Lecture 7
CS4860
September 9, 2016

• Hilbert style axiom system based on &, ∨, ⊃, and ∼.

• Kleene Postulates
  Group A1 - propositional calculus
  1. (a) \( A \supset (B \supset A) \)
     (b) \( (A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C)) \)
  2. \( A, A \supset B \)
     \[\begin{array}{c}
     B \\
     \end{array}\]
  3. \( A \supset (B \supset A \& B) \)
  4. (a) \( A \& B \supset A \)
     (b) \( A \& B \supset B \)
  5. (a) \( A \supset (A \lor B) \)
     (b) \( B \supset (A \lor B) \)
  6. \( (A \supset C) \supset ((B \supset C) \supset A \lor B \supset C) \)
  7. \( (A \supset B)((A \supset \sim B) \supset \sim A) \)
  8. \( \sim \sim A \supset A \)

Example Proof
  1. \( A \supset (A \supset A) \) Axiom scheme 1a.
  2. \( \{A \supset (A \supset A)\} \supset \{[(A \supset ((A \supset A) \supset A)) \supset [A \supset A]]\} \) Axiom scheme 1b.
  3. \( [A \supset ((A \supset A) \supset A)] \supset [A \supset A] \) Rules 2,1,2 (Rule 2 on lines 1,2)
  4. \( A \supset ((A \supset A) \supset A) \) Axiom Scheme 1a.
  5. \( A \supset A \) Rule 2,4,3

Which axioms are programmable?
Natural Deduction style proof

\[(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))\]

**Proof**

1. Assume \((A \supset B)\)
   
   Show \((A \supset (B \supset C)) \supset (A \supset C)\)

2. Assume \(A \supset (B \supset C)\)
   
   Show \((A \supset C)\)

3. Assume \(A\)
   
   Show \(C\)

4. \(B \supset C\) from 2,3 by Modus Ponens (i.e. \(\frac{X, X \supset Y}{\therefore Y}\))

5. \(B\) from 1,3

6. \(C\) from 5,4

Q.E.D

• On the next page you will find an example of natural deduction style applied in a “programming logic.”
DIVIDE: PROCEDURE (A, B, Q, R);
DCL (A, B) READONLY;
DCL (Q, R) FIXED;

// ASSUME A >= 0, B > 0;
ATTAIN A = B*R, Q, R < R < B; /*

R = A;
Q = 0;
A = B*R + R; /*
SOME I FIXED, (I >= 0 & R <= I) BY INTRO, R; */

DO WHILE (R-B >= 0);
// ASSUME A = B*R, R >= 0;
ARES I FIXED WHERE R <= I;
^R(R <= 0) BY ARITH, R-B >= 0, B > 0;
A = R*Q+1 + (R-B) BY ARITH, A = B*R+R;
R-B <= I-1 BY ARITH, R <= I, B > 0; /*
R = R-B;
Q = Q+1;

END;
// R < B BY ARITH, ^R(R >= 0), B = B; */
RETURN;

END DIVIDE;

NUMBER OF VCODE INSTRUCTIONS 81
LENGTH OF ASSERTIONS PROCESSED 774