Manuel Kauers
RISC-Linz

Hagenberg, January 29, 2003

Formal Specification of Abstract Datatypes
Exercise 2: Initial Specifications

Consider the classical algebra of integers containing the operators Zero, Succ, Pred, Plus, Minus, Mult, and Leq.

1. Design an initial specification for the abstract data type "integer."

initial spec sp

sorts: $bool, int$

operators:

$True\colon \ \to bool$
$False\colon \ \to bool$
$And\colon bool \times bool \to bool$
$Impl\colon bool \times bool \to bool$
$Succ\colon int \to int$
$Pred\colon int \to int$
$Zero\colon \ \to int$
$Plus\colon int \times int \to int$
$Minus\colon int \times int \to int$
$Mult\colon int \times int \to int$
$Leq\colon int \times int \to bool$

generated sorts: $bool, int$

variables: a, b, m, n, k

eqns:

$True \neq False$
$And(a, True) = a$
$And(a, False) = False$
$Impl(False, a) = True$
$Impl(True, a) = a$
$Succ(Pred(n)) = n$
$Pred(Succ(n)) = n$
$Plus(m, Succ(n)) = Succ(Plus(m, n))$
$Plus(m, Pred(n)) = Pred(Plus(m, n))$
$Plus(m, Zero) = m$
$Minus(m, Succ(n)) = Pred(Minus(m, n))$
$Minus(m, Pred(n)) = Succ(Minus(m, n))$
$Minus(m, Zero) = m$
$Mult(m, Succ(n)) = Plus(Mult(m, n), m)$
$Mult(m, Pred(n)) = Minus(Mult(m, n), m)$
$Mult(m, Zero) = Zero$
$Leq(Zero, Zero) = True$
$Leq(Zero, Succ(Zero)) = True$
$Leq(Zero, Pred(Zero)) = False$
$Impl(And(Leq(m, n), Leq(n, k)), Leq(m, k)) = True$
$Leq(m, n) = Leq(Succ(m), Succ(n))$

end spec.

2. Show that this specification is adequate using the proof technique of characteristic term algebras.

First we extend the abbreviating notation $\mathit{Succ}^n(\mathit{Zero})$ also to negative n. In particular, we mean

$$\mathit{Succ}^n(\mathit{Zero}) = \begin{cases} \mathit{Zero} & \text{if } n = 0 \\ \mathit{Succ}(\mathit{Succ}^{n-1}(\mathit{Zero})) & \text{if } n > 0 \\ \mathit{Pred}(\mathit{Succ}^{n+1}(\mathit{Zero})) & \text{if } n < 0 \end{cases}$$

For instance, $\mathit{Succ}^{-2}(\mathit{Zero}) = \mathit{Pred}(\mathit{Pred}(\mathit{Zero}))$, where "=" means that both sides denote the same term.

With this, we are ready to define the characteristic term algebra as follows:

$$\begin{aligned} C(\mathit{bool}) &= \{\mathit{True}, \mathit{False}\} \\ C(\mathit{int}) &= \{\mathit{Succ}^n(\mathit{Zero}) : n \in \mathbb{Z}\} \end{aligned}$$

where the operations of sp are defined as follows:

$$\begin{aligned} C(\mathit{True}) &:= \mathit{True} \\ C(\mathit{False}) &:= \mathit{False} \\ C(\mathit{Succ})(\mathit{Succ}^n(\mathit{Zero})) &:= \mathit{Succ}^{n+1}(\mathit{Zero}) \\ C(\mathit{Pred})(\mathit{Succ}^n(\mathit{Zero})) &:= \mathit{Succ}^{n-1}(\mathit{Zero}) \\ C(\mathit{Plus})(\mathit{Succ}^n(\mathit{Zero}), \mathit{Succ}^m(\mathit{Zero})) &:= \mathit{Succ}^{n+m}(\mathit{Zero}) \\ C(\mathit{Minus})(\mathit{Succ}^n(\mathit{Zero}), \mathit{Succ}^m(\mathit{Zero})) &:= \mathit{Succ}^{n-m}(\mathit{Zero}) \\ C(\mathit{Mult})(\mathit{Succ}^n(\mathit{Zero}), \mathit{Succ}^m(\mathit{Zero})) &:= \mathit{Succ}^{n\cdot m}(\mathit{Zero}) \\ C(\mathit{Leq})(\mathit{Succ}^n(\mathit{Zero}), \mathit{Succ}^m(\mathit{Zero})) &:= \begin{cases} \mathit{True} & \text{if } n \geq m \\ \mathit{False} & \text{otherwise} \end{cases} \end{aligned}$$

