Natural Formalism

Peter Koepke, University of Bonn, Germany

Philosophy of Mathematics Seminar, Oxford, 2 February 2015

Whitehead and Russell, *Principia Mathematica*

1+1=2:

$\vdash .(3).*11{\cdot}11{\cdot}35.*54{\cdot}101.\supset \vdash .\mathrm{Prop}$

***54·43.** $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash .*54{\cdot}26.\supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51·231] $\equiv . \iota`x \cap \iota`y = \Lambda .$

[*13·12] $\equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash .(1).*11{\cdot}11{\cdot}35.\supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash .(2).*11{\cdot}54.*52{\cdot}1.\supset \vdash .\mathrm{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

***54·44.** $\vdash :. z, w \in \iota`x \cup \iota`y . \supset_{z,w} . \phi(z, w) :\equiv . \phi(x, x) . \phi(x, y) . \phi(y, x) . \phi(y, y)$

Dem.

$\vdash .*51{\cdot}234.*11{\cdot}62.\supset \vdash :. z, w \in \iota`x \cup \iota`y . \supset \quad \phi(z, w) :\equiv :$

Bertrand Russell, *The Principles of Mathematics*

Logicism and formalism:

... the proof that all pure mathematics deals exclusively with concepts definable in terms of a very small number of fundamental logical concepts, and that all its propositions are deducible from a very small number of fundamental logical principles, is undertaken in [...] this Volume, and will be established by strict symbolic reasoning in Volume II.

The Gödel completeness theorem

Die Vollständigkeit der Axiome des logischen Funktionenkalküls [1].

Von **Kurt Gödel** in Wien.

Whitehead und Russell haben bekanntlich die Logik und Mathematik so aufgebaut, daß sie gewisse evidente Sätze als Axiome an die Spitze stellten und aus diesen nach einigen genau formulierten Schlußprinzipien auf rein formalem Wege (d. h. ohne weiter von der Bedeutung der Symbole Gebrauch zu machen) die Sätze der Logik und Mathematik deduzierten. Bei einem solchen Vorgehen erhebt sich natürlich sofort die Frage, ob das an die Spitze gestellte System von Axiomen und Schlußprinzipien vollständig ist, d. h. wirklich dazu ausreicht, jeden logisch-mathematischen Satz zu deduzieren, oder ob vielleicht wahre (und nach anderen Prinzipien ev. auch beweisbare) Sätze denkbar sind, welche in dem betreffenden System nicht abgeleitet werden können. Für den Bereich der logischen Aussageformeln ist diese Frage in positivem Sinn entschieden, d. h.

Gödel on the possibility of Formal Mathematics

Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I[1]).

Von Kurt Gödel in Wien.

1.

Die Entwicklung der Mathematik in der Richtung zu größerer Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete von ihr formalisiert wurden, in der Art, daß das Beweisen nach einigen wenigen mechanischen Regeln vollzogen werden kann. Die umfassendsten derzeit aufgestellten formalen Systeme sind das System der Principia Mathematica (PM)[2]) einerseits, das Zermelo-Fraenkelsche (von J. v. Neumann weiter ausgebildete) Axiomensystem der Mengenlehre[3]) andererseits. Diese beiden Systeme sind so weit, daß alle heute in der Mathematik angewendeten Beweismethoden in ihnen formalisiert, d. h. auf einige wenige Axiome und Schlußregeln zurückgeführt sind. Es liegt daher die Vermutung nahe, daß diese Axiome

... These two systems are strong enough that all proof methods applied in mathematics today can be formalized in them, i.e., can be reduced to a small number of axioms and derivation rules. ...

Formal proofs - derivations

E.g., derivation rules in Ebbinghaus, Flum, Thomas:

$$\frac{\Gamma \quad \varphi}{\Gamma \quad \psi \quad \varphi}$$

$$\frac{}{\Gamma \quad \varphi \quad \varphi}$$

$$\frac{\Gamma \quad \varphi \quad \psi}{\Gamma \quad \varphi \to \psi}$$

$$\frac{\Gamma \quad \varphi \qquad \Gamma \quad \varphi \to \psi}{\Gamma \quad \psi}$$

$$\frac{\Gamma \quad \varphi \qquad \Gamma \quad \neg\varphi}{\Gamma \quad \bot}$$

$$\frac{\Gamma \quad \varphi \qquad \Gamma \quad \neg\varphi}{\Gamma \quad \bot}$$

$$\frac{\Gamma \quad \neg\varphi \quad \bot}{\Gamma \quad \varphi}$$

$$\frac{\Gamma \quad \varphi\frac{y}{x}}{\Gamma \quad \forall x\varphi}\ ,$$

if $y \notin \mathrm{free}(\Gamma \cup \{\forall x\varphi\})$

$$\frac{\Gamma \quad \forall x\varphi}{\Gamma \quad \varphi\frac{t}{x}}$$

$$\frac{}{\Gamma \quad t \equiv t}$$

$$\frac{\Gamma \quad \varphi\frac{t}{x} \qquad \Gamma \quad t \equiv t'}{\Gamma \quad \varphi\frac{t'}{x}}$$

First-order set-theoretic axioms

Axiom of extensionality: $\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x \equiv y)$

...

Set comprehension schema: $\forall x_1 ... \forall x_n \forall x \exists y \forall z \, (z \in y \leftrightarrow z \in x \wedge \varphi(z, x_1, ..., x_n))$

...

Axiom of infinity:$\exists x (\exists y \, (y \in x \wedge \forall z \neg z \in y) \wedge \forall y (y \in x \rightarrow \exists z (z \in x \wedge \forall w (w \in z \leftrightarrow w \in y \vee w \equiv y))))$

...

The Gödel completeness theorem

Every logically true mathematical statement has a formal derivation.

The Gödel completeness theorem + set theoric / type theoric foundations

Every logically true mathematical statement has a formal derivation.

Every true mathematical statement has a formal derivation within some (foundational) axiom system.

The Gödel completeness theorem + set theoric / type theoric foundations

Every logically true mathematical statement has a formal derivation.

Every true mathematical statement has a formal derivation within some (foundational) axiom system.

Every mathematical proof can be replaced by a formal derivation.

The Gödel completeness theorem + set theoric / type theoric foundations

Every logically true mathematical statement has a formal derivation.

Every true mathematical statement has a formal derivation within some (foundational) axiom system.

Every mathematical proof can be replaced by a formal derivation.

Mathematics can be in principle be carried out completely formal (*Formal mathematics*).

