Inductions and Strings

Mark Greenstreet, CpSc 421, Term 1, 2006/07

Lecture Outline

Mathematical background for the “Theory of Computing”

- Induction
- Strings
- An Example

Axioms for the Natural Numbers

Axiom 0: 0 is a natural number.

Axiom 1: if x is a natural number, so is $succ(x)$

Axiom 2: if x is a natural number, $succ(x) > x$.

Axiom 3: if x and y are natural numbers and $x > y$, then $succ(x) > y$.

Axiom 4: if x and y are natural numbers and $x > y$, then $x \neq y$.

We write $\mathbb{N}$ to denote the set of natural numbers.

[Outline I.A.1]

Operations on the Natural Numbers

- Addition:

$$\begin{aligned} x + 0 &= x, \\ x + succ(y) &= succ(x + y). \end{aligned}$$

- Multiplication:

$$\begin{aligned} x * 0 &= 0, \\ x * succ(y) &= (x * y) + x. \end{aligned}$$

[Outline I.A.2]

Two More Operations

- Division:

$$(x/y) = q \quad \Leftrightarrow \quad y * q = x.$$

- Exponentiation:

$$\begin{aligned} x^0 &= succ(0), \\ x^{succ(y)} &= (x^y) * x. \end{aligned}$$

[Outline I.A.2]

Abbreviations

- Decimal digits:

$$1 = succ(0), \quad 2 = succ(1), \quad 3 = succ(2), \quad 4 = succ(3),$$
$$5 = succ(4), \quad 6 = succ(5), \quad 7 = succ(6), \quad 8 = succ(7),$$
$$9 = succ(8), \quad 10 = succ(9).$$

- Multidigit numbers:

$$1437 = 1*10^3 + 4*10^2 + 3*10^1 + 7*10^0$$
$$= \underbrace{succ(succ(succ(\ldots(succ(}_{1437\text{ ``succ('' s}}0\underbrace{))\ldots)))}_{1437\text{)s}}$$

0 is the primitive element for the naturals.

[Outline I.A.3]

Lazy Proofs

To prove: For all natural numbers, n, $\sum_{k=0}^{n} k = \frac{k^2 + k}{2}$.

Strategy:

- Wait for you to propose a particular m.
- Ask you to prove that m is a natural number. You'll have to me you that
$$m = succ(succ(succ(\ldots succ(0)\ldots))).$$
- I'll Prove that the formula holds for $m = 0$.
- For each $succ$ in the formula for m, I'll show that the formula for the sum holds.

[Outline I.B]

Visualize Laziness

If you show me:

m = succ(
succ(
succ(
⋮ ⋮
succ(
succ(
succ(
0)))...)))

then, I'll show you:

proof for m = succ(succ(succ(... succ(succ(succ(0)))...)))
proof for m = succ(succ(... succ(succ(succ(0)))...))
proof for m = succ(... succ(succ(succ(0)))...)
⋮
proof for m = succ(succ(succ(0)))
proof for m = succ(succ(0))
proof for m = succ(0)
proof for m = 0

[Outline I.B]

Proof for $m = 0$

- $\sum_{k=0}^{0} k = 0$.
- $$\begin{aligned}\frac{0^2+0}{2} &= \frac{0^2}{2}, && \text{def. } + \\ &= \frac{0^{succ(succ(0))}}{2}, && \text{def. 2} \\ &= \frac{(0*0)*0}{2}, && \text{def. exponentiation} \\ &= \frac{0}{2}, && \text{def. multiplication} \\ &= 0, && 2*0=0\text{, def. division}\end{aligned}$$
- $\square$

[Outline I.B]

Proof for $succ(m)$

$$
\begin{array}{rll}
& \frac{succ(x)^2 + succ(x)}{2} & \\
= & \frac{(x+1)^2+(x+1)}{2}, & x+1 = succ(x) \\
= & \frac{(x^2+2*x+1)+(x+1)}{2}, & \text{algebra} \\
= & \frac{(x^2+x)+2*(x+1)}{2}, & \text{more algebra} \\
= & \frac{x^2+x}{2} + \frac{2*(x+1)}{2}, & \text{more algebra} \\
= & \frac{x^2+x}{2} + (x+1), \text{ def. division} & \\
= & \left(\sum_{k=0}^{x} k\right) + (x+1), & \text{already shown: } \sum_{k=0}^{x} k \ = \ \frac{k^2+k}{2} \\
= & \sum_{k=0}^{succ(x)} k, & \text{def. summation}
\end{array}
$$