In these definitions, m and n denote integers, and $\cdot, +, -$ denote the usual operations on $\mathbb{Z}$. Furthermore, $C(\mathit{And})$ and $C(\mathit{Impl})$ are defined as usual.

In order to show that sp is adequate, we show that $C \models \mathit{sp}$ and that C is a characteristic term algebra. For the latter, we have to show that $A \models (C(t) = t)$ for every model A and every term t.

In a first step, we have to show that C is actually a model of sp. For the boolean sort, this is trivial and left to the reader. (However, we don't claim that what we don't leave to the reader is not trivial...)

We proceed by checking consistency of C with the axioms of sp. Throughout the proofs, we assume $C(m) = \mathit{Succ}^p(\mathit{Zero})$, $C(n) = \mathit{Succ}^q(\mathit{Zero})$ and $C(k) = \mathit{Succ}^r(\mathit{Zero})$ with $p, q, r \in \mathbb{Z}$.

- $\mathit{Succ}(\mathit{Pred}(m)) = \mathit{Pred}(\mathit{Succ}(m)) = m$ is immediate from the definition.

- $Plus(m, Succ(n)) = Succ(Plus(m, n))$:

$$\begin{aligned}
C(Plus(m, Succ(n))) &= C(Plus)(C(m), C(Succ(n))) \\
&= C(Plus)(C(m), C(Succ)(C(n))) \\
&= C(Plus)(Succ^p(Zero), C(Succ)(Succ^q(Zero))) \\
&= C(Plus)(Succ^p(Zero), Succ^{q+1}(Zero)) \\
&= Succ^{p+q+1}(Zero) = Succ(Succ^{p+q}(Zero)) \\
&= C(Succ)(Succ^{p+q}(Zero)) \\
&= C(Succ)(C(Plus)(Succ^p(Zero), Succ^q(Zero))) \\
&= C(Succ)(C(Plus)(C(m), C(n))) \\
&= C(Succ(Plus(m, n))).
\end{aligned}$$

  The axioms $Plus(m, Zero)$ and

$$Plus(m, Pred(n)) = Pred(Plus(m, n))$$

  are verified in the same way.

- $Minus(m, Succ(n)) = Pred(Minus(m, n))$:

$$\begin{aligned}
C(Minus(m, Succ(n))) &= C(Minus)(C(m), C(Succ(n))) \\
&= C(Minus)(C(m), C(Succ)(C(n))) \\
&= C(Minus)(Succ^p(Zero), Succ(Succ^q(Zero))) \\
&= C(Minus)(Succ^p(Zero), Succ^{q+1}(Zero)) \\
&= Succ^{p-(q+1)}(Zero) \\
&= Succ^{(p-q)-1}(Zero) \\
&= Pred(Succ^{p-q}(Zero)) \\
&= C(Pred)(Succ^{p-q}(Zero)) \\
&= C(Pred)(C(Minus)(Succ^p(Zero), Succ^q(Zero))) \\
&= C(Pred)(C(Minus)(C(m), C(n))) \\
&= C(Pred)(C(Minus(m, n))) \\
&= C(Pred(Minus(m, n))).
\end{aligned}$$

  The axioms $Minus(m, Zero) = m$ and

$$Minus(m, Pred(n)) = Succ(Plus(m, n))$$

  are verified in the same way.

