Foundations of formal proof systems

Benjamin Werner

Ecole Polytechnique

MPRI

2-7-1

2024

How do we define mathematics ?

All humans are mortal, Socrates is human, thus Socrate is mortal.

correction : *syntaxic* criterion

$$\frac{\vdash A \Rightarrow B \qquad \vdash A}{\vdash B}$$

The stones to build mathematical proofs

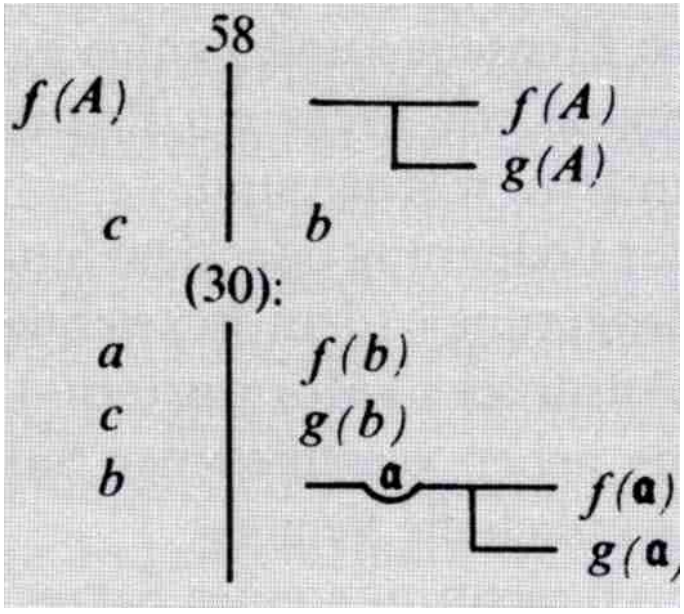
$$\frac{\dfrac{\vdash \forall x.H(x) \Rightarrow M(x)}{\vdash H(s) \Rightarrow M(S)} \qquad \vdash H(S)}{\vdash M(S)}$$

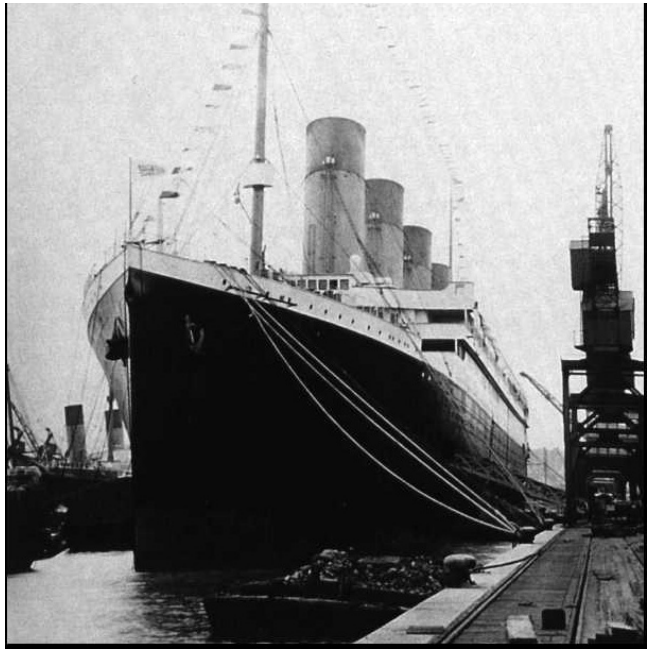
A mathematical proof is a *construction*

Birth of modern mathematical logic

Mathematical truth defined through totally objective rules

1872 : The *Begriffsschrift* of Frege





mechanical verification

proof = tree structure

A century later

Mechanical verification
becomes real

First proof system : Automath (1968)

N. G. de Bruijn

Formal proofs are *actually* built.

Today

A modern proof system : Coq

- Same principle
- More modern formalism

What do we ask from a formalism

Before (informal proofs) : we want the formalism to be expressive (many theorems)

Now (formal proofs) we want also :

- Concise proofs
- Close to our intuition (no spurious syntactical hacking)
- ...