1.	Φ_{Gr}	$\neg \circ v_0\, e \equiv v_0$		$\neg\exists v_0\, \neg \circ v_0\, e \equiv v_0$	Assumpt
2.	Φ_{Gr}	$\neg \circ v_0\, e \equiv v_0$		$\neg \circ v_0\, e \equiv v_0$	Assumpt
3.	Φ_{Gr}	$\neg \circ v_0\, e \equiv v_0$		$\exists v_0\, \neg \circ v_0\, e \equiv v_0$	$\exists$Intro with 2
4.	Φ_{Gr}			$\circ v_0\, e \equiv v_0$	Contr with 1,3
5.				$(v_2 \equiv \circ v_0\, e)\frac{\circ v_0\, e}{v_2}$	$(\equiv)$
6.		$\circ v_0\, e \equiv v_0$		$(v_2 \equiv \circ v_0\, e)\frac{v_0}{v_2}$	Sub with 5
7.	Φ_{Gr}	$\circ v_0\, e \equiv v_0$		$v_0 \equiv \circ v_0\, e$	Mono with 6
8.	Φ_{Gr}			$v_0 \equiv \circ v_0\, e$	Cut with 4,7
9.	Φ_{Gr}	$v_0 \equiv e$		$v_0 \equiv e$	Assumpt
10.	Φ_{Gr}	$v_0 \equiv e$		$(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\vee$Intro with 9
11.	Φ_{Gr}	$\neg v_0 \equiv e$		$(\neg v_2 \equiv e)\frac{v_0}{v_2}$	Assumpt
12.	Φ_{Gr}	$\neg v_0 \equiv e$	$v_0 \equiv \circ v_0\, e$	$(\neg v_2 \equiv e)\frac{\circ v_0\, e}{v_2}$	Sub with 11
13.	Φ_{Gr}	$\neg v_0 \equiv e$	$v_0 \equiv \circ v_0\, e$	$\neg \circ v_0\, e \equiv e$	12
14.	Φ_{Gr}	$\neg v_0 \equiv e$		$v_0 \equiv \circ v_0\, e$	Mono with 8
15.	Φ_{Gr}	$\neg v_0 \equiv e$		$\neg \circ v_0\, e \equiv e$	$\equiv$Sym with 14
16.	Φ_{Gr}	$\neg v_0 \equiv e$		$(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\vee$Intro with 15
17.	Φ_{Gr}			$(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Cases with 10,16
18.	Φ_{Gr}	$\neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\neg\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Mono with 17
19.	Φ_{Gr}	$\neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\neg\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Assumpt
20.	Φ_{Gr}	$\neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$		$\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Contr with 18,19
21.	Φ_{Gr}	$\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$		$\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	$\exists$Intro with 20
22.	Φ_{Gr}	$\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$		$\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Assumpt
23.	Φ_{Gr}			$\neg\exists v_0 \neg(\neg \circ v_0\, e \equiv e \vee v_0 \equiv e)$	Cases with 21,22

Bourbaki, *Theory of Sets*

Description of Formal Mathematics

1. TERMS AND RELATIONS

1. SIGNS AND ASSEMBLIES

The *signs* of a mathematical theory $\mathfrak{T}$ (*) are the following :

(1) The *logical signs* (†) : $\square$, τ, $\vee$, $\neg$.
(2) The *letters*.

Bourbaki, *Theory of Sets*

Infeasibility of formal mathematics:

If formalized mathematics were as simple as the game of chess, then once our chosen formalized language had been described there would remain only the task of writing out our proofs in this language, [...] But the matter is far from being as simple as that, and no great experience is necessary to perceive that such a project is absolutely unrealizable: the tiniest proof at the beginnings of the Theory of Sets would already require several hundreds of signs for its complete formalization. [...] formalized mathematics cannot in practice be written down in full, [...] We shall therefore very quickly abandon formalized mathematics, [...]

Saunder Mac Lane

Formal mathematics as ultimate standard for correctness:

As to precision, we have now stated an absolute standard of rigor: A mathematical proof is rigorous when it is (or could be) written out in the first-order predicate language $L(\in)$ as a sequence of inferences from the axioms ZFC, each inference made according to one of the stated rules. [...] When a proof is in doubt, its repair is usually a partial approximation to the fully formal version.

John McCarthy

(Formal) mathematics with computer assistance:

Checking mathematical proofs is potentially one of the most interesting and useful applications of automatic computers. ... Proofs to be checked by computer may be briefer and easier to write than the informal proofs acceptable to mathematicians. This is because the computer can be asked to do much more work to check each step than a human is willing to do, and this permits longer and fewer steps.

McCarthy, J. "Computer Programs for Checking Mathematical Proofs," Proceedings of the Symposium in Pure Math, Recursive Function Theory,Volume V, pages 219-228, AMS, Providence, RI, 1962.

N. G. de Bruijn

Automatic proof checking:

Automath (~1967)

Automath: $i*i=-1$

```
ic:=pli(0,1rl):complex
+10300
t1:=tsis12a(0,1rl,0,1rl):is(ts(ic,ic),pli(mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),pl"r"(ts"r"(0,1rl),
ts"r"(1rl,0))))
t2:=tris(real,mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),m0"r"(ts"r"(1rl,1rl)),m0"r"(1rl),pl01(ts"r"(0,0),
m0"r"(ts"r"(1rl,1rl)),ts01(0,0,refis(real,0))),ism0"r"(ts"r"(1rl,1rl),1rl,satz195(1rl))):
is"r"(mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),m0"r"(1rl))
t3:=tris(real,pl"r"(ts"r"(0,1rl),ts"r"(1rl,0)),ts"r"(1rl,0),0,pl01(ts"r"(0,1rl),ts"r"(1rl,0),
ts01(0,1rl,refis(real,0))),ts02(1rl,0,refis(real,0))):is"r"(pl"r"(ts"r"(0,1rl),ts"r"(1rl,0)),0)
t4:=isrecx12(mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),m0"r"(1rl),pl"r"(ts"r"(0,1rl),
ts"r"(1rl,0)),0,t2,t3):is(pli(mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),
pl"r"(ts"r"(0,1rl),ts"r"(1rl,0))),cofrl(m0"r"(1rl)))
t5:=satz298j(1rl):is(cofrl(m0"r"(1rl)),m0(1c))
-10300
satz2300:=tr3is(cx,ts(ic,ic),pli(mn"r"(ts"r"(0,0),ts"r"(1rl,1rl)),
pl"r"(ts"r"(0,1rl),ts"r"(1rl,0))),cofrl(m0"r"(1rl)),m0(1c),t1".10300",t4".10300",t5".10300"):
is(ts(ic,ic),m0(1c))
```

Andrzej Trybulec

The MIZAR system, 1973 - ... :

Language modeled after
“mathematical vernacular”