[Outline I.B]

Inductive Definitions

- Induction applies when the domain of interest is defined inductively.
- An inductive definition consists of a collection cases:
  - Primitive elements. We can write these cases as:

    $$s_0 \quad \in \quad S$$

    For example, $0 \in \mathbb{N}$.
  - Inductive cases that build larger elements from smaller ones. We can write:

    $$\forall s_1, s_2, \ldots s_k \in S.\ C(s_1, s_2, \ldots s_k) \in S$$

    For example, $\forall x \in \mathbb{N}.\ succ(x) \in \mathbb{N}$.

[Outline I.C]

Proof By Induction

If S is a set that is defined inductively, and $P : S \rightarrow \{0, 1\}$ is a predicate over elements of S, then we can prove that P holds for all elements of S by showing

- For each primitive element, s_0, of S show that $P(s_0)$ is true.
- For each inductive case, show that for any non-primitive element of s, you can find $s_1, s_2, \ldots s_k$ such that $s = C(s_1, s_2, \ldots s_k)$, and that

$$(P(s_1) \wedge P(s_2) \wedge \ldots \wedge P(s_k)) \Rightarrow P(s)$$

[Outline I.C]

Strong Induction

- Let $\mathcal{S}$ be the set such that $x \in \mathcal{S}$ iff
  - $x = 0$, or
  - $x = 1$, or
  - there are y and z in $\mathcal{S}$ such that $x = y + z$.

  It is straightforward to show that $S = \mathbb{N}$, the natural numbers as defined on slide 3.
- Proof by strong induction.
  To prove that $P(n)$ holds for all natural number, n, show:
  - $P(0)$, and
  - $P(1)$, and
  - for any natural number $x > 1$, we can find natural numbers $y < x$ and $z < x$ such that $x = y + z$, and $(P(y) \wedge P(z)) \implies P(x)$.
- There are many more ways we could generate the integers, and each leads to its own template for induction proofs.

Strings

Let Σ be a finite set of “symbols”.

- Informal definition: a string is a sequence of zero or more elements from Σ.
- Inductive definition: $s \in \Sigma^*$ iff
  - $s = \epsilon$, the empty string.
  - There is a $w \in \Sigma^*$ and a $c \in \Sigma$ such that $s = w \cdot c$.
- Note: The operator $\cdot$ represents concatenation, and we often omit writing it, just like skipping the $*$ for multiplication.

[Outline Section II.A]

Operations on Strings:

- String concatenation:

$$\begin{aligned} x \cdot \epsilon &= x \\ x \cdot (y \cdot c) &= (x \cdot y) \cdot c \end{aligned}$$

- Length:

$$\begin{aligned} length(\epsilon) &= 0 \\ length(w \cdot c) &= length(w) + 1 \end{aligned}$$

- Equality:

$$\begin{aligned} x = y \quad \leftrightarrow & \quad (x = \epsilon) \wedge (y = \epsilon) \\ \vee & \quad (x = u \cdot c) \wedge (y = v \cdot d) \wedge (u = v) \wedge (c = d) \end{aligned}$$

[Outline Section II.B]

One More Operation:

- Ordering:

$$
\begin{aligned}
x = y \quad \leftrightarrow \quad & \qquad length(x) < length(y) \\
& \vee \quad (length(x) = length(y)) \wedge (x = c \cdot u) \wedge (y = d \cdot v) \wedge (\\
& \vee \quad (length(x) = length(y)) \wedge (x = c \cdot u) \wedge (y = c \cdot v) \wedge (
\end{aligned}
$$

Note that “zebra” $<$ “aardvark” by this ordering.

[Outline Section II.B]

Putting it All Together

- Let $\Sigma = \{0, 1\}$.
- Let $S \subseteq \Sigma^*$, such that w is in S iff
  - $w = \epsilon$; or
  - There is a string x in S such that $w = 0x1$ or $w = 1x0$; or
  - There are strings x and y in S such that $w = xy$.
- Prove that w is in S iff the number of O's in w is equal to the number of 1's.
- We'll work this out on the whiteboard.

[Outline section III]