This course : study formalisms with these aims in mind

First-order logic - language

A set of variables : $x, y, z, \ldots$
A set of function symbols : $f, g, h, \ldots$ each function symbol has an arity (number of arguments).
A set of predicate symbols : $A, B, C, P, R \ldots$ each with an arity.

Objects :

- a variable is a term,
- if f is of arity n and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

Propositions :

- if P is of arity n then $P(t_1, \ldots, t_n)$ is a (atomic) proposition
- is A and B are propositions,
  $A \wedge B,\ A \vee B,\ A \Rightarrow B,\ \bot,\ \forall x.A,\ \exists x.B$ are propositions.

Examples (languages of FOL)

Arithmetic (Peano, 1889)

Function symbols : $0, S, +, \times$

Predicate symbol : $=$

Set Theory (Cantor, Russell, Zermelo, Fraenkel...)

Predicate symbols : $\in, =$

A theory is :

- A language (functions + predicate symbols)
- A set of axioms (propositions of the language)

Axioms of arithmetic :

$$\forall x, 0 + x = x \qquad \forall x, 0 \times x = 0$$
$$\forall x\ y, S(x) + y = S(x + y) \qquad \forall x\ y, S(x) \times y = y + x \times y$$

$$\forall x, \neg(0 = S(x))$$
$$\forall x\ y, S(x) = S(y) \Rightarrow x = y$$

$$P(0) \wedge (\forall x, P(x) \Rightarrow P(S(x))) \ \Rightarrow \ \forall x, P(x).$$

$$\forall x, x = x$$
$$\forall x\ y, P(x) \wedge x = y \Rightarrow P(y).$$

Truth : natural deduction

Γ set of propositions

$\Gamma \vdash A$ A is provable under hypothesises+axioms Γ

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ (\text{Ax})$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge\text{-I}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge\text{-E}_1) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge\text{-E}_2)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee\text{-I}_1) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee\text{-I}_2)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee\text{-E})$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\Rightarrow\text{-I}) \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\Rightarrow\text{-E})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ (\forall\text{-I}) \quad \text{if } x \text{ not free in } \Gamma$$

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[x \setminus t]}\ (\forall\text{-E})$$

$$\frac{\Gamma \vdash A[x \setminus t]}{\Gamma \vdash \exists x.A}\ (\exists\text{-I})$$

$$\frac{\Gamma, A \vdash B \qquad \Gamma \vdash \exists x.A}{\Gamma \vdash B}\ (\exists\text{-E}) \quad \text{if } x \text{ not free in } \Gamma, B$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \ (\bot\text{-E})$$

(this gives intuitionistic logic

$$\frac{}{\Gamma \vdash A \vee \neg A} \ (\text{EM})$$

(this gives classical logic)

Relating correctness and truth : models and semantics

A set $\mathcal{U}$ (universe)
For every f of arity n, a function $|f| : \mathcal{U}^n \to \mathcal{U}$
For every P of arity n, a function $|P| : \mathcal{U}^n \to \{0, 1\}$ (equivalently $|P| \subset \mathcal{P}(\mathcal{U}^n)$)
Given any $\mathcal{I}$ mapping variables x to $\mathcal{U}$ we define $|t|_{\mathcal{I}} \in \mathcal{U}$ by :

- $|x|_{\mathcal{I}} \equiv \mathcal{I}(x)$
- $|f(t_1, \ldots, t_n)|_{\mathcal{I}} \equiv |f|(|t_1|_{\mathcal{I}}, \ldots |t_n|_{\mathcal{I}})$

Given any $\mathcal{I}$ we define $|A| \in \{0, 1\}$ by :

- $P(t_1, \ldots, t_n)|_{\mathcal{I}} \equiv |P|(|t_1|_{\mathcal{I}}, \ldots |t_n|_{\mathcal{I}})$
- $|A \wedge B|_{\mathcal{I}} \equiv |A|_{\mathcal{I}} \wedge |B|_{\mathcal{I}}$
- similar for $\vee$, $\Rightarrow$, $\bot \ldots$
- $|\forall x.A|_{\mathcal{I}} \equiv \min_{\alpha \in \mathcal{U}} |A|_{\mathcal{I};x \leftarrow \alpha}$
- $|\exists x.A|_{\mathcal{I}} \equiv \max_{\alpha \in \mathcal{U}} |A|_{\mathcal{I};x \leftarrow \alpha}$ (this is very much classical logic)