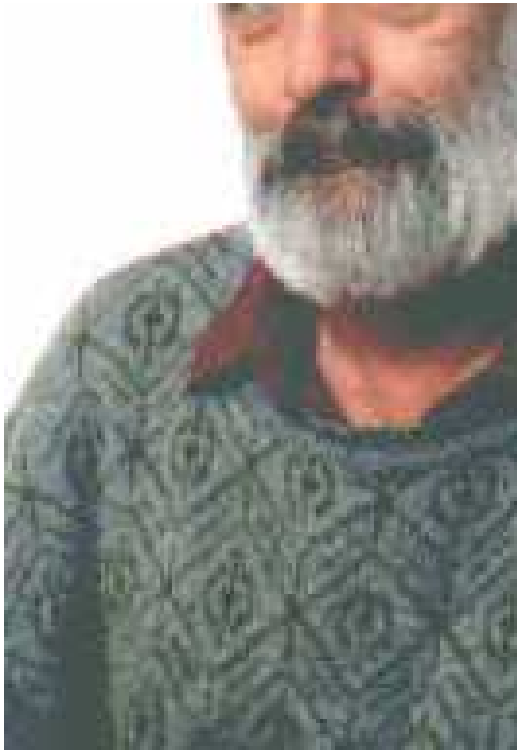
Natural deduction style

Automatic proof checker

Large mathematical library

Journal
Formalized Mathematics

www.mizar.org



MIZAR example

Proof of Pythagoras theorem:

```
theorem for p1,p2,p3 st p1<>p2 & p3<>p2 &
    (angle(p1,p2,p3)=PI/2 or angle(p1,p2,p3)=3/2*PI) holds
    (|.p1-p2.|^2+|.p3-p2.|^2=|.p1-p3.|^2
    proof let p1,p2,p3; assume A1: p1<>p2 & p3<>p2 &
    (angle(p1,p2,p3)=PI/2 or angle(p1,p2,p3)=3/2*PI);
  then A2: euc2cpx(p1)<> euc2cpx(p2) by Th6;
  A3: euc2cpx(p3)<> euc2cpx(p2) by A1,Th6;
  A4: euc2cpx(p1)-euc2cpx(p2)=euc2cpx(p1-p2) by Th19;
  A5: euc2cpx(p3)-euc2cpx(p2)=euc2cpx(p3-p2) by Th19;
  A6: euc2cpx(p1)-euc2cpx(p3)=euc2cpx(p1-p3) by Th19;
   A7:  angle(p1,p2,p3)=angle(euc2cpx(p1),euc2cpx(p2),euc2cpx(p3))
by Def4;
  A8: |.euc2cpx(p1-p2).|=|.p1-p2.| by Th31;
  A9: |.euc2cpx(p3-p2).|=|.p3-p2.| by Th31;
   |.euc2cpx(p1-p3).|=|.p1-p3.| by Th31;
  hence thesis by A1,A2,A3,A4,A5,A6,A7,A8,A9,COMPLEX2:91;
end;
```

Further development of formal mathematics systems

- Automath, de Bruijn, ~1967
- Mizar, Trybulec, ~1973
- Isabelle/Isar, Paulson, Nipkow, Wenzel, ~1980's
- Coq, ~1990's
- HOL Light, Harrison
- many others

Substantial mathematics in Mizar

Banach Fixed Point Theorem for compact spaces

Brouwer Fixed Point Theorem

Fermat's Little Theorem

Fundamental Theorem of Algebra

Fundamental Theorem of Arithmetic

Gödel Completeness Theorem, the Hahn-Banach Theorem

Jordan Curve Theorem for special polygons, ...

Mizar proof of the Gödel Completeness Theorem

```
...
...
:: Completeness Theorem
theorem
PSI |= p implies PSI |- p
proof
  set CHI = PSI \/ {'not' p};
  assume A1: PSI |= p;
  assume not PSI |- p;
  then CHI is consistent by HENMODEL:9;
  then ex A,J,v st J,v |= CHI by Def1;
  hence contradiction by GOEDELCP:37,A1;
end;
```

Substantial mathematics in Isabelle/Isar

The relative consistency of the axiom of choice (Gödel)

Gödel's incompleteness theorems

Substantial mathematics in Coq

Fundamental Theorem of Algebra

Four Colour Theorem

Feit-Thompson-Theorem (Odd order theorem)

...

Georges Gonthier: Coq proof of the Four Colour Theorem

```
.....
Theorem four_color_finite :
   forall m : map R, finite_simple_map m -> map_col-
orable 4 m.
Proof.
exact (fun m Hm =>
                let: ex_intro2 g Hg Hgm := dis-
cretize_to_hypermap Hm in
       Hgm (four_color_hypermap Hg)).
Qed.

Theorem four_color : forall m : map R, simple_map m ->
map_colorable 4 m.
Proof.
exact (compactness_extension four_color_finite).
Qed.
```

Freek Wiedijk, 2007

Why does formal mathematics not catch on?

> The other reason that there has not been much progress on the vision from the QED manifesto is that currently formalized mathematics does not resemble real mathematics at all. Formal proofs look like computer program source code.

Euclid

Natural language formalism in the proof of Pythagoras' theorem:

Dem.—On the sides $A\,B$, $B\,C$, $C\,A$ describe squares [xlvi.]. Draw $C\,L$ parallel to $A\,G$. Join $C\,G$, $B\,K$. Then because the angle $A\ C\ B$ is right (hyp.), and $A\ C\ H$ is right, being the angle of a square, the sum of the angles $A\,C\,B$, $A\,C\,H$ is two right angles; therefore $B\,C$, $C\,H$ are in the same right line [xiv.]. In like manner $A\,C$, $C\,D$ are in the same right line. Again, because $B\,A\,G$ is the angle of a square it is a right angle: in like manner $C\ A\ K$ is a right angle. Hence $B\ A\ G$ is equal to $C\ A\ K$: to each add $B\ A\ C$, and we get the angle $C\,A\,G$ equal to $K\,A\,B$. Again, since $B\,G$ and $C\,K$ are squares, $B\,A$ is equal to $A\,G$, and $C\,A$ to $A\,K$. Hence the two triangles $C\,A\,G$, $K\,A\,B$ have the sides $C\,A$, $A\,G$ in one respectively equal to the sides $K\,A$, $A\,B$ in the other, and the contained angles $C\,A\,G$, $K\,A\,B$ also equal. Therefore [iv.] the triangles are equal; but the parallelogram $A\ L$ is double of the triangle $C\ A\ G$ [xli.], because they are on the same base $A\,G$, and between the same parallels $A\ G$ and $C\ L$. In like manner the parallelogram $A\ H$ is double of the triangle $K\ A\ B$, because they are on the same base $A\,K$, and between the same parallels $A\,K$ and $B\,H$; and since doubles of equal things are equal (Axiom vi.), the parallelogram $A\,L$ is equal to $A\,H$. In like manner it can be proved that the parallelogram $B\ L$ is equal to $B\ D$. *Hence the whole square* $A\ F$ *is equal to the sum of the two squares* $A\,H$ *and* $B\,D$.

