Corecursion and coinduction: what they are and how they relate to recursion and induction

Mike Gordon
## Contents

- **Preface** 3

- **Summary** 4
  - Data, codata, constructors and destructors 4
  - Recursion and corecursion 5
  - Fixed points, induction, coinduction and bisimulation 6
  - Overview of the rest of this article 7

- **Natural numbers, Peano’s axioms and Peano structures** 8

- **Algebras and coalgebras** 8
  - Numbers and conumbers 9
  - Example of corecursion for numbers 11
  - Lists and colists 12
  - Example of corecursion for lists 15

- **Coinduction and bisimulation** 17
  - Bisimulation coinduction for conumbers 17
    - Example of bisimulation coinduction for numbers 17
    - Justification of bisimulation coinduction for numbers 18
  - Bisimulation coinduction for lists 19
    - Examples of bisimulation coinduction for lists 20
    - Justification of bisimulation coinduction for lists 23

- **F-algebras and F-coalgebras** 24
  - Set theory notation 24
  - Numbers and lists 25
  - Morphisms 26
  - Initial and terminal algebras 28

- **Least and greatest fixed points** 28
  - Fixed points, numbers and conumbers 28
  - Summary of fixed point proof rules for numbers and conumbers 29
  - Fixed points, lists and colists 30
  - Summary of fixed point proof rules for lists and colists 31

- **Use in programming** 32

- **Concluding thoughts** 34

This article is at [http://www.cl.cam.ac.uk/~mjcg/plans/Coinduction.html](http://www.cl.cam.ac.uk/~mjcg/plans/Coinduction.html) and is meant for reading in a browser, but the web page can take several minutes to load because MathJax is slow. The PDF version is quicker to load, but the latex generated by Pandoc is not as beautifully formatted as it would be if it were generated from bespoke \( \text{LaTeX} \).
Preface

For years I’ve been vaguely aware of corecursion and coinduction as something dual to recursion and induction, and related to maximal fixed points and bisimulation – but I’ve never really grasped exactly what they are and what the “co” means.

The Wikipedia article on corecursion says:

... recursion works analytically, starting on data further from a base case and breaking it down into smaller data and repeating until one reaches a base case, corecursion works synthetically, starting from a base case and building it up, iteratively producing data further removed from a base case.

and the Wikipedia article on coinduction says:

Coinduction is the mathematical dual to structural induction. Coinductively defined types are known as codata and are typically infinite data structures, such as streams.

I googled “what is coinduction” and saw that other people were puzzled too. For example, Google found links to an answer to the question What the heck is coinduction. At a recent event I asked several people for a brief outline of induction versus coinduction and found that even eminent experts in the use of coinductive methods sometimes had a somewhat fuzzy grasp of how induction and coinduction are dual. Google also found a couple of excellent tutorials:

- An introduction to (co)algebra and (co)induction by Bart Jacobs and Jan Rutten;

and I spotted a new book Introduction to Coalgebra by Bart Jacobs whilst browsing in the CUP bookshop – subsequent googling discovered a preliminary version of this online here.

My goal in writing this article is to reduce my lack of understanding through the activity of creating a short and coherent explanation of the essence of corecursion and coinduction and how they relate to recursion and induction. The goal is not to show applications – the examples I give are not meant to demonstrate the utility of the concepts, just to concretely illustrate them.

There is nothing new here. The material is adapted from several sources, particularly those mentioned above, as well as other papers and web pages that
I happened to stumble across and found enlightening – links to some of these are included in the text. I mostly didn’t read these beyond the introductory and motivational parts, so it’s inevitable that I’ve misunderstood some things. As my sources are just those I happened to find, there might be better ones I could have read and cited. Please let me know if you have any suggestions.

Summary

This article is mostly about corecursion and coinduction for numbers and lists. Numbers are the most well-known setting for recursion and induction, but corecusion and coinduction on numbers are pretty useless ... however, they do provide a simple setting for explaining the core ideas. I use lists as a second example as it generalises and extends the ideas first introduced for numbers, and provides a setting where corecusion and coinduction can be seen to be useful and are used in applications (though I don’t discuss applications here). Lists are also a stepping stone to my regrettably superficial account of corecursion and coinduction in the more general setting of algebras and coalgebras.

My early drafts were rather formal and included proofs of everything, some of which I even started to check using a computer proof assistant. This was partly because I was struggling to understand the details and wanted to be confident I’d got them right. After a while I realised that writing the article was taking too long. Furthermore, the notational infrastructure needed for fully rigorous formal precision was obscuring the essence of the ideas. I also realised that the thing I was producing was in danger of ending up as an amateur and inferior version of existing expositions. I decided to scale back on mathematical precision and largely give up on including formal proofs. A result of this is that I say things that I haven’t checked in detail, so there are bound to be errors, technical mistakes and embarrassing conceptual misunderstandings. If you happen to be reading this and spot any of these, then please let me know!

The rest of this section is a very condensed preview of the core ideas in the rest of the article as they apply to lists. The sections that follow provide more explanation and details, starting with corecursion and coinduction for numbers. At the end of the article there are brief discussions of how the number and list examples fit into the more general framework of algebras and coalgebras, and then how this relates to programming language datatypes and function definitions on these types.

Data, codata, constructors and destructors

Data represents finite values and is built by evaluating applications of constructor functions. Codata often – but not necessarily – represents infinite values and is defined by specifying the values of destructor functions. Here are two examples.
• Data: The finite list \( L = [1, 1, 1, 1] \) is built by specifying 
\( L = \