Proofs and Types
Introduction

Bow-Yaw Wang

Academia Sinica

Spring 2012

What is Mathematics?

- Consider the following equality

$$27 \times 37 = 999.$$

- Clearly, "27×37" is not "999."
  - Both sides have different *senses*. They are not equal.
- On the other hand, the number obtained by computing "27×37" is indeed "999."
  - Both sides have the same *denotation*. They are equal.
- Given a sentence A, there are two ways of viewing it (by Frege):
  - as a sequence of instructtions, which determine its sense.
    - ★ $A \vee B$ means "A or B."
  - as the ideal result found by the instructions. This is denotation.
    - ★ False (**f**) or True (**t**).

Sense and Denotation

- The dichotomy of sense and denotation gives the following association:
  - sense, syntax, proofs;
  - denotation, truth, semantics, algebraic operations.
- Denotation has been fruitful in mathematical logic.
  - for example, model theory.
- Sense unfortunately has not reached its rival (until, I think, the influence from computer science).
  - for example, interactive theorem proving.

Tarski Semantics

- In Tarski semantics, we are only interested in the denotation.
- For atomic sentences, we assume the denotation is known.
  - $27 \times 37 = 999$ is **t**;
  - $3 \times 13 = 37$ is **f**.
- The denotation of composed sentences are obtained by the truth table:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$\neg A$
f	**f**	**f**	**f**	**t**	**t**
f	**t**	**f**	**t**	**t**	**t**
t	**f**	**f**	**t**	**f**	**f**
t	**t**	**t**	**t**	**t**	**f**

- The denotation of $\forall\xi.A$ is **t** if for every a in the domain of interpretation, $A[a/\xi]$ is **t**. Similarly, $\exists\xi.A$ is **t** if $A[a/\xi]$ is **t** for some a.

Heyting Semantics

- In Heyting semantics, we are interested in witnesses to truth.
- Instead of asking "when is A true?", we ask "what is the proof of A?"
- For atomic sentences, the proofs are intrinsic. For example, the proof of $27 \times 37 = 999$ is by calculation.
- A proof of $A \wedge B$ is a pair (p, q) where p and q are proofs of A and B respectively.
- A proof of $A \vee B$ is a pair (i, p) with
  - $i = 0$, and p is a proof of A;
  - $i = 1$, and p is a proof of B.
- A proof of $A \Rightarrow B$ is a function f that maps each proof p of A to the proof $f(p)$ of B.
- $\neg A$ is treated as $A \Rightarrow \bot$ where $\bot$ is a sentence without proof.
- A proof of $\forall \xi.A$ is a function f that maps each point a in the domain of definition to a proof $f(a)$ of $A[a/\xi]$.
- A proof of $\exists \xi.A$ is a pair (a, p) where a is in the domain of definition and p is a proof of $A[a/\xi]$.

Intuitionistic Logic

- Consider the sentence $A \vee \neg A$.
- In classical logic, $A \vee \neg A$ is **t**.
  - It follows from denotation (or Tarski's semantics).
- But this is not clear from a witness's point of view.
  - Do you mean you always have either a proof of A or a proof of $\neg A$?
  - If so, give me a proof of $P = NP$ or $P \neq NP$.
- Brouwer's intuitionistic logic does not accept $A \vee \neg A$ as an axiom.
  - It coincides with Heyting's semantics.
- Intuitionistic logic is influential in constructive mathematics.

Interactive Theorem Proving

- The interactive theorem prover COQ is based on intuitionistic logic.
- The theory of COQ is initially developed by Thierry Coquand and Gérard Heut.
- The tool COQ has been developed for over 20 years.
- In 2004, the proof of four color theorem is formalized in COQ.
- COQ is used in CompCert.
  - The project CompCert builds formally verified optimizing compiler for a subset of C programming language.