COMPSCI 250: Introduction to Computation

Lecture #19: Proving the Basic Facts of Arithmetic
David Mix Barrington and Ghazaleh Parvini
18 October 2023

Proving the Facts of Arithmetic

- The Semiring of the Naturals
- The Definitions of Addition and Multiplication
- A Warmup: $\forall x: 0 + x = x$
- Commutativity of Addition
- Associativity of Addition
- Commutativity of Multiplication
- Associativity and the Distributive Law

Example: Making Change

- Suppose I have \$5 and \$12 gift certificates, and I would like to be able to give someone a set of certificates for any integer number of dollars.
- I clearly can't do \$4 or \$11, but if the amount is large enough I should be able to do it. By trial and error (or more cleverly) you can show that \$43 is the last bad amount.

Example: Making Change

- Let $P(n)$ be the statement "\$n can be made with \$5's and \$12's".
- I'd like to prove $\forall n: (n \geq 44) \rightarrow P(n)$ by strong induction, starting with $P(44)$.
- It's easy to prove $\forall n: P(n) \rightarrow P(n+5)$, which helps with the strong inductive step, namely $\forall n: Q(n) \rightarrow P(n+1)$, where $Q(n)$ is the statement $\forall i:((i \geq 44) \wedge (i \leq n)) \rightarrow P(i)$.

Example: Making Change

- So let n be arbitrary and assume Q(n). If $n \geq 48$, Q(n) includes P(n-4), and I can prove P(n+1) from P(n-4). But there are the cases of P(45), P(46), P(47), and P(48) which I have to do separately. One way to think of this is that with an inductive step of $P(n) \rightarrow P(n+5)$, I need five base cases.
- If my sum proving P(n) had at least two \$12's, I could replace them with five \$5's and get the inductive step for an ordinary induction.

The Semiring of the Naturals

- The natural numbers form an algebraic structure called a **semiring**, obeying these axioms:

1. There are two binary operations called $+$ and $\times$.
2. Both operations are **commutative**.
3. Both operations are **associative**.
4. There is an **additive identity** called 0 and a **multiplicative identity** called 1.
5. Multiplication **distributes** over addition, so that $\forall u: \forall v: \forall w: u \times (v + w) = (u \times v) + (u \times w)$.

Details of the Semiring Axioms

- Commutativity means $\forall u{:}\forall v{:}\ (u + v) = (v + u)$ and $\forall u{:}\forall v{:}\ (u \times v) = (v \times u)$.
- Associativity means $\forall u{:}\forall v{:}\forall w{:}(u + (v + w)) = ((u + v) + w)$ and $\forall u{:}\forall v{:}\forall w{:}\ (u \times (v \times w)) = ((u \times v) \times w)$.
- Identity rules are $\forall u{:}\ (0 + u) = (u + 0) = u$, $\forall u{:}(1 \times u) = (u \times 1) = u$, and $\forall u{:}\ (0 \times u) = (u \times 0) = 0$.

Clicker Question #1

- Consider the maximum operator on naturals, $\max(x, y) = x$ if $x \geq y$, else y
  Which of the following statements is true?
  commutative: $\max(x,y) = \max(y,x)$
  associative: $\max(x,\max(y,z)) = \max(\max(x,y),z)$
- (a) max is commutative but not associative
- (b) max is both commutative and associative
- (c) max is associative but not commutative
- (d) max is neither commutative nor associative

Not the Answer

Clicker Answer #1

- Consider the maximum operator on naturals, $\max(x, y) = x$ if $x \geq y$, else y
  Which of the following statements is true?
  commutative: $\max(x,y) = \max(y,x)$
  associative: $\max(x,\max(y,z)) = \max(\max(x,y),z)$
- (a) max is commutative but not associative
- (b) max is both commutative and associative
- (c) max is associative but not commutative
- (d) max is neither commutative nor associative

Implication is Not Associative

- Non-Commutativity is obvious,
  but non-associativity less so:

(p	→	q)	→	r	(p	→	(q	→	r)
0	1	0	**0**	0	0	**1**	0	1	0
0	1	0	**1**	1	0	**1**	0	1	1
0	1	1	**0**	0	0	**1**	1	0	0
0	1	1	**1**	1	0	**1**	1	1	1
1	0	0	**1**	0	1	**1**	0	1	0
1	0	0	**1**	1	1	**1**	0	1	1
1	1	1	**0**	0	1	**0**	1	0	0
1	1	1	**1**	1	1	**1**	1	1	1

Definition of Addition

- We defined addition recursively using the successor operation (now called “S” here to save space).
- We defined x + 0 to be x, and defined x + Sy to be S(x + y).
- This definition turned into a recursive method that always terminates because the *number added*, the second argument, always gets smaller.