- $\mathit{Mult}(m, \mathit{Succ}(n)) = \mathit{Plus}(\mathit{Mult}(m,n), n)$:

$$\begin{aligned}
C(\mathit{Mult}(m, \mathit{Succ}(n))) &= C(\mathit{Mult})(C(m), C(\mathit{Succ}(n))) \\
&= C(\mathit{Mult})(C(m), C(\mathit{Succ})(C(n))) \\
&= C(\mathit{Mult})(\mathit{Succ}^p(\mathit{Zero}), C(\mathit{Succ})(\mathit{Succ}^q(\mathit{Zero}))) \\
&= C(\mathit{Mult})(\mathit{Succ}^p(\mathit{Zero}), \mathit{Succ}^{q+1}(\mathit{Zero})) \\
&= \mathit{Succ}^{p\cdot(q+1)}(\mathit{Zero}) = \mathit{Succ}^{pq+p}(\mathit{Zero}) \\
&= C(\mathit{Plus})(\mathit{Succ}^{pq}(\mathit{Zero}), \mathit{Succ}(p)(\mathit{Zero})) \\
&= C(\mathit{Plus})(C(\mathit{Mult})(\mathit{Succ}^p(\mathit{Zero}), \mathit{Succ}^q(\mathit{Zero})), \\
&\qquad\qquad \mathit{Succ}^p(\mathit{Zero})) \\
&= C(\mathit{Plus})(C(\mathit{Mult})(C(m), C(n)), C(m)) \\
&= C(\mathit{Plus})(C(\mathit{Mult}(m,n)), C(m)) \\
&= C(\mathit{Plus}(\mathit{Mult}(m,n)), m).
\end{aligned}$$

  The axioms

$$\mathit{Mult}(m, \mathit{Pred}(n)) = \mathit{Minus}(\mathit{Mult}(m,n), m) \quad \text{and} \quad \mathit{Mult}(n, \mathit{Zero}) = \mathit{Zero}$$

  are verified in the same way.

- $\mathit{Leq}(\mathit{Zero}, \mathit{Zero}) = \mathit{True}$, $\mathit{Leq}(\mathit{Zero}, \mathit{Succ}(\mathit{Zero})) = \mathit{True}$ and

$$\mathit{Leq}(\mathit{Zero}, \mathit{Pred}(\mathit{Zero})) = \mathit{False}$$

  are immediate from the definition (because $0 \leq 1$ and $0 > -1$ in the integers).

- $\mathit{Impl}(\mathit{And}(\mathit{Leq}(m,n), \mathit{Leq}(n,k)), \mathit{Leq}(m,k)) = \mathit{True}$:

$$\begin{aligned}
&C(\mathit{Impl}(\mathit{And}(\mathit{Leq}(m,n), \mathit{Leq}(n,k)), \mathit{Leq}(m,k))) \\
&= C(\mathit{Impl})(C(\mathit{And}(\mathit{Leq}(m,n), \mathit{Leq}(n,k))), C(\mathit{Leq}(m,k))) \\
&= C(\mathit{Impl})(C(\mathit{And})(C(\mathit{Leq})(C(m), C(n)), C(\mathit{Leq})(C(n), C(k))), \\
&\qquad\qquad C(\mathit{Leq})(C(m), C(k))) \\
&= C(\mathit{Impl})(C(\mathit{And})(C(\mathit{Leq})(\mathit{Succ}^p(\mathit{Zero}), \mathit{Succ}^q(\mathit{Zero})), \\
&\qquad\qquad\qquad C(\mathit{Leq})(\mathit{Succ}^q(\mathit{Zero}), \mathit{Succ}^r(\mathit{Zero}))), \\
&\qquad\qquad C(\mathit{Leq})(\mathit{Succ}^p(\mathit{Zero}), \mathit{Succ}^r(\mathit{Zero}))).
\end{aligned}$$

  By the definition of $C(\mathit{Impl})$, $C(\mathit{And})$, and $C(\mathit{Leq})$, and by the fact that

$$p \leq q \wedge q \leq r \Rightarrow p \leq r$$

  in the integers (because of $\leq$'s properties there), the last term is equal to *True* as was to be shown.