Model of a theory

A model is a triple : $\mathcal{U}$, interpretation of fs, interpretation of Ps. It is a model of a theory $\mathcal{T}$ if for any $A \in \mathcal{T}$, $|A|_{\mathcal{I}} = 1$ (for any $\mathcal{I}$ since A is closed)

Correctness : If $\Gamma \vdash A$, and $\forall B \in \Gamma, |B|_{\mathcal{I}} = 1$, then $|A|_{\mathcal{I}} = 1$.
proof : quite straightforward (good exercise)

Coherence : There is no proof of $\mathcal{T} \vdash \bot$ (easy consequence of correctness)

Completeness : If for any model validating Γ, $|A|_{\mathcal{I}} = 1$, then $\Gamma \vdash A$ is provable.
proof : more difficult (Gödel's PhD)

- Relates correctness with truth
- incompleteness : limit of « truth » in math

An extension of first-order logic

Deduction modulo : we add rewrite rules to the language

$$\begin{array}{rcl} 0 + x & \triangleright & x \\ S(x) + y & \triangleright & S(x + y) \\ O \times x & \triangleright & 0 \\ S(x) \times y & \triangleright & y + x \times y \end{array}$$

we allow reasoning modulo the rewrite rules :

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \psi} \text{ if } \phi =_R \psi$$

How to prove $2 + 2 = 4$?

Replacing more axioms by rewrite rules

How to ensure $0 \neq 1$?

$$\forall x.0 \neq S(x)$$

Add a new predicate symbol EQZ

$$\begin{aligned} \mathrm{EQZ}(0) &\rhd \top \\ \mathrm{EQZ}(S(x)) &\rhd \bot \end{aligned}$$

Exercise : finish the proof
Important : avoiding messy rewrite rules ($A \wedge B \rhd \bot \ldots$)

Replacing more axioms by rewrite rules(2)

How to ensure $\forall x.\forall y.S(x) = S(y) \Rightarrow x = y$?
(injectivity of S)
Add a new function symbol pred

$$\begin{aligned} \text{pred}(S(x)) &\triangleright x \\ \text{pred}(0) &\triangleright 0 \quad \text{(or whatever)} \end{aligned}$$

Exercise : finish the proof

A "simple" presentation of Arithmetic

Rules :

$$
\begin{array}{rcl}
0 + x & \triangleright & x \\
S(x) + y & \triangleright & S(x + y) \\
O \times x & \triangleright & 0 \\
S(x) \times y & \triangleright & y + x \times y
\end{array}
\qquad
\begin{array}{rcl}
\mathrm{EQZ}(0) & \triangleright & \top \\
\mathrm{EQZ}(S(x)) & \triangleright & \bot \\
\mathrm{pred}(S(x)) & \triangleright & x \\
\mathrm{pred}(0) & \triangleright & 0
\end{array}
$$

Axioms :

$$\forall x.x = x$$

$$\forall x.\forall y.x = y \wedge P(x) \Rightarrow P(y)$$

$$P(0) \wedge (\forall x.P(x) \Rightarrow P(S(x))) \Rightarrow \forall y.P(y)$$

Cuts in proofs

Another form of dynamics / computation / transformation in proofs

What is a cut ?

1. Prove $\forall a.\forall b.(a+b)^2 = a^2 + b^2 + 2ab$ (ends with $\forall$-intro)
2. Deduces $\forall b.(3+b)^2 = 9 + b^2 + 6b$ (use $\forall$-elim)

We could have proved (2) directly (following the same scheme as 1)

Logical Cut

An introduction rule followed by the corresponding elimination rule

$$\dfrac{\dfrac{\dfrac{\sigma_1}{\Gamma \vdash A} \quad \dfrac{\sigma_2}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ (\wedge\text{-i})}{\Gamma \vdash A}\ (\wedge\text{-e1})$$

Simplifies to :

$$\dfrac{\sigma_1}{\Gamma \vdash A}$$

exercise : find the simplification for the other logical cuts

Cut Elimination

- Does this process terminate ?
- If we have a proof of $\Gamma \vdash A$, can we find a cut-free proof ?