Definition of Multiplication

- We also defined multiplication recursively using the successor and addition operations.
- We defined $x \times 0$ to be 0, and defined $x \times Sy$ to be $(x \times y) + x$.
- Again there is a recursive method that always terminates because the second argument always gets smaller.

What We May Assume

- We *don't* want to assume any properties of the operations that we haven't proved, and only a few of the semiring properties are true "by definition".
- Our notation can accidentally make such assumptions -- when we write "$(x \times y) + x$" we really mean `plus(times(x, y), x)` using the pseudo-Java methods we have defined.

Top-Down and Bottom-Up

- We can prove the big properties either **top-down** or **bottom-up**.
- A top-down approach identifies subproperties that we need to prove as we attack the overall problem through divide-and-conquer.
- A bottom-up approach has us guess what subproperties might be useful to prove, just as we build up a library of methods in a Java class.

A Warmup: $\forall x: 0 + x = x$

- The property $\forall x: 0 + x = x$ does not appear in our definition, though $\forall x: x + 0 = x$ does.
- It would follow from commutativity of addition, but we don't have that yet.
- Let's prove it by ordinary induction on the (natural) variable x, letting P(x) be "$0 + x = x$".
- The base case P(0) says "$0 + 0 = 0$", and this *does* follow from the definition and so is true.

A Warmup: $\forall x: 0 + x = x$

- For the inductive case we assume "$0 + x = x$" and try to prove "$0 + Sx = Sx$".
- We evaluate $0 + Sx$ as $S(0 + x)$ by the definition, then use the IH to substitute "x" for "$0 + x$" and get that this is Sx.
- This finishes the inductive case and proves $\forall x: P(x)$.

Clicker Question #2

- Which of these pairs of pseudo-Java method calls *does* always return equal naturals?
- (a) plus(successor(x), successor(x)) and successor(plus(x, x))
- (b) plus(successor(0), successor(x)) and successor(plus(0, x))
- (c) successor(plus(0, successor(x))) and plus(successor(x), successor(0))
- (d) successor(successor(plus(x, x))) and plus(x, successor(x))

Not the Answer

Clicker Answer #2

- Which of these pairs of pseudo-Java method calls *does* always return equal naturals?
- (a) plus(successor(x), successor(x)) and successor(plus(x, x))   2x+2 vs. 2x+1
- (b) plus(successor(0), successor(x)) and successor(plus(0, x))   x+2 vs. x+1
- (c) successor(plus(0, successor(x))) and plus(successor(x), successor(0))   both x+2
- (d) successor(successor(plus(x, x))) and plus(x, successor(x)) 2x+2 vs. 2x+1

Commutativity of Addition

- How shall we prove $\forall x: \forall y: x + y = y + x$?
- The usual technique is to let one variable be arbitrary and use induction on the other. Since addition operates by recursion on the second argument, we'll let x be arbitrary and use induction on y, letting P(y) be "$x + y = y + x$".
- The base case P(0) is "$x + 0 = 0 + x$", and after our warmup we know that both of these are equal to x, so the base case is done.

Commutativity of Addition

- The inductive case assumes "$x + y = y + x$" and wants to prove "$x + Sy = Sy + x$".
- The definition tells us that $x + Sy = S(x + y)$, so we need to show that $Sy + x = S(y + x)$ or $y + Sx$.
- Then we can use the IH to replace $y + x$ by $x + y$.
- So we just need the **lemma** $\forall x: \forall y: Sy + x = S(y + x)$ or $y + Sx$.

Proving the Lemma

- For the lemma $\forall x: \forall y: Sy + x = y + Sx$, we'd prefer to let y be arbitrary and use induction on x (we can switch the two $\forall$ quantifiers).
- The P(x) for this induction is thus "$Sy + x = y + Sx$".
- The base case is "$Sy + 0 = y + S0$", which follows from the definition.
- For the inductive case, we compute $Sy + Sx$ as $S(Sy + x)$ which is $S(y + Sx)$ by the IH, which is $y + SSx$, the RHS of P(Sx).

Associativity of Addition

- To prove $\forall x: \forall y: \forall z: x + (y + z) = (x + y) + z$, we let x and y be arbitrary and use ordinary induction on z.
- The base case P(0) is "$x + (y + 0) = (x + y) + 0$", which follows by using the base case of the definition once on each side.
- So we assume P(z), which is "$x + (y + z) = (x + y) + z$", and try to prove P(Sz), which is "$x + (y + Sz) = (x + y) + Sz$".

Associativity of Addition

- Working with the LHS, $x + (y + Sz) = x + S(y + z) = S(x + (y + z))$, using the definition of addition each time.
- This is $S((x + y) + z)$ by the IH.
- Using the definition of addition one more time, $S((x + y) + z)$ is equal to $(x + y) + Sz$, which completes the inductive step and thus the proof.