- $\mathit{Leq}(m,n) = \mathit{Leq}(\mathit{Succ}(m), \mathit{Succ}(n))$: Similar to the last item, it is easy to see that this equation holds if and only if

$$p \leq q \Rightarrow p+1 \leq q+1$$

  which is true in the integers, so the equation is true as well.

We finally conclude $C \models sp$, i.e. C is a model of sp. It remains to show that C is characteristic, i.e. that $A \models (C(t) = t)$ for every model A of sp and every term t.

Let A be a model of sp. In the sequel, we will omit $A(\cdot)$ to make the proofs more readable. Moreover, we will write $m \equiv n$ instead of $A \models (m = n)$. By simply writing "=" we mean syntactical equality of terms.

We have to prove $C(t) \equiv t$ for all terms t. We proceed by structural induction. For $t = \mathit{Zero}$ we have $C(\mathit{Zero}) = \mathit{Zero}$ by definition of C, i.e. there is nothing to prove.

Now assume that $C(s) \equiv s$, and $C(t) \equiv t$ for arbitrary terms s, t with $C(s) = \mathit{Succ}^m(\mathit{Zero})$, $C(t) = \mathit{Succ}^n(\mathit{Zero})$ $(m, n \in \mathbb{Z})$.

- $C(\mathit{Succ}(s)) \equiv \mathit{Succ}(s)$, $C(\mathit{Pred}(s)) \equiv \mathit{Pred}(s)$ are immediate from the definition of C and the induction hypothesis.
- $C(\mathit{Plus}(s,t)) \equiv \mathit{Plus}(s,t)$:

$$\begin{aligned} C(\mathit{Plus}(s,t)) &= C(\mathit{Plus})(C(s), C(t)) \\ &= C(\mathit{Plus})(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\ &= \mathit{Succ}^{m+n}(\mathit{Zero}) \stackrel{*}{\equiv} \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\ &= \mathit{Plus}(C(s), C(t)) \stackrel{\text{IH}}{\equiv} \mathit{Plus}(s,t). \end{aligned}$$

  The asterix $*$ in the 5th step is now proven by two inductions on n. For $n = 0$, it is just

$$\mathit{Succ}^m(\mathit{Zero}) \equiv \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Zero})$$

  which is one of the axioms. Now assume that

$$\mathit{Succ}^{m+n}(\mathit{Zero}) \equiv \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero}))$$

  for some $n > 0$ and show the claim for $n + 1$. Then

$$\begin{aligned} &\mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^{n+1}(\mathit{Zero})) \\ &= \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}(\mathit{Succ}^n(\mathit{Zero}))) \\ &\equiv \mathit{Succ}(\mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero}))) \\ &\stackrel{\text{IH}}{\equiv} \mathit{Succ}(\mathit{Succ}^{m+n}(\mathit{Zero})) \\ &= \mathit{Succ}^{m+n+1}(\mathit{Zero}). \end{aligned}$$

  This shows the claim for $n \geq 0$. Now assume that

$$\mathit{Succ}^{m+n}(\mathit{Zero}) \equiv \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero}))$$

  for some $n < 0$, and show the claim for $n - 1$. Then

$$\begin{aligned} &\mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^{n-1}(\mathit{Zero})) \\ &= \mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Pred}(\mathit{Succ}^n(\mathit{Zero}))) \\ &\equiv \mathit{Pred}(\mathit{Plus}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero}))) \\ &\stackrel{\text{IH}}{\equiv} \mathit{Pred}(\mathit{Succ}^{m+n}(\mathit{Zero})) \\ &= \mathit{Succ}^{m+n-1}(\mathit{Zero}). \end{aligned}$$

  Putting things together, we showed the claim for all $n \in \mathbb{Z}$.