Termination : a major point of this course

Cut-free proofs

Why does it matter to us ?

In a cut-free proof, there are only axiom rules above elimination rules (or the EM)

If a proof is cut-free, without axiom and constructive, it ends with an introduction rule.

A proof of $\vdash A \vee B$ that is constructive and cut-free ends with $\vee - i1$ of $\vee - i2$.

A proof of $\vdash \exists x.A(x)$ that is constructive and cut-free contains a *witness*.

Cut Free - axiom free proofs

Lemma : a cut free derivation (proof) of $[] \vdash A$ always ends with an introduction rule.

Proof : by induction over the derivation (could be the length of the derivation, but not necessary).

Let us do a few cases.

Why "natural" deduction ?

The ND rules aim at corresponding to actual (human) deduction steps.
Indeed :

Coq's formalism includes / extends first-order logic with some rewrite/computation rules.

Proofs are built top-down (goal-driven) and basic tactics correspond to ND rules

Next : : cuts and constructivity in Heyting Arithmetic

MPRI
2-7-1

Benjamin Werner

Cuts in Heyting Arithmetic

Sept. 2024

A presentation of Heyting Arithmetic

Axioms

$\forall\ x.\ x=x$

$\forall\ x.\forall\ y.\ x=y \wedge P(x) \Rightarrow P(y)$

$P(0) \wedge (\forall\ x.P(x) \Rightarrow P(S(x))\ \Rightarrow\ \forall\ y.\ P(y)$

closed normal object:
0, S(0), S(S(O)), …

closed normal atomic proposition
n=m (⊤ and ⊥ are not atomic)

Rewrite rules

$0 + x \ \triangleright\ x$ $\qquad$ $0 \times x \ \triangleright\ 0$

$S(x) + y \ \triangleright\ S(x+y)$ $\qquad$ $S(x) \times y \ \triangleright\ x \times y + y$

$pred(S(x)) \ \triangleright\ x$ $\qquad$ $pred(0) \triangleright 0$

$EQZ(S(x)) \triangleright \bot$ $\qquad$ $EQZ(0) \ \triangleright\ \top$

Cuts in deduction modulo

Previous presentation: new additional rule

$$\text{(conv)}\ \frac{\Gamma \vdash A}{\Gamma \vdash B} \quad \text{if } A =_R B$$

we do not want it to interfere with cuts.

should be a cut

$$\wedge\text{-e}\ \frac{\wedge\text{-i}\ \dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A'}$$

We can rather reformulate the rules:

$$\wedge\text{-i}\ \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash C} \quad \text{if } C =_R A \wedge B$$

