CMPSCI 250: Introduction to Computation

Lecture #19: Proving the Basic Facts of Arithmetic
David Mix Barrington
7 March 2012

Proving the Basic 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

The Semiring of the Naturals

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

1. There are two binary operations called + and ×.

2. Both operations are **commutative**, so that $\forall x: \forall y: (x+y) = (y+x)$ and $\forall u: \forall v: (u \times v) = (v \times u)$.

3. Both operations are **associative**, so that $\forall x: \forall y: \forall z: x + (y + z) = (x + y) + z$ and $\forall u: \forall v: \forall w: u \times (v \times w) = (u \times v) \times w$.

4. There is an **additive identity** called 0, so that $x + 0 = 0 + x = x$, and a **multiplicative identity** called 1, so that $1 \times u = u \times 1 = u$. Also $0 \times u = u \times 0 = 0$.

5. Multiplication **distributes** over addition, so that $\forall u: \forall v: \forall w: u \times (v + w) = (u \times v) + (u \times w)$.

Definitions of Addition and Multiplication

- 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.

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

- 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 accidently make such assumptions -- when we write "(x × y) + x" we really mean `plus(times(x, y), x)` using our methods.

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

- 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.

- The property $\forall x: 0 + x = 0$ 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. 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 get that this is Sx. This finishes the inductive case and proves $\forall x: P(x)$.

Commutativity of Addition

- How shall we prove ∀x: ∀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.

- 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.

- For the lemma ∀x: ∀y: Sy + x = y + Sx, we'd prefer to let y be arbitrary and use induction on x (we can switch the two ∀ 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 ∀x: ∀y: ∀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”.

- 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.

- Note that we didn’t need commutativity to prove associativity here, though with multiplication the order of our proofs will matter. Also note that we need to be sure not to assume associativity in our notation by writing “x + y + z”.

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.

- 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 "$Su \times Sv = (u \times Sv) + Sv$". 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 Multiplication

- 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 "$(u \times v) = (v \times u)$". 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 $(v \times u) + u$ 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 the Distributive Law

- 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 “$u \times (v \times Sw) = (u \times v) \times Sw$”.

- 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!