Computing proofs

Gilles Dowek

I. A bad start

Two problems in mathematics

Is it the case that

$$19 \times 29 = 464$$

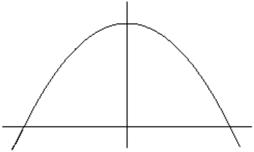
?

Is it the case that

$$\forall n \forall p \; n^2 \neq 2 \times p^2$$

?

Replace deduction with computation



Is the surface below the parabola $4/3$?
Archimedes: a long deduction (cutting the surface into an infinite number of triangles)

After the invention of calculus

$$\int_{-1}^{1} (1 - x^2)\, dx = [x - x^3/3]_{-1}^{1} = 4/3$$

Hilbert's program

Why restricting to the parabola?

Find an algorithm that takes a proposition as an argument and returns a proof (deduction) of it or tells there is none

Church and Turing (1936)

There is no such algorithm

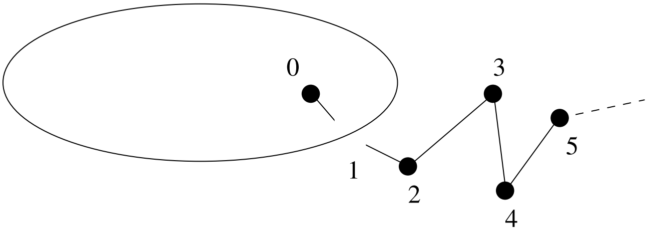
Deduction and computation are two completely different things

Deduction is stronger

Computation should be relegated to a minor heuristic concept (as it has always been)

(Fortunately) mathematicians are not engineers

II. From constructvity to cut elimination



Does there exist a number x such that $x \in E$ and $x + 1 \notin E$?

Existence with no witness

We can prove theorems of the form $\exists x \; A(x)$

without knowing a t such that we can prove $A(t)$

Proving a proposition of the form $\exists x\ A$

Just one possibility
prove $A(t)$ the deduce $\exists x\ A$ ($\exists$-intro)

For example: $2 \in \text{Even}$ hence $\exists x\ (x \in \text{Even})$

How can such a witness get lost?

Proving a proposition of the form $\exists x\ A$

If $1 \in E$ then $(1 \in E$ and $1 + 1 \notin E)$ thus
$\exists n\ (n \in E$ and $n + 1 \notin E)$
so far so good, the witness is 1

Proving a proposition of the form $\exists x\ A$

If $1 \in E$ then $(1 \in E$ and $1 + 1 \notin E)$ thus
$\exists n\ (n \in E$ and $n + 1 \notin E)$
so far so good, the witness is 1
If $1 \notin E$ then $(0 \in E$ and $0 + 1 \notin E)$ thus
$\exists n\ (n \in E$ and $n + 1 \notin E)$
here also everything is fine, the witness is 0

Then...

a proof by case

From (A or B), $A \Rightarrow C$, $B \Rightarrow C$ deduce C

Here we have proved
$1 \in E \Rightarrow \exists n\ (n \in E \text{ and } n+1 \notin E)$
$1 \notin E \Rightarrow \exists n\ (n \in E \text{ and } n+1 \notin E)$

Then...

a proof by case

From (A or B), $A \Rightarrow C$, $B \Rightarrow C$ deduce C

Here we have proved
$1 \in E \Rightarrow \exists n\ (n \in E \text{ and } n+1 \notin E)$
$1 \notin E \Rightarrow \exists n\ (n \in E \text{ and } n+1 \notin E)$
We can deduce $\exists n\ (n \in E \text{ and } n+1 \notin E)$
... here we start loosing the witness: 0 or 1?

Then...

a proof by case

From (A or B), $A \Rightarrow C$, $B \Rightarrow C$ deduce C

Here we have proved
$1 \in E \Rightarrow \exists n \ (n \in E \text{ and } n+1 \notin E)$
$1 \notin E \Rightarrow \exists n \ (n \in E \text{ and } n+1 \notin E)$
We can deduce $\exists n \ (n \in E \text{ and } n+1 \notin E)$
But we still need to prove ($1 \in E$ or $1 \notin E$)

The excluded middle

We can always prove "A or not A" without having to do anything

In particular neither proving A nor proving not A

For example

$\exists n \; ((n = 0 \text{ and } G) \text{ or } (n = 1 \text{ and not } G))$

A witness?

Constructive proofs

Definition: a proof that does not use the excluded middle

Theorem (Gentzen 1934):
If $\exists x\ A$ has a constructive proof, then a witness exists

An algorithm to extract the witness from the proof

Detours in proofs

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma \vdash A} \qquad \dfrac{\pi_2}{\Gamma \vdash B}}{\Gamma \vdash A \text{ and } B}\,\text{and-intro}}{\Gamma \vdash A}\,\text{and-elim}$$

A cut: an introduction rule followed by an elimination rule
A simpler proof of $\Gamma \vdash A$?

