CS 145 – Foundations of Computer Science

Professor Eric Aaron

Lecture – M W 10:30am
Lab – F 3:10pm

Lecture Meeting Location: SP 105
Lab Meeting Location: SP 309

Business

• HW4 out, extended due dates April 10 & 11
  – Programming due April 10, non-programming and printouts the 11th

• Reading: Makinson, Ch.4.1-4.6
  – Our coverage of the material will be different from that in the textbook, but it’s good to see the textbook’s presentation, as well

• Reading: Prof. Hunsberger’s document “The Natural Numbers, Induction, and Numeric Recursion”
  – Posted on the Additional Notes / Readings page of the CS145 website
More Addition

• If the Peano axioms define the natural numbers…
  – How could we define the addition function?
  – Hint: Recursively! Because our definition of the numbers is recursive…

• Definition of addition:
  1. Case z=0 -- For all n in \( \mathbb{N} \), \( n + 0 = n \)
  2. Case \( z = S(m) \) -- For all \( n \) in \( \mathbb{N} \), \( z = S(m) \) for some \( m \) in \( \mathbb{N} \):
     \[ n + S(m) = S(n + m) \]

• Let’s prove something with that definition!
  – Claim: This addition function is associative (i.e., \( a + (b + c) = (a + b) + c \), for all \( a, b, c \) in \( \mathbb{N} \))
  – Proof: ??

Recall: We proved that every natural number is either 0 or \( S(m) \) for some \( m \).

Proof: Associativity of Addition

• Definition of addition:
  1. Case z=0 -- For all \( n \) in \( \mathbb{N} \), \( n + 0 = n \)
  2. Case \( z = S(m) \) -- For all \( n \) in \( \mathbb{N} \), \( z = S(m) \) for some \( m \) in \( \mathbb{N} \):
     \[ n + S(m) = S(n + m) \]

• Let’s prove something with that definition—associativity!
  – To prove: For all \( a, b, c \) in \( \mathbb{N} \), \( a + (b + c) = (a + b) + c \)
  – Proof: Prove by induction on \( c \).
  – Let \( P(c) \) be the proposition: For all \( a, b \) in \( \mathbb{N} \), \( a + (b + c) = (a + b) + c \)
  – Base—\( c=0 \).
  – \( P(0) \) is the proposition: For all \( a, b \) in \( \mathbb{N} \), \( a + (b + 0) = (a + b) + 0 \)
  – To prove \( P(0) \): \( a + (b + 0) = (a + b) + 0 \)
    * Start with the left hand side: \( a + (b + 0) = a + b \), because \( (b + 0) = b \) (by equation 1 of the definition of addition, with \( b \) in place of \( n \)); then, \( a + b = (a + b) + 0 \), also by equation 1, with \( a + b \) in place of \( n \). Thus, \( a + (b + 0) = (a + b) + 0 \), completing the proof of the base case.
Proof: Associativity of Addition

• Definition of addition:
  1. Case z=0 -- For all n in N, n + 0 = n
  2. Case z=S(m) -- For all n in N, z = S(m) for some m in N: n + S(m) = S(n + m)

• Let’s prove something with that definition—associativity!
  – Inductive case—c=S(y) for some y in N. Then, assume P(y) and prove P(S(y)): For all a,b in N, a + (b + S(y)) = (a + b) + S(y).

    • Start with the left hand side: a + (b + S(y)) = a + S(b + y), by eqn 2 of the definition of addition, with b in place of n and y in place of m;
    • Then, a + S(b + y) = S(a + b + y), by eqn 2, with a in place of n and (b + y) in place of m;
    • Then, S(a + b + y) = S((a + b) + y), because a + b + y = (a + b) + y, by the inductive hypothesis; (Be sure to explicitly note where the I.H. is used!)
    • Then, S((a + b) + y) = (a + b) + S(y), by eqn 2 with (a + b) in place of n and y in place of m;
    • Thus, a + (b + S(y)) = (a + b) + S(y), completing the inductive case.

Proof: Associativity of Addition

• Definition of addition:
  1. Case z=0 -- For all n in N, n + 0 = n
  2. Case z=S(m) -- For all n in N, z = S(m) for some m in N: n + S(m) = S(n + m)

• Let’s prove something with that definition—associativity!
  – To prove: For all a,b,c in N, a + (b + c) = (a + b) + c
  – Proof: Prove by induction on c
  – Let P(c) be the proposition: For all a, b in N, a + (b + c) = (a + b) + c
  – Base—c=0. Prove P(0).
  – Inductive case—c=S(y) for some y. Prove P(S(y)).
  – Both cases are proved, on the previous slides. Therefore, the claim holds for all numbers c in N, by induction. (Specifically, by the Axiom of induction!)
Theorem: George

• Definition of addition:
  1. Case z=0 -- For all n in N, n + 0 = n
  2. Case z=S(m) -- For all n in N, z = S(m) for some m in N; n + S(m) = S(n + m)
• Theorem: George—x + 0 = 0 + x for all natural numbers x
• Proof: Let P(n) be the proposition n + 0 = 0 + n
  – To prove: P(n) holds for all numbers n in N. Proof by induction on n.
• Base case: P(0). To prove …
• Inductive case: Assume for (arbitrarily chosen) k that P(k) holds. Then, prove P(S(k)). To prove…

What is the Inductive Hypothesis, in this case?

Theorem: Crackie

• Definition of addition:
  1. Case z=0 -- For all n in N, n + 0 = n
  2. Case z=S(m) -- For all n in N, z = S(m) for some m in N; n + S(m) = S(n + m)
• Theorem: Crackie—x + S(y) = S(x) + y for all natural numbers x, y
• Proof: Let P(z) be the proposition x + S(z) = S(x) + z
  – To prove: P(z) holds for all numbers z in N. Proof by induction on z.
• Base case: P(0). To prove …
• Inductive case: Assume for arbitrarily chosen y that P(y) holds. Then, prove P(S(y)). To prove…
Multiplication

- Multiplication on the naturals can be defined recursively, similarly to addition on the naturals
- Definition of addition:
  1. Case z=0 -- For all n in N, n + 0 = n
  2. Case z=S(m) -- For all n in N, z = S(m) for some m in N: n + S(m) = S(n + m)

- Definition of multiplication:
  3. Base case: x * 0 = 0
  4. Inductive case: x * Sy = (x*y) + x

- Some notes about the phrasing of that definition
  - Abbreviations and condensed forms are used, but it really means what we would expect, based on the definition of addition
  - Sy is a shorthand for S(y)
  - Variables are implicitly universally quantified over the naturals. E.g., the base case is “For all x in N, x * 0 = 0”. (cf. definition of addition)