Euclid

Formalism in the proof of Pythagoras' theorem:

Dem.—On the sides $A\,B$, $B\,C$, $C\,A$ describe squares [xlvi.]. Draw $C\,L$ parallel to $A\,G$. Join $C\,G$, $B\,K$. Then because the angle $A\ C\ B$ is right (hyp.), and $A\ C\ H$ is right, being the angle of a square, the sum of the angles $A\,C\,B$, $A\,C\,H$ is two right angles; therefore $B\,C$, $C\,H$ are in the same right line [xiv.]. In like manner $A\,C$, $C\,D$ are in the same right line. Again, because BAG is the angle of a square it is a right angle: in like manner CAK is a right angle. Hence $B\ A\ G$ is equal to $C\ A\ K$: to each add $B\ A\ C$, and we get the angle $C\,A\,G$ equal to $K\,A\,B$. Again, since $B\,G$ and $C\,K$ are squares, $B\,A$ is equal to $A\,G$, and $C\,A$ to $A\,K$. Hence the two triangles $C\,A\,G$, $K\,A\,B$ have the sides $C\,A$, $A\,G$ in one respectively equal to the sides $K\,A$, $A\,B$ in the other, and the contained angles $C\,A\,G$, $K\,A\,B$ also equal. Therefore [iv.] the triangles are equal; but the parallelogram $A\ L$ is double of the triangle $C\ A\ G$ [xli.], because they are on the same base $A\,G$, and between the same parallels $A\ G$ and $C\ L$. In like manner the parallelogram $A\ H$ is double of the triangle $K\ A\ B$, because they are on the same base $A\,K$, and between the same parallels $A\,K$ and $B\,H$; and since doubles of equal things are equal (Axiom vi.), the parallelogram $A\,L$ is equal to $A\,H$. In like manner it can be proved that the parallelogram $B\ L$ is equal to $B\ D$. *Hence the whole square* $A\ F$ *is equal to the sum of the two squares* $A\,H$ *and* $B\,D$.

Euclid

Formalism in the proof of Pythagoras' theorem:

Dem.—On the sides $A\,B$, $B\,C$, $C\,A$ describe squares [xlvi.]. Draw $C\,L$ parallel to $A\,G$. Join $C\,G$, $B\,K$. Then because the angle $A\ C\ B$ is right (hyp.), and $A\ C\ H$ is right, being the angle of a square, the sum of the angles $A\,C\,B$, $A\,C\,H$ is two right angles; therefore $B\,C$, $C\,H$ are in the same right line [xiv.]. In like manner $A\,C$, $C\,D$ are in the same right line. Again, because $B\,A\,G$ is the angle of a square it is a right angle: in like manner $C\,A\,K$ is a right angle. Hence $B\,A\,G$ is equal to $C\,A\,K$: to each add $B\ A\ C$, and we get the angle $C\,A\,G$ equal to $K\,A\,B$. Again, since $B\,G$ and $C\,K$ are squares, $B\,A$ is equal to $A\,G$, and $C\,A$ to $A\,K$. Hence the two triangles $C\,A\,G$, $K\,A\,B$ have the sides $C\,A$, $A\,G$ in one respectively equal to the sides $K\,A$, $A\,B$ in the other, and the contained angles $C\,A\,G$, $K\,A\,B$ also equal. Therefore [iv.] the triangles are equal; but the parallelogram $A\ L$ is double of the triangle $C\ A\ G$ [xli.], because they are on the same base $A\,G$, and between the same parallels $A\ G$ and $C\ L$. In like manner the parallelogram $A\ H$ is double of the triangle $K\ A\ B$, because they are on the same base $A\,K$, and between the same parallels $A\,K$ and $B\,H$; and since doubles of equal things are equal (Axiom vi.), the parallelogram $A\,L$ is equal to $A\,H$. In like manner it can be proved that the parallelogram $B\ L$ is equal to $B\ D$. *Hence the whole square* $A\ F$ *is equal to the sum of the two squares* $A\,H$ *and* $B\,D$.

Hilbert, *Foundations of Geometry*

Natural language in Hilbert's axiomatism / formalism:

§ 1.

Die Elemente der Geometrie und die fünf Axiomgruppen.

Erklärung. Wir denken drei verschiedene Systeme von Dingen: die Dinge des ersten Systems nennen wir *Punkte* und bezeichnen sie mit $A, B, C, \ldots$; die Dinge des zweiten Systems nennen wir *Gerade* und bezeichnen sie mit $a, b, c, \ldots$; die Dinge des dritten Systems nennen wir *Ebenen* und bezeichnen sie mit $\alpha, \beta, \gamma, \ldots$; die Punkte heißen auch die *Elemente der linearen Geometrie*, die Punkte und Geraden heißen die *Elemente der ebenen Geometrie* und die Punkte, Geraden und Ebenen heißen die *Elemente der räumlichen Geometrie* oder *des Raumes*.

Wir denken die Punkte, Geraden, Ebenen in gewissen gegenseitigen Beziehungen und bezeichnen diese Beziehungen durch Worte wie „liegen", „zwischen", „parallel", „kongruent", „stetig"; die genaue und vollständige Beschreibung dieser Beziehungen erfolgt durch die *Axiome der Geometrie*.

Hilbert, *Foundations of Geometry*

Natural language in Hilbert's axiomatism / formalism:

I 1. *Zwei von einander verschiedene Punkte A, B bestimmen stets eine Gerade a.*

Statt „bestimmen" werden wir auch andere Wendungen gebrauchen, z. B. *a* „geht durch" *A* „und durch" *B*, *a* „verbindet" *A* „und" oder „mit" *B*. Wenn *A* ein Punkt ist, der mit einem anderen Punkte zusammen die Gerade *a* bestimmt, so gebrauchen wir auch die Wendungen: *A* „liegt auf" *a*, *A* „ist ein Punkt von" *a*, „es gibt den Punkt" *A* „auf" *a* u. s. w. Wenn *A* auf der Geraden *a* und außerdem auf einer anderen Geraden *b* liegt, so gebrauchen wir auch die Wendung: „die Geraden" *a* „und" *b* „haben den Punkt *A* gemein" u. s. w.

I 2. *Irgend zwei voneinander verschiedene Punkte einer Geraden bestimmen diese Gerade.*

Felix Hausdorff

Review of Russel's *The Principles of Mathematics. Vol. I* (1905)

> [...] *Formalismus* [...], der in immer wachsender Bestimmtheit und Bewusstheit die moderne Mathematik beherrscht; [...] Formalismus, der ursprünglich nichts weiter will als die Voraussetzungen jeder Deduktion ausdrücklich hervorheben und nebelhafte Berufungen auf scheinbar Selbstverständliches vermeiden, der in seiner weiteren Entwicklung zur völligen Emanzipation von der "Anschauung" und sonstigen spezifischen, ausserlogischen Erkenntnisquellen geführt hat, und der in seiner gegenwärtigen Gestalt zugleich eine Pflicht und ein Recht der reinen Mathematik bezeichnet: die Pflicht, nirgends auf die zufällige aktuelle Bedeutung der Objekte und ihrer Verknüpfungen zu rekurrieren, sondern aus präzise angegebenen undefinierten Begriffen und undeduzierten Urteilen (Axiomen) alles Uebrige zu definieren und zu deduzieren, und das Recht, einem solchermassen rein logisch aufgebauten System von Dingen und Beziehungen jede logisch zulässige Interpretation zu geben.

Felix Hausdorff

Review of Russel's *The Principles of Mathematics. Vol. I* (1905)

> ([...] *formalism* [...], which dominates modern mathematics in an ever growing determinateness and consciousness; [...] formalism which originally only intends to clearly bring out the premises of each deduction and to avoid nebulous appeals to the seemingly self-evident, and which in its further development has lead to the complete emancipation from "intuition" and other specific, extra-logical sources of knowledge, and which in its present form also defines a duty and a right of pure mathematics: the duty, never to recurr onto the accidental actual meaning of the objects and their relation, but to define and deduce from precisely given undefined notions and undeduced judgments (axioms) everything else, and the right to give such a logically built system of things and relations every logically admissable interpretation.)