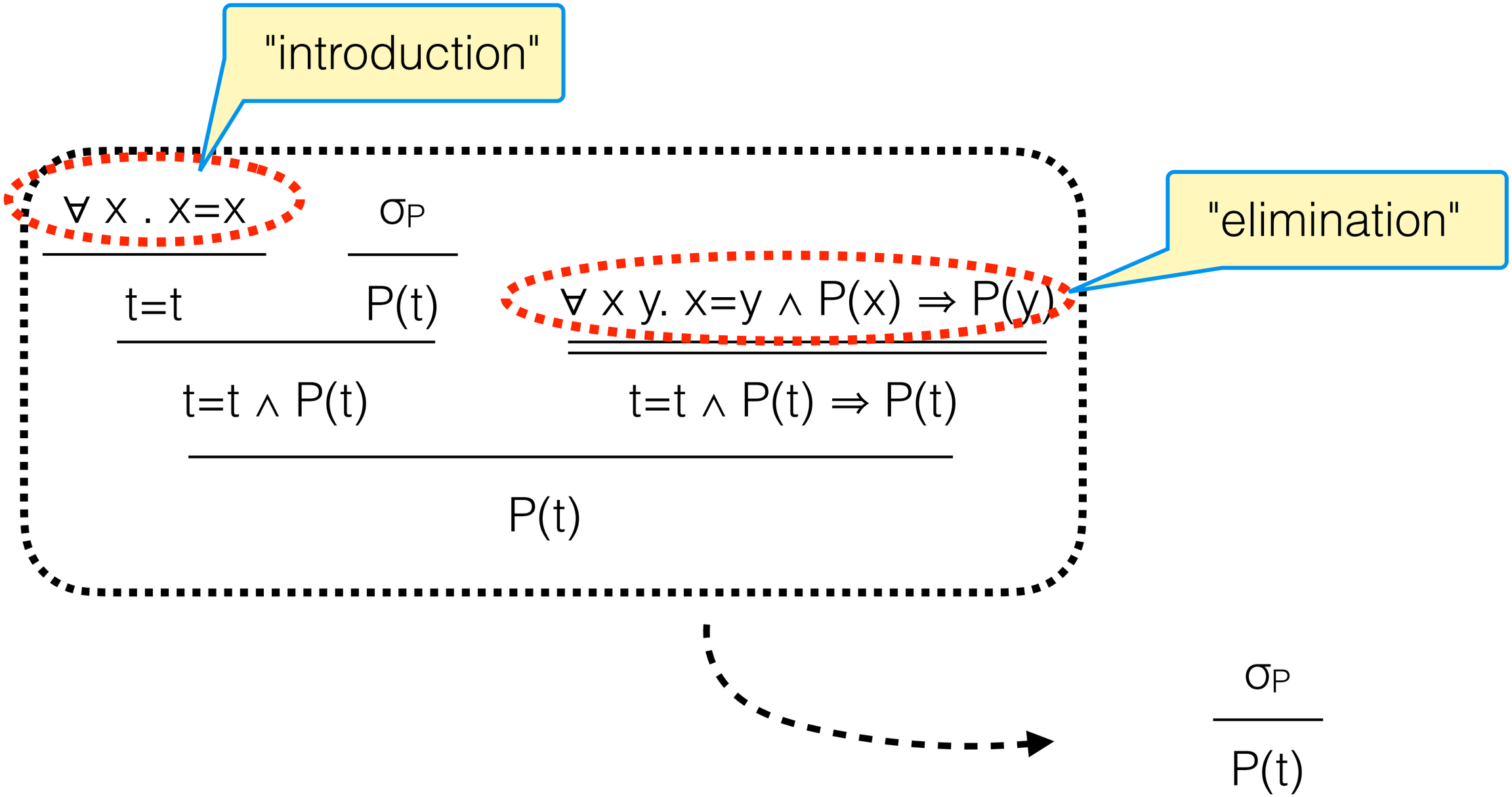
is now a cut

$$\wedge\text{-i}\ \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\wedge\text{-e}\ \dfrac{\Gamma \vdash A' \wedge B}{\Gamma \vdash A'}}$$

(we do the same for all rules)

