n = 7$