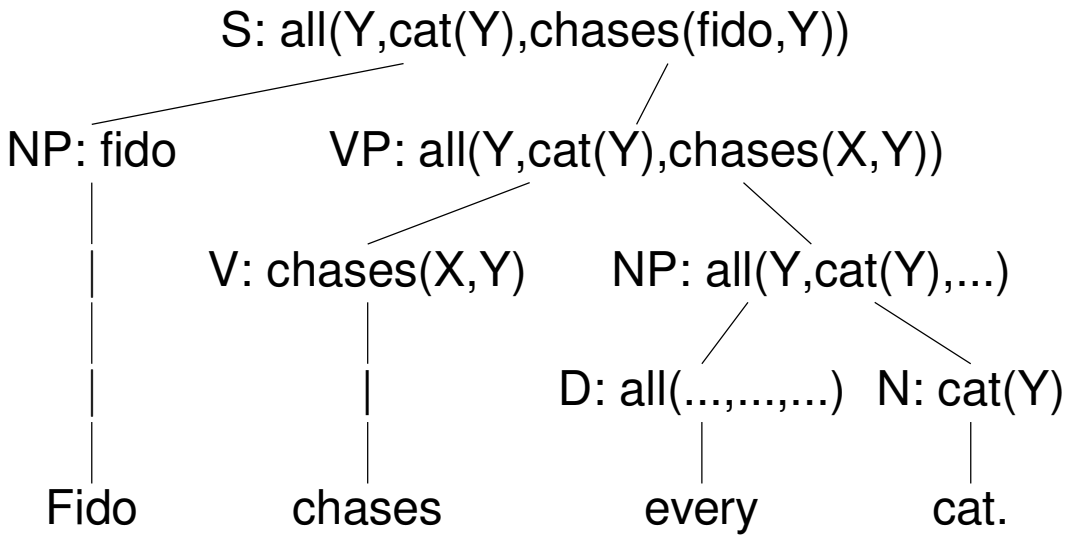
Richard Montague

English as a formal language:

> There is in my opinion no important theoretical difference between natural languages and the artificial languages of logicians: indeed, I consider it possible to comprehend the syntax and semantics of both kinds of languages within a single natural and mathematically precise theory.

Linguistic analysis

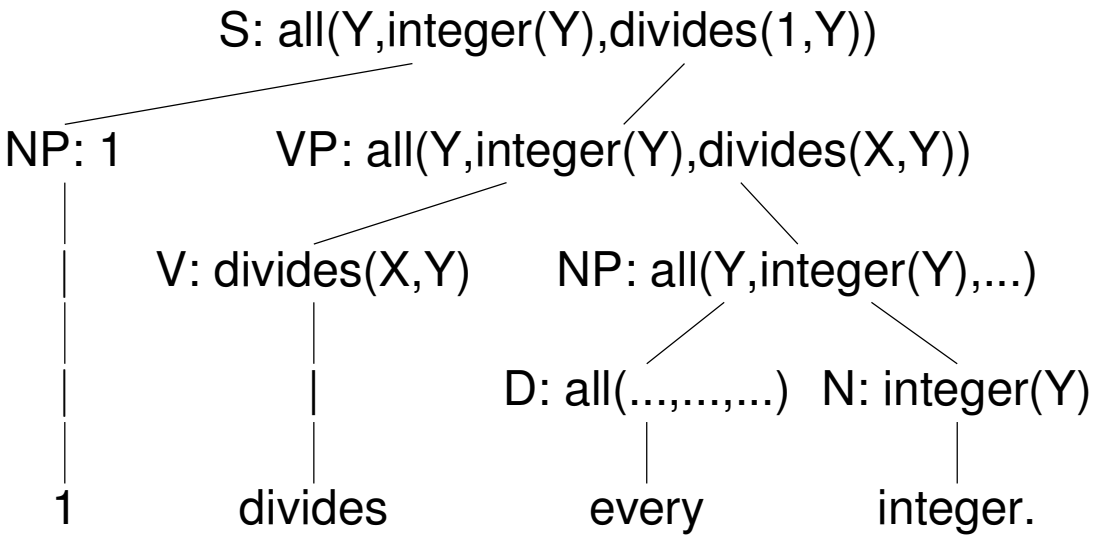
“Fido chases every cat.”



$\forall Y(\mathrm{cat}(Y) \rightarrow \mathrm{chases}(\mathrm{fido}, Y))$.

Linguistic analysis

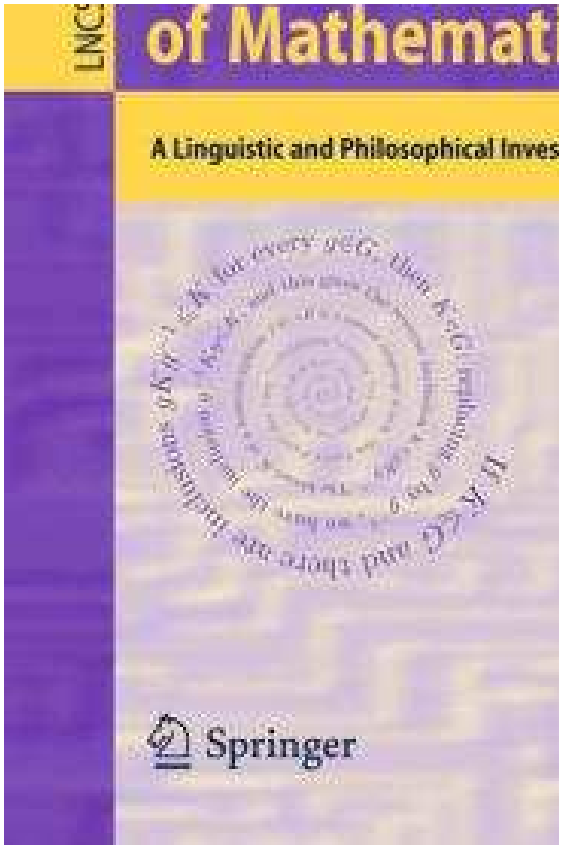
“1 divides every integer.”



$\forall Y\,(\mathrm{integer}(Y) \to 1|Y)$.

The Language of Mathematics

- Mohan Ganesalingam: *The Language of Mathematics*,



(Statement-level) natural formalism

- there are natural language statements that have definite, unambiguous translations into first-order logic
- those statements can be generated by grammars familiar from formal linguistics
- grammars can/must be computer-implemented
- grammars can also encompass LaTeX-style symbolic material
- such a grammar defines a *controlled natural language for mathematics*
- the controlled language should be mathematically natural and expressive
- rich (weak) type / sort system
- common (LaTeX) constant, function, and relation symbols

The Naproche project: Natural language proof checking

- studies the syntax and semantics of the language of proofs, emphasizing natural language and natural argumentation aspects
- models natural language proofs using computer-supported methods of formal linguistics and formal logic
- “reverse engineering” approach to derivation-indication
- joint work with Bernhard Schröder, linguistics; Bonn, Essen, Cologne; www.naproche.net
- development of a mathematical authoring system with a LaTeX-quality graphical interface

The Naproche project: Natural language proof checking

- devise a strictly formal system for mathematics, implemented by computer, whose input language is an extensive part of the common mathematical language, and whose proof style is close to proof styles found in the mathematical literature.

