# The Origin of Proof Theory and its Evolution

## Lecturer: Bill Tait

### Introduction

Proof theory is the study of mathematics and mathematical reasoning in a general and abstract sense itself. It examines the mathematical theories as such, especially with respect to their logical structure. It concentrates mainly on the way in which theorems are derived from axioms.

### ε-calculus

Hilbert's ε-calculus is based on an extension of the language of predicate logic by a term-forming operator $\varepsilon_x$. This operator is governed by the critical axiom

$$A(t) \supset A(\varepsilon_x A(x)), \text{ where } t \text{ is an arbitrary term.}$$

Within the ε-calculus quantifiers become definable by

$$xA(x) \Leftrightarrow A(\varepsilon_x A(x)) \text{ and } \forall x\, A(x) \Leftrightarrow A(\varepsilon_x \neg A(x))$$

The expression $\varepsilon_x A(x)$ is called ε -term.

### Substitution Method

- *Natural Deduction*: is used to prove that some reasoning is correct, or to check the validity of a sequent, but not the invalidity;
- *Sequent Calculus*: a technical device for proving consistency of predicate logic in natural deduction;
- *Cut Elimination*: states that every sequent calculus derivation can be transformed into another derivation with the same end sequent and in which the cut rule does not occur.

### Transfinite ordinals Theory

For example:

- Consider the totality of the numbers 1, 2, 3, 4 … itself as a completed entity
- Regard the points of a line segment as a totality of objects, e.g. [0, 1]

This kind of infinite is called the *actual infinite*, compared to *potential infinite*.

Moreover, if we denote the type of this ordering by ω, then the denumeration continues in a natural way as:

$1, 2, 3, \ldots, \omega$

$\omega, \omega + 1, \omega + 2, \ldots, \omega + \omega$

$\omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \ldots, \omega \cdot \omega$

$\omega^2, \omega^3, \omega^4, \ldots, \omega^\omega$

$\omega^\omega, \ldots$

These are first transfinite numbers, the numbers of the second number class. By means of transfinite counting, one could enumerate the elements of sets that are not denumerable in the ordinary sense.

## First-Order Number Theory - PA (Peano Arithmetic)

First-order logic has sufficient expressive power for the formalization of virtually all of mathematics. A first-order theory consists of a set of axioms (usually finite or recursively enumerable) and the statements deducible from them.

Peano arithmetic is a first-order theory commonly formalized independently in first-order logic. It constitutes a fundamental formalism for arithmetic, and the Peano axioms can be used to construct many of the most important number systems and structures of modern mathematics.

**Function Constants & Relation Constants**
A function is a set of lists in which the items in every list except for the last determine the last item, i.e. there cannot be two lists that agree on all but the last item and disagree on the last item.
A relation is an arbitrary set of lists. A collection of objects satisfies a relation if and only if the list of those objects is a member of this set.

Logical connectives are $\{\vee, \wedge\}$ for the propositional logic, and $\{\vee, \wedge, \exists, \forall\}$ for the predicate logic (and for the ε -logic).

**Axiom**

$$\Gamma, \neg A, A$$

For any sequent Γ and a *first order formula* A.

**Define Matrix - N-matrix:**
$f_A (C_1, C_2, C_3, \ldots, C_n) \in x \; A (C_1, C_2, C_3, \ldots, C_n, x)$

**Logical Axioms & non-logical Axioms**
Logical Axioms are certain formulas in a language that are universally valid, that is, formulas that are satisfied by every structure under every variable assignment function. Non-logical axioms are formulas that play the role of theory-specific assumptions. Reasoning about two different structures, for example the natural numbers and the integers, may involve the same logical axioms; the non-logical axioms aim to capture what is special about a particular structure.

**For each n-matrix A, of the axioms:**
$\exists x \, A (S_1, S_2, S_3, \ldots, S_n, x) := A (S_1, S_2, S_3, \ldots, S_n, f_A (S_1, S_2, S_3, \ldots, S_n))$

**Finite Deduction:**
$A (S_1, S_2, S_3, \ldots, S_n, t) \rightarrow A (S_1, S_2, S_3, \ldots, S_n, f_A (S_1, S_2, S_3, \ldots, S_n))$
$T = \max \{t_1, t_2, t_3, \ldots, t_k\}$

One of the most common ways of taking proofs as objects to be manipulated is to write proofs as tree diagrams.

## Prime Sequences of PA

Prime sequences: $\vee\{A, B\}$ and $\wedge\{A, B\}$
Components: $A\Phi$ and $B\Phi$

**Rules of Inference:**

| | | |
|---|---|---|
| Ax | $r, A$ | (A is a true prime sequence) |
| $\vee$ | $\frac{r, \vee\Phi, A}{r, \vee\Phi}$ | (For some $A \in \Phi$) |
| $\wedge$ | $\frac{\ldots\ r, \wedge\Phi, A\ \ldots}{r, \wedge\Phi}$ | (For all $A \in \Phi$) |
| CUT | $\frac{r, A \quad r, \overline{A}}{r}$ | |

**Deductions from PA:**

$r, \overline{A(0)}, \vee\{\overline{A(k)} \wedge A(k+1) \mid k < \omega\}, A(n)$