Axiomatic Cuts

Equality Cut

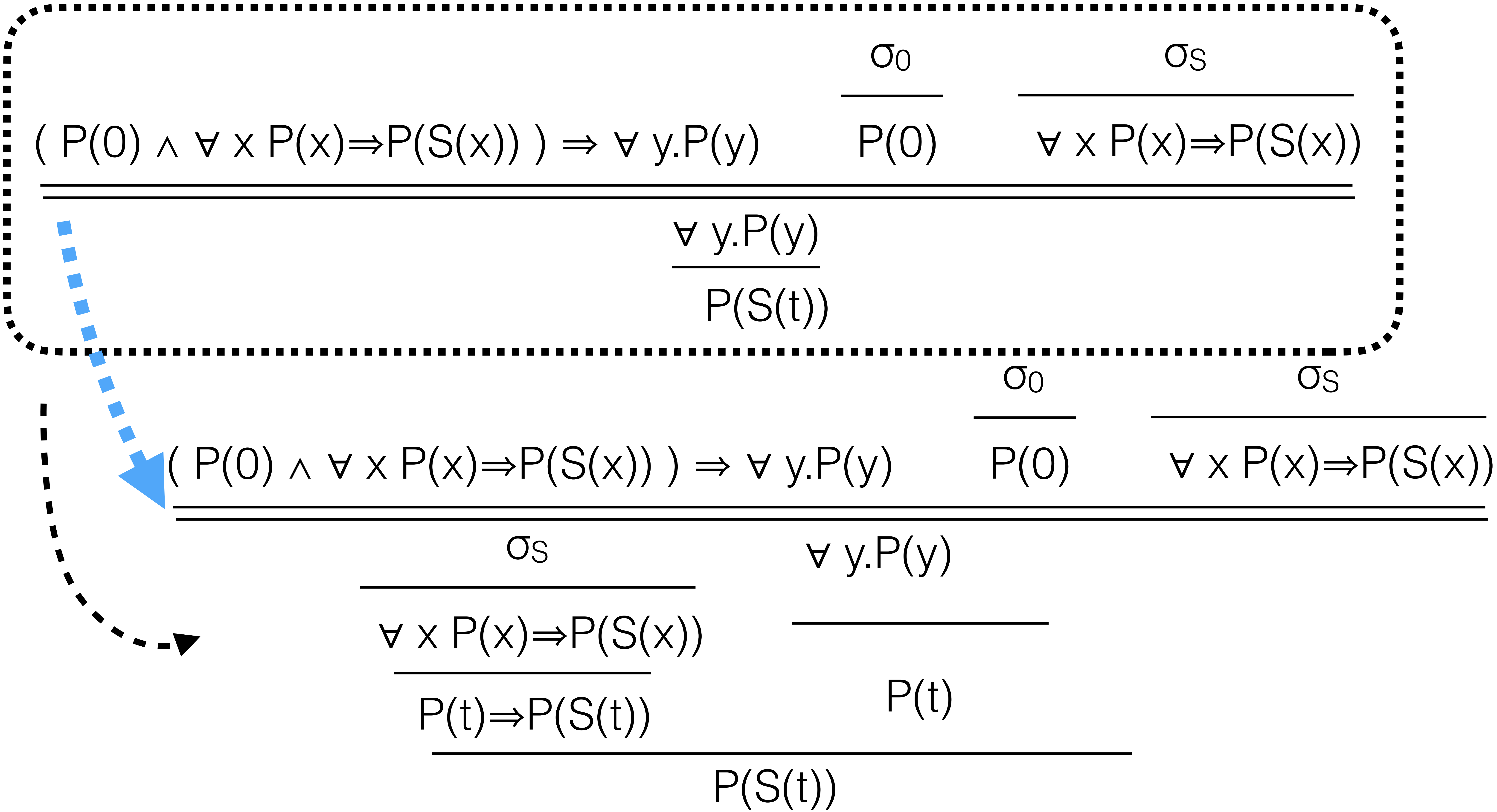


Induction Cut (1)

$$\dfrac{\dfrac{}{(\ P(0) \wedge \forall\ x\ P(x) \Rightarrow P(S(x))\ ) \Rightarrow \forall\ y.P(y)} \qquad \dfrac{\sigma_0}{P(0)} \qquad \dfrac{\sigma_S}{\forall\ x\ P(x) \Rightarrow P(S(x))}}{\dfrac{\forall\ y.P(y)}{P(0)}}$$

$$\dfrac{\sigma_0}{P(0)}$$

Induction cut (2)



Cut Free Proofs

Properties

easy:

If t is a term without free variables, then $t \rhd^* S^n(0)$

Cut free proofs:

Take A without free variables. Any cut-free proof of A in HA either :

- ends with an introduction
- is refl or t=t (from refl)
- is Leibniz or partial application of L : $\forall\, y.\ t=y \wedge P(t) \Rightarrow P(y)$, $u=t \wedge P(t) \Rightarrow P(u)$
- Is Induction or a partial application of it: $\forall\, y.\ P(y)$

by induction over the structure of the proof (somewhat tedious)

A without free variables. A cut-free proof of A in HA is either :

- ends with an introduction
- is refl or t=t (from refl)
- is Leibniz or partial application of L : $\forall$ y. t=y$\wedge$ P(t) $\Rightarrow$ P(y), u=y$\wedge$ P(t) $\Rightarrow$ P(u)
- Is Induction of proof partial application: $\forall$ y. P(y)

Constructivity :

- If $\vdash_{HA}$ A$\vee$ B, then either $\vdash_{HA}$ A or $\vdash_{HA}$ B
- if $\vdash_{HA}$ $\exists$ x. A(x) then we can extract n and a proof of $\vdash_{HA}$ A(n)