More examples

$$\dfrac{\dfrac{\dfrac{\pi}{\Gamma \vdash A}}{\Gamma \vdash \forall x\ A}\ \forall\text{-intro}}{\Gamma \vdash (t/x)A}\ \forall\text{-elim}$$

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B}\ \Rightarrow\text{-intro} \qquad \dfrac{\pi_2}{\Gamma \vdash A}}{\Gamma \vdash B}\ \Rightarrow\text{-elim}$$

The cut elimination algorithm

always terminates and yields a cut free proof

A proof that is (1.) constructive, (2.) cut-free and (3.) with no axiom always end with an introduction rule

$$\frac{\vdash A(t)}{\vdash \exists x\ A(x)}\ \exists\text{-intro}$$

Why do we care about computing witnesses?

Prove

$$\forall x \; \exists y \; (x = 2 \times y \text{ or } x = 2 \times y + 1)$$

Deduce

$$\exists y \; (25 = 2 \times y \text{ or } 25 = 2 \times y + 1)$$

Extract the witness

?

Why do we care about computing witnesses?

The (constructive) proof of

$$\forall x \; \exists y \; (x = 2 \times y \text{ or } x = 2 \times y + 1)$$

is a program computing the half of a number
It expresses an algorithm

Cut elimination: execution process of this programming language

- Programs always terminate
- and are always correct with respect to their specification, for example $x = 2 \times y$ or $x = 2 \times y + 1$

There is no algorithm that decides if a proposition has a proof or not (Church, Turing)

But proofs are algorithms

Proofs are algorithms

What is a proof of $A \Rightarrow B$?

Brouwer-Heyting-Komogorov interpretation
Curry-de Bruijn-Howard correspondence

But how can we prove

$$\forall x \ \exists y \ (x = 2 \times y \text{ or } x = 2 \times y + 1)$$

?

III. Cut elimination for axiomatic theories

Axiomatic theories

Proofs are built with deduction rules, for example

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \text{ and } B} \text{ and-intro}$$

$$\frac{}{\Gamma, A \vdash A} \text{ axiom}$$

that define the meaning of the logical symbols: "and", "or", "$\Rightarrow$", "$\forall$", "$\exists$"
The meaning of "point", "line", "parallel", "number", "even", "set", $\in$ not defined by the deduction rules, but by the axioms (theory)

A constructive cut free proof of $\emptyset \vdash A$ ends with introduction rule
What about cut free proofs of $\Gamma \vdash A$?

Need not end with an introduction rule: no witness property

Computation rules vs. axioms: the case of arithmetic

$$\forall y\ (0 + y = y)$$

$$\forall x \forall y\ (S(x) + y = S(x + y))$$

Prove $S(S(0)) + S(S(0)) = S(S(S(S(0))))$

But do we need such axioms?

$2+2$ should compute to 4 not be provably equal to 4

Instead of axioms: computation rules

$$0 + y \longrightarrow y$$

$$S(x) + y \longrightarrow S(x + y)$$

Prove $S(S(0)) + S(S(0)) = S(S(S(S(0))))$

A trickier axiom

$$\forall x \forall y \ (S(x) = S(y) \Rightarrow x = y)$$

$$\mathrm{Pred}(0) \longrightarrow 0$$

$$\mathrm{Pred}(S(x)) \longrightarrow x$$

An even trickier one: induction (but possible)

Deduction rules

Replace the rule

$$\frac{\Gamma \vdash (x/t)A}{\Gamma \vdash \exists x \; A} \; \exists\text{-intro}$$

with

$$\frac{\Gamma \vdash B}{\Gamma \vdash \exists x \; A} \; \exists\text{-intro if } B \equiv (t/x)A$$

where the relation $\equiv$ is defined by the computation rules

Example: prove $\exists x \; (2 \times x = 6)$

A completely new situation

- No axioms, but computation rules
- (1.) constructive, (2.) cut-free and (3.) with no axiom proofs always end with an introduction rule
- But proof reduction does not terminate all theories
  $P \longrightarrow (P \Rightarrow \bot)$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{P \vdash P \Rightarrow \bot}\,\text{axiom}
\qquad
\dfrac{}{P \vdash P}\,\text{axiom}
}{P \vdash \bot}\,\Rightarrow\text{-elim}
}{\vdash P \Rightarrow \bot}\,\Rightarrow\text{-intro}
\qquad
\dfrac{
\dfrac{
\dfrac{}{P \vdash P \Rightarrow \bot}\,\text{axiom}
\qquad
\dfrac{}{P \vdash P}\,\text{axiom}
}{P \vdash \bot}\,\Rightarrow\text{-elim}
}{\vdash P}\,\Rightarrow\text{-intro}
}{\vdash \bot}\,\Rightarrow\text{-elim}
$$

How far can we go?

Can all theories be expressed with computation rules only?

Of course not: inconsistent theories, theories that do not have the witness property...

But are these theories good?

Axioms: anything goes, computation rules: more restrictive
But properties in return: consistency, witness...

Proofs and algorithms

Not only proofs are algorithms

But also proofs are expressed in theories that are algorithms

An idea that has many origins

- Proof theory: Prawitz, Crabbé, Hallnäs, Ekman, Plato, Negri...
- Higher-order substitution: Russell, Whitehead, Church, Henkin, Prawitz...
- Automated theorem proving: Plotkin, Andrews, Huet, Boyer-Moore...
- Type theory: Martin-Löf, Coquand, Huet...