Layers of the Naproche system:

↓ Standard or web editor

TeX-style input text

↕ Natural language processing (NLP)

Proof representation structure (PRS)

↕ First-order translation

First-order logic format (TPTP)

↕ Proof checker or automatic theorem prover (ATP)

“Accepted”/“Not accepted”, with error messages

E. Landau, *Grundlagen der Analysis*, 1930

Theorem 30 (Distributive Law):

$$x(y+z) = xy + xz.$$

Preliminary Remark: The formula

$$(y+z)x = yx + zx$$

which results from Theorem 30 and Theorem 29, and similar analogues later on, need not be specifically formulated as theorems, nor even be set down.

Proof: Fix x and y, and let $\mathfrak{M}$ be the set of all z for which the assertion holds true.

I) $x(y+1) = xy' = xy + x = xy + x \cdot 1$;

1 belongs to $\mathfrak{M}$.

II) If z belongs to $\mathfrak{M}$, then

$$x(y+z) = xy + xz,$$

hence

$$x(y+z') = x((y+z)') = x(y+z)+x = (xy+xz)+x = xy+(xz+x) = xy+xz',$$

so that z' belongs to $\mathfrak{M}$.

Therefore, the assertion always holds.

Theorem 30: For all x, y, z, $x*(y+z) = (x*y)+(x*z)$.

Proof: Fix x, y. $x*(y+1) = x*y' = x*y + x = (x*y)+(x*1)$.

Now suppose $x*(y+z) = (x*y)+(x*z)$. Then $x*(y+z') = x*((y+z)') = (x*(y+z))+x = ((x*y)+(x*z))+x = (x*y)+((x*z)+x) = (x*y)+(x*z')$.

Thus by induction, for all z, $x*(y+z) = (x*y)+(x*z)$. Qed.

Andrei Paskevich' System of Automatic Deduction (SAD)

- started by Victor Glushkov, continued with Alexander Lyaletski and Konstantin Verchinine

- simple phrase structure grammar

- has reasoner and automatic theorem prover

- http://nevidal.org/sad.en.html

The SAD project: System for Automated Deduction

- A. Lyaletski, A. Paskevich, K. Verchinine
- ForTheL: Formula Theory Language, a controlled English with mathematical notation
- Reasoner performing “obvious” inferences
- generic interface to first-order provers

The SAD project: System for Automated Deduction

$\sqrt{p}$ *is irrational*:

Theorem Main.

For all nonzero natural numbers n,m,p if p * (m * m) = (n * n) then p is compound.

Proof by induction. Let n,m,p be nonzero natural numbers. Assume that p * (m * m) = (n * n). Assume that p is prime. Hence p divides n * n and p divides n. Take q = n / p.
Then m * m = p * (q * q). Indeed p * (m * m) = p * (p * (q * q)). m < n. Indeed n <= m => n * n <= m * m.

Hence p is compound.

qed.

The SAD project: System for Automated Deduction

SAD *as a formal calculus*:

Theorem Main.

For all nonzero natural numbers n,m,p if p * (m * m) = (n * n) then p is compound.

Proof by induction. Let n,m,p be nonzero natural numbers. Assume that p * (m * m) = (n * n). Assume that p is prime. Hence p divides n * n and p divides n. Take q = n / p.
Then m * m = p * (q * q). Indeed p * (m * m) = p * (p * (q * q)). m < n. Indeed n <= m => n * n <= m * m.

Hence p is compound.

qed.

The SAD project: System for Automated Deduction

SAD *as a formal calculus*:

Theorem Main.

For all nonzero natural numbers n,m,p if p * (m * m) = (n * n) then p is compound.

Proof by induction. Let n,m,p be nonzero natural numbers. Assume that p * (m * m) = (n * n). Assume that p is prime. Hence p divides n * n and p divides n . Take q = n / p.
Then m * m = p * (q * q). Indeed p * (m * m) = p * (p * (q * q)). m < n. Indeed n <= m => n * n <= m * m.

Hence p is compound.

qed.

The SAD project: System for Automated Deduction

SAD *as a formal calculus*:

Theorem Main.

For all nonzero natural numbers n,m,p if p * (m * m) = (n * n) then p is compound.

Proof by induction. Let n,m,p be nonzero natural numbers. Assume that p * (m * m) = (n * n). Assume that p is prime. Hence p divides n * n and p divides n. Take q = n / p.
Then m * m = p * (q * q). Indeed p * (m * m) = p * (p * (q * q)). m < n. Indeed n <= m => n * n <= m * m.

Hence p is compound. qed.

The Ganesalingam-Gowers Project

- http://gowers.wordpress.com/2013/04/14/answers-results-of-polls-and-a-brief-description-of-the-program/

- Mohan Ganesalingam and Timothy Gowers

- automatically generating canonical natural language proofs

- tested for “naturality“

The Ganesalingam-Gowers Project

Problem 2. Let X and Y be metric spaces, let $f\colon X \to Y$ be continuous, and let U be an open subset of Y. Then $f^{-1}(U)$ is an open subset of X.

Solution 2(a) Let x be an element of $f^{-1}(U)$. Then $f(x) \in U$. Therefore, since U is open, there exists $\eta > 0$ such that $u \in U$ whenever $d(f(x), u) < \eta$. We would like to find $\delta > 0$ s.t. $y \in f^{-1}(U)$ whenever $d(x, y) < \delta$. But $y \in f^{-1}(U)$ if and only if $f(y) \in U$. We know that $f(y) \in U$ whenever $d(f(x),\ f(y)) < \eta$. Since f is continuous, there exists $\theta > 0$ such that $d(f(x), f(y)) < \eta$ whenever $d(x, y) < \theta$. Therefore, setting $\delta = \theta$, we are done.

The Ganesalingam-Gowers Project: Reasoning

- “Our main priority when writing the program was that the steps it took should be ones that a human would naturally take. ... the program should not do silly things.“

- work on the natural mathematical statements

- rewriting definitions

- “peeling off“ existential quantifiers

- deleting “used up“ hypothesis

- ...

Andrei Paskevich' SAD (System of Automatic Deduction) Project

Theorem 1. *The set of prime numbers is infinite.*

Proof. Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. ran $p \subseteq \mathbb{N}^+$. $\prod_{i=1}^{r} p_i \in \mathbb{N}^+$. Take $n = \prod_{i=1}^{r} p_i + 1$. n is non-trivial. Take a prime divisor q of n .

Let us show that q is not an element of A. Assume the contrary. Take j such that ($1 \leqslant j \leqslant r$ and $q = p_j$). p_j divides $\prod_{i=1}^{r} p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.