Consider : $\forall$ x. $\exists$ y. x=y+y $\vee$ x = S(y+y)

Heyting's semantics

To make the point of *constructivity*

- a proof of $n=n$ is 0 (some trivial object)
- a proof of $A \wedge B$ is (can be reduced to) (a,b) with a:A and b:B
- a canonical proof of $A \vee B$ is (ε,c) with $\varepsilon=0$ and c:A or $\varepsilon=1$ and c:B
- a proof of $A \Rightarrow B$ is a computational function f, s.t. if a:A, then $f(a)$: B
- a canonical proof of $\exists$ x.A is a pair (t,a) s.t. a: A[x \ t]
- a proof of $\forall$ x.A is a computational function f, s.t. for all n, $f(n)$: A[x \ n]

Why is arithmetic undecidable ?

t=u is decidable

In HA, we can *prove* $\forall x, \forall y, x=y \vee x \neq y$
(which is the good way to state decidability)
Let's do it

If A and B are decidable, so are $A \wedge B$, $A \vee B$, $A \Rightarrow B$

Undecidability comes "only" from the quantifiers

Even if for all x, we can determine A(x) or $\neg A(x)$, we do not know

whether $\forall x.A(x)$ is true or not

Simple game semantics

Let us keep a first–order language (actually arithmetic)
We drop the implication ⇒

For every predicate P we add its negation *P (same arity)
We *define* the negation of any proposition as:

$$\neg\, P(t_1, \ldots, t_n) \equiv {}^*P(t_1, \ldots, t_n)$$
$$\neg\, (A \vee B) \equiv \neg\, A \ \wedge \neg\, B$$
$$\neg\, (A \wedge B) \equiv \neg\, A \ \vee \neg\, B$$
$$\neg\, \forall\, x.\ A \equiv \exists\, x.\ \neg\, A$$
$$\neg\, \exists\, x.\ A \equiv \forall\, x.\ \neg\, A$$

Now ! Every closed proposition can be viewed as a *game* !
a game between the mathematician and nature

The game

The mathematician plays when the proposition is:

- ∃ x . A provides an object t, game becomes A[x \ t]
- A ∨ B chose left or right, game becomes A or B

Nature plays when the proposition is:

- ∀ x. A provides an object t, game becomes A[x \ t]
- A ∧ B chose left or right, game becomes A or B

The game stops when the proposition is atomic $P(t_1, \ldots t_n)$

- if $P(t_1, \ldots t_n)$ is true, mathematician wins
- if $P(t_1, \ldots t_n)$ is false, nature wins

Paul Lorenzen (1958)

A true intuitionistically: mathematician has a *winning strategy*

Going beyond intuitionistic logic

Remember we have classical logic in sequent calculus by authorizing sequents with several conclusions: $A_1, \ldots, A_n \vdash B_1, \ldots B_m$

We go to multigames: $A_1, \ldots, A_n$

idea: mathematician has to "prove" only one A_i

- if nature has to play on at least one A_i, it plays
- if not, mathematician plays on one A_i
- if A_i is $B \vee C$, mathematician can break it without choosing

  $B \vee C \rightsquigarrow B, C$
- if A_i is $\exists\, x.A$, then mathematician can "keep" the existential for another later attempt $\exists\, x.A \rightsquigarrow \exists\, x.A, A[x \setminus t]$

Excluded Middle in multi-games

$A \vee \neg A \quad \twoheadrightarrow \quad A, \neg A$

Now let us look at A:

if $B \wedge C$, then nature plays B or C

if $B \vee C$, then nature plays $\neg B$ or $\neg C$

if $\forall x.B$, then nature plays $B[x\backslash t]$

if $\exists x.B$, then nature plays $\neg B[x\backslash t]$

mathematician plays $\neg B$ or $\neg C$

mathematician plays B or C

mathematician plays $\neg B[x\backslash t]$

mathematician plays $B[x\backslash t]$

Mathematician wins !

when $\vdash A$ (in classical logic), there is a winning strategy (essentially a termination argument)

see for instance the page of Thierry Coquand about game semantics

Links with Curry-Howard for classical logic