Clicker Question #3

- Which of the following could define multiplication?
- (a) $\forall u\colon u \times 0 = 0; \forall u\colon \forall v\colon u \times Sv = (u \times v) + v$
- (b) $\forall u\colon u \times 0 = 0; \forall u\colon \forall v\colon u \times Sv = (u \times v) + u$
- (c) $\forall u\colon u \times 0 = 0; \forall u\colon \forall v\colon u \times Sv = S(u \times v)$
- (d) $\forall u\colon u \times 0 = 0; \forall u\colon \forall v\colon u \times Sv = Su \times v$

Not the Answer

Clicker Question #3

- Which of the following could define multiplication?
- (a) $\forall u: u \times 0 = 0; \forall u: \forall v: u \times Sv = (u \times v) + v$
- (b) $\forall u: u \times 0 = 0; \forall u: \forall v: u \times Sv = (u \times v) + u$
- (c) $\forall u: u \times 0 = 0; \forall u: \forall v: u \times Sv = S(u \times v)$
- (d) $\forall u: u \times 0 = 0; \forall u: \forall v: u \times Sv = Su \times v$

Notes on Associativity

- Note that we didn't need commutativity to prove associativity here, though with multiplication the order of our proofs will matter.
- Also note that *during this proof* we need to be sure not to *assume* associativity by our use of notation, by writing things like "$x + y + z$".
- Once we have associativity, we can omit parentheses in such cases as we have done.

Commutativity of Multiplication

- Now we want to prove $\forall u: \forall v: u \times v = v \times u$, and we will work bottom-up.
- Our first lemma is $\forall u: u \times 0 = 0 \times u$. We let u be arbitrary and note that $u \times 0 = 0$ by the definition. We need induction to prove $\forall u: 0 \times u = 0$.
- We let P(u) be "$0 \times u = 0$", note that P(0) follows from the definition, assume P(u), and prove P(Su) or "$0 \times Su = 0$" by applying the definition to $0 \times Su$ to get $(0 \times u) + 0$, which is $0 + 0$ by the IH and 0 by the definition of addition.

Commutativity of Multiplication

- Our second lemma is $\forall u: \forall v: Su \times v = (u \times v) + v$. We let u be arbitrary and use induction on v, so that P(v) is "$Su \times v = (u \times v) + v$".
- The base case P(0) is "$Su \times 0 = (u \times 0) + 0$" and is easy to verify. We assume $Su \times v = (u \times v) + v$ and try to prove "$Su \times Sv = (u \times Sv) + Sv$".

Commutativity of Multiplication

- Working the LHS, $Su \times Sv = (Su \times v) + Su$, which is $((u \times v) + v) + Su$ by the IH, and then $(u \times v) + (v + Su)$ by associativity of addition.
- This is $(u \times v) + (Su + v)$ by commutativity of addition, $(u \times v) + (u + Sv)$ by a lemma above, $((u \times v) + u) + Sv$ by associativity of addition again, and finally $(u \times Sv) + Sv$ by the definition of multiplication.

Finishing Commutativity of $\times$

- We want to prove $\forall u: \forall v: (u \times v) = (v \times u)$, so we let u be arbitrary and use induction on v. Our statement P(v) is "$(u \times v) = (v \times u)$".
- The base case P(0) is "$(u \times 0) = (0 \times u)$", and this is exactly the conclusion of our first lemma.
- For the inductive step, our IH is P(v) or "$(u \times v) = (v \times u)$".

Finishing Commutativity of $\times$

- We want to prove P(Sv), which is "(u $\times$ Sv) = (Sv $\times$ u)".
- The left-hand side is (u $\times$ v) + u by the definition of multiplication.
- The right-hand side is (v $\times$ u) + u by the second lemma, reversing the roles of u and v. (We use Specification on the result.)
- Our IH now tells us that this form of the LHS is equal to this form of the RHS, completing the inductive step and thus completing the proof.

Associativity and Distributivity

- As in the textbook, we'll start proving the associative law for multiplication, which is $\forall u: \forall v: \forall w: u \times (v \times w) = (u \times v) \times w$.
- We let u and v be arbitrary, and use induction on w with P(w) as "$u \times (v \times w) = (u \times v) \times w$". The base case P(0) is "$u \times (v \times 0) = (u \times v) \times 0$", which reduces to "$0 = 0$" by known rules.
- We assume P(w) and try to prove P(Sw) which is "$u \times (v \times Sw) = (u \times v) \times Sw$".

Associativity and Distributivity

- The LHS reduces to $u \times ((v \times w) + v)$ by the definition, which is $(u \times (v \times w)) + (u \times v)$ by *distributivity*, which unfortunately we haven't proved yet.
- If we had done distributivity first, we could finish by using the IH to get $((u \times v) \times w) + (u \times v)$, and then the definition of multiplication to get $(u \times v) \times Sw$, the desired right-hand side.
- This makes proving the Distributive Law a rather important exercise! (Problem 4.6.2)