Hence A is not the set of prime numbers. □

(Text-level) natural formalism

- There are texts in a controlled natural language that are acceptable (i.e., natural) ordinary mathematical proof texts
- those texts can be generated by “text grammars” involving automatic theorem provers to fill in proof steps
- such systems define a *controlled natural proof language for mathematics*
- texts should be mathematically natural and expressive
- computer implementations provide proof checking and proof assistant tools

Further aspects of computer-fortified natural formalism

- formalism could become practically applicable in mathematics
- are there impacts on debates between formalism, naturalism, platonism, ...
- ...

Jody Azzouni: The derivation-indicator view of mathematical practice

ABSTRACT. A version of Formalism is vindicated: Ordinary mathematical proofs indicate (one or another) mechanically checkable derivation of theorems from the assumptions those ordinary mathematical proofs presuppose. The indicator view explains why mathematicians agree so readily on results established by proofs in ordinary language that are (palpably) not mechanically checkable. Mechanically checkable derivations in this way structure ordinary mathematical practice without its being the case that ordinary mathematical proofs can be 'reduced to' such derivations. In this way, one threat to formalist-style positions is removed: Platonic objects aren't needed to explain how mathematicians understand the import of ordinary mathematical proofs.– (Philosophia Mathematica, 2004)

Derivation-indication

N. Bourbaki:

If formalized mathematics were as simple as the game of chess, ...

... there would remain only the task of writing out our proofs in this language, ...

Derivation-indication

Saunders Mac Lane:

As to precision, we have now stated an absolute standard of rigor: A mathematical proof is rigorous when it is (or could be) written out in the first-order predicate language $L(\in)$ as a sequence of inferences from the axioms ZFC, each inference made according to one of the stated rules. [...] When a proof is in doubt, its repair is usually a partial approximation to the fully formal version.

Derivation-indication

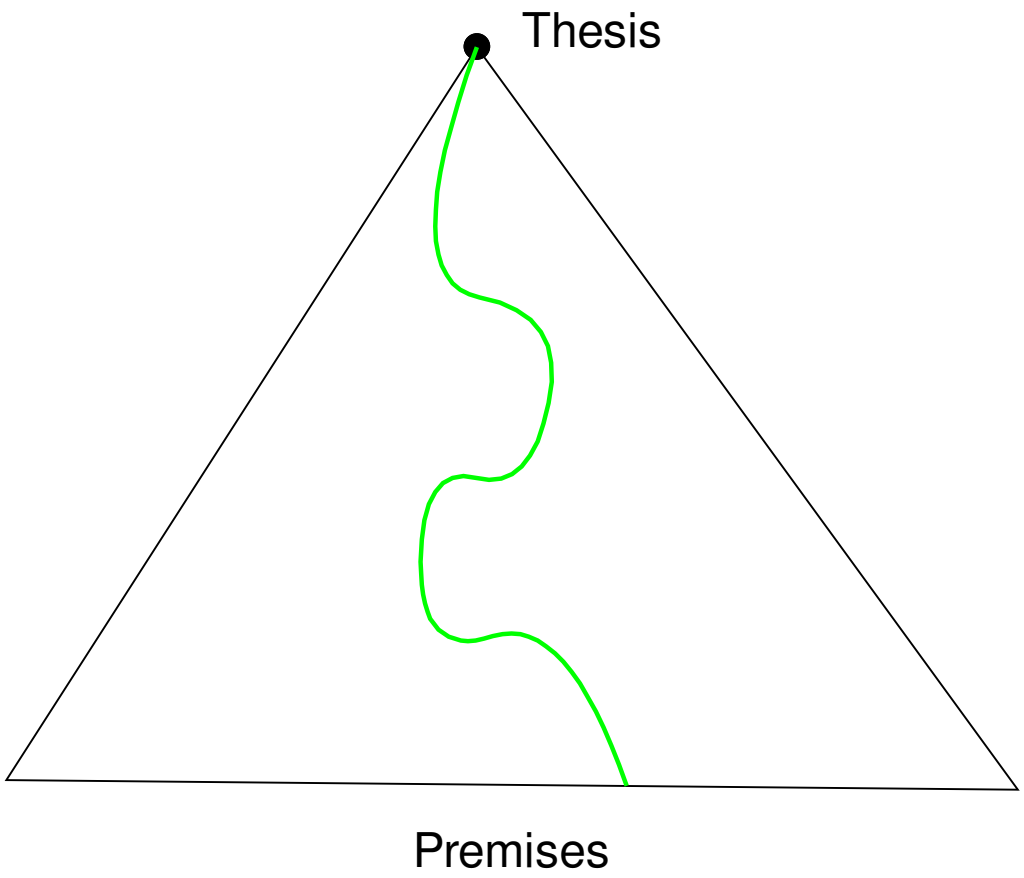
- Mathematicians agree that proofs can be written out in increasingly formal detail

- Do the indicators lie mainly in natural language parts of proofs?

- Can one identify indicators by natural language processing?

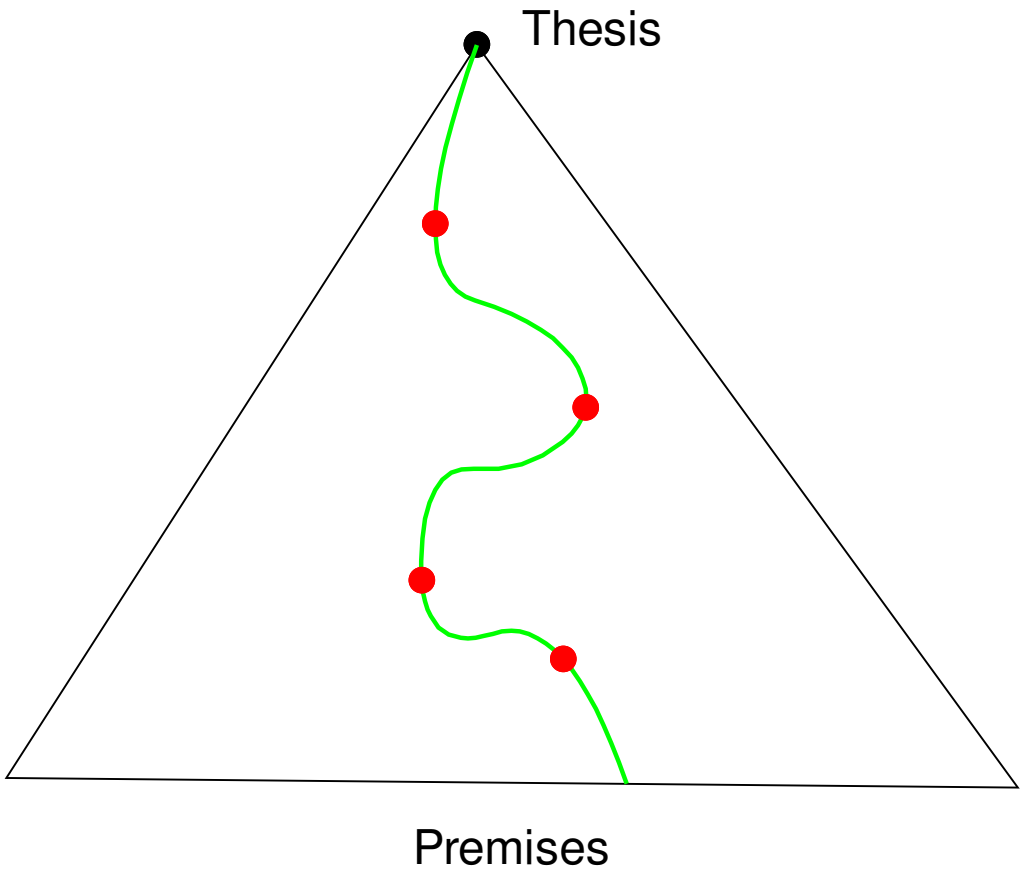
- Does natural language proof checking provide an implementation of the derivation-indicator view?

Complexity of Derivation Search in Large Search Space

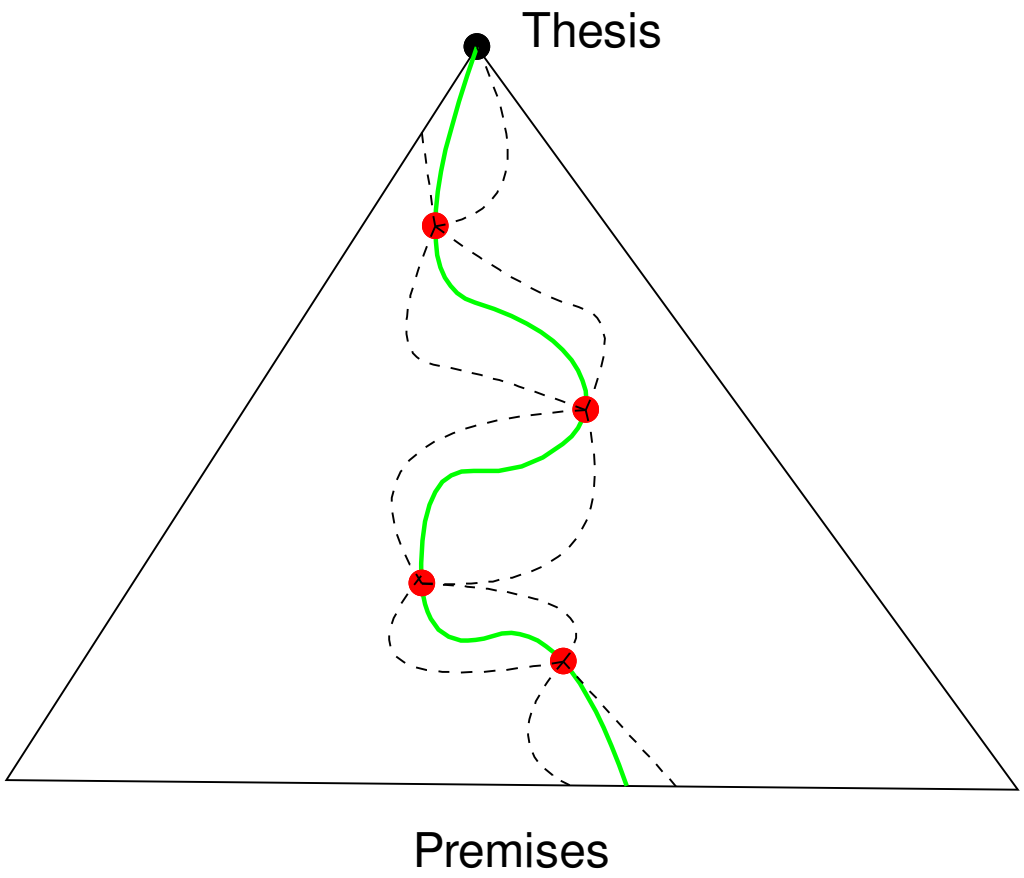


Complexity of Derivation Search

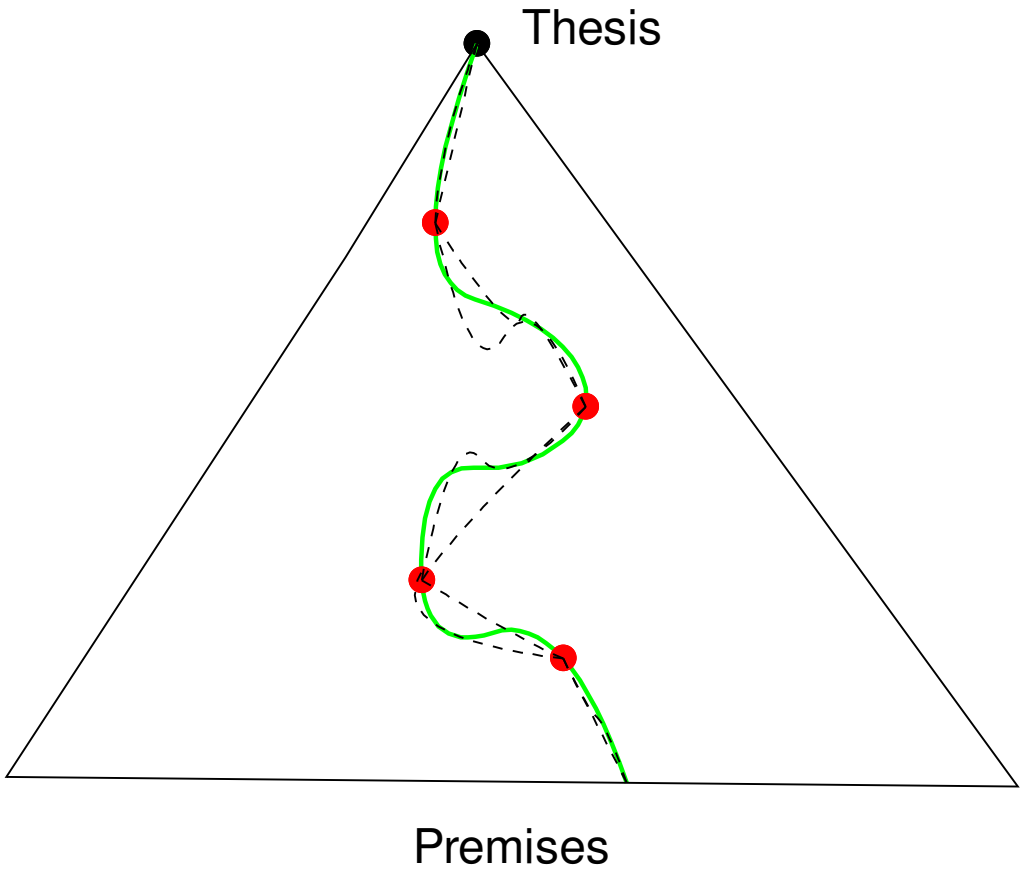
Derivation-indication can reduce the search space:



Complexity of Derivation Search



Can One Radically Prune the Local Searches by Reasoning?



Outlook

- Combine best practices from various formal mathematics systems to obtain naturalness and power
- will this achieve acceptance by mathematical practioneers?
- Jeremy Avigad: *On a personal note, I am entirely convinced that formal verification of mathematics will eventually become commonplace.*
- What would be the implications of a widespread use of formal mathematics for the methodology, practice, and philosophy of mathematics?

Thank You!