- $C(Minus(s,t)) \equiv Minus(s,t)$: This should work in the same fashion. Let's see:

$$\begin{aligned} C(Minus(s,t)) &= C(Minus)(C(s), C(t)) \\ &= C(Minus)(Succ^m(Zero), Succ^n(Zero)) \\ &= Succ^{m-n}(Zero) \overset{*}{\equiv} Minus(Succ^m(Zero), Succ^n(Zero)) \\ &= Minus(C(s), C(t)) \overset{\text{IH}}{\equiv} Minus(s,t). \end{aligned}$$

We prove $*$ again by induction on n. First, for $n = 0$ we have

$$Succ^m(Zero) \equiv Minus(Succ^m(Zero), Zero)$$

by the corresponding axiom. Now assume that $*$ holds for $n > 0$ and show that it also holds for $n + 1$:

$$\begin{aligned} & Minus(Succ^m(Zero), Succ^{n+1}(Zero)) \\ =\ & Minus(Succ^m(Zero), Succ(Succ^n(Zero))) \\ \equiv\ & Pred(Minus(Succ^m(Zero), Succ^n(Zero))) \\ \overset{\text{IH}}{\equiv}\ & Pred(Succ^{m-n}(Zero)) \\ \equiv\ & Succ^{m-n-1}(Zero) = Succ^{m-(n+1)}(Zero). \end{aligned}$$

Note that $Pred(Succ^k(Zero)) \equiv Succ^{k-1}(Zero)$ is true for both $k \geq 0$ (by the axiom $Pred(Succ(x)) = x$) and $k < 0$ (by the definition of $Succ^k(Zero)$).

For the second induction, assume $*$ for $n < 0$ and show it for $n - 1$.

$$\begin{aligned} & Minus(Succ^m(Zero), Succ^{n-1}(Zero)) \\ =\ & Minus(Succ^m(Zero), Pred(Succ^n(Zero))) \\ \equiv\ & Succ(Minus(Succ^m(Zero), Succ^n(Zero))) \\ \overset{\text{IH}}{\equiv}\ & Succ(Succ^{m-n}(Zero)) \\ \equiv\ & Succ^{m-n+1}(Zero) = Succ^{m-(n-1)}(Zero), \end{aligned}$$

where the last but one step is tackled the same way as above.

- $C(Mult(s,t)) \equiv Mult(s,t)$:

$$\begin{aligned} C(Mult(s,t)) &= C(Mult)(C(s), C(t)) \\ &= C(Mult)(Succ^m(Zero), Succ^n(Zero)) \\ &= Succ^{m \cdot n}(Zero) \overset{*}{\equiv} Mult(Succ^m(Zero), Succ^n(Zero)) \\ &= Mult(C(s), C(t)) \overset{\text{IH}}{\equiv} Mult(s,t) \end{aligned}$$

Proof of $*$ by induction on n: For $n = 0$, we have

$$Succ^{m \cdot 0}(Zero) = Zero \equiv Mult(Succ^m(Zero), Zero)$$

by an axiom. Assume $*$ for $n > 0$ and prove it for $n + 1$.

$$\begin{aligned}
& \mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^{n+1}(\mathit{Zero})) \\
=\ & \mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}(\mathit{Succ}^n(\mathit{Zero}))) \\
\equiv\ & \mathit{Plus}(\mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})), \mathit{Succ}^n(\mathit{Zero})) \\
\stackrel{\mathrm{IH}}{\equiv}\ & \mathit{Plus}(\mathit{Succ}^{m\cdot n}(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\
\equiv\ & \mathit{Succ}^{m\cdot n+n}(\mathit{Zero}) = \mathit{Succ}^{m\cdot(n+1)}(\mathit{Zero}).
\end{aligned}$$

Note that the last but one step has already been proven in the second subproof, i.e. in the proof of $C(\mathit{Plus}(s,t)) \equiv \mathit{Plus}(s,t)$.

Now, assume that $*$ holds for $n < 0$ and prove it for $n - 1$.

$$\begin{aligned}
& \mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^{n-1}(\mathit{Zero})) \\
=\ & \mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Pred}(\mathit{Succ}^n(\mathit{Zero}))) \\
\equiv\ & \mathit{Minus}(\mathit{Mult}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})), \mathit{Succ}^n(\mathit{Zero})) \\
\stackrel{\mathrm{IH}}{\equiv}\ & \mathit{Minus}(\mathit{Succ}^{m\cdot n}(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\
\equiv\ & \mathit{Succ}^{m\cdot n-n}(\mathit{Zero}) = \mathit{Succ}^{m\cdot(n-1)}(\mathit{Zero}).
\end{aligned}$$

- $C(\mathit{Leq}(s,t)) \equiv \mathit{Leq}(s,t)$. First case: Assume $m \le n$.

$$\begin{aligned}
C(\mathit{Leq}(s,t)) &= C(\mathit{Leq})(C(s), C(t)) = C(\mathit{Leq})(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\
&= \mathit{True} \stackrel{*}{\equiv} \mathit{Leq}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \\
&= \mathit{Leq}(C(s), C(t)) \stackrel{\mathrm{IH}}{\equiv} \mathit{Leq}(s,t).
\end{aligned}$$

To see $*$, we prove

$$\mathit{Leq}(\mathit{Zero}, \mathit{Succ}^k(\mathit{Zero})) \equiv \mathit{True} \tag{1}$$

for $k \ge 0$, and

$$\mathit{Leq}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \equiv \mathit{Leq}(\mathit{Zero}, \mathit{Succ}^{n-m}(\mathit{Zero})). \tag{2}$$

Then

$$\mathit{Leq}(\mathit{Succ}^m(\mathit{Zero}), \mathit{Succ}^n(\mathit{Zero})) \stackrel{(2)}{\equiv} \mathit{Leq}(\mathit{Zero}, \mathit{Succ}^{n-m}(\mathit{Zero})) \stackrel{(1)}{\equiv} \mathit{True}$$

taking $k = n - m \ge 0$ in the second step.

The proofs of (1) and (2) proceed by induction (what a surprise...).

(1) For the base case, $\mathit{Leq}(\mathit{Zero}, \mathit{Zero}) \equiv \mathit{True}$ is an axiom. Now assume that $\mathit{Leq}(\mathit{Zero}, \mathit{Succ}^k(\mathit{Zero})) \equiv \mathit{True}$. Then, by the linearity axiom

$$\mathit{Leq}(\mathit{Succ}(\mathit{Zero}), \mathit{Succ}^{k+1}(\mathit{Zero})) = \mathit{True},$$

and using transitivity and $\mathit{Leq}(\mathit{Zero}, \mathit{Succ}(\mathit{Zero}))$ leads to

$$\mathit{Leq}(\mathit{Zero}, \mathit{Succ}^{k+1}(\mathit{Zero})) = \mathit{True}.$$

(2) For the base case we have

$$Leq(Succ^0(Zero), Succ^n(Zero)) = Leq(Zero, Succ^{n-0}(Zero)),$$

i.e., there is nothing to prove. Now assume that

$$Leq(Succ^m(Zero), Succ^n(Zero)) = Leq(Zero, Succ^{n-m}(Zero)),$$

holds for some $m \in \mathbb{Z}$ and any $n \in \mathbb{Z}$. Then by the linearity axiom

$$\begin{aligned}
& Leq(Succ^{m+1}(Zero), Succ^n(Zero)) \\
\equiv\ & Leq(Succ^{m+1-1}(Zero), Succ^{n-1}(Zero)) \\
\overset{\text{IH}}{\equiv}\ & Leq(Zero, Succ^{n-1-m}(Zero)) \\
=\ & Leq(Zero, Succ^{n-(m+1)}(Zero).
\end{aligned}$$

For the case when $m > n$, an analogous argument is possible.

Sumarizing, we have shown that C is a characteristic term algebra and C is a model of sp. Obviously, C is a isomorphic to the natural algebra of integers, and putting all this things together is is shown that sp is an adequate specification of the integers.