

- Does procedure P satisfy spec S ?
- Does specification S' ^{refine} spec S ?
- Does operation O preserve inv I ?
- Does system spec S have consequence C ?

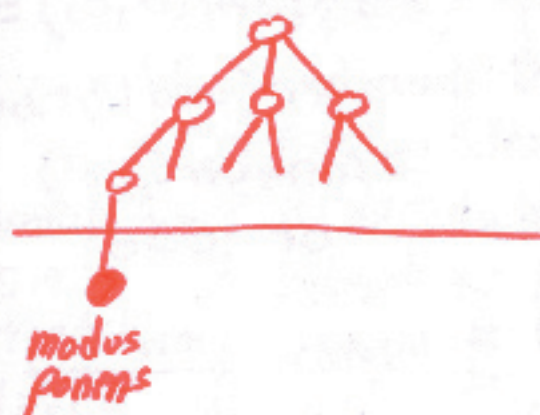
Natural Deduction

$$\frac{A, A \Rightarrow B}{B} \quad \frac{\neg B, A \Rightarrow B}{\neg A}$$

$$\frac{A \wedge B}{A, B} \quad \frac{A, B}{A \wedge B}$$

LF logical framework

Theorem as abstract Datatype



ex: HOL ^{prover} ~~proof~~
 PCL - proof carrying code
 TCB - trusted computing Base

Larch - algebraic, rewriting

stack: $\text{pop}(\text{push}(s, e)) = e$

set: $\text{member}(\text{add}(s, e), e') = \text{member}(s, e')$
 or $e = e'$

where $=$ means rewrite

Donald Knuth did rewriting

LP (Steve Garland) - larch prover

Sophistication:

tactics + decision procedures
 + heuristics

↓
 prove statements
 in decidable
 subset of logic

uninterp. fun.
 SAT
 arithmetic
 lists

ex: ^{BSch.} Simplify
 Boyer-Moore
 ACL2
 PVS Prototype verification system
 Complex, "grind", non-trusted

$a = b$
 $g(x, x) = x$
 $g(f(a), f(b)) = c$
 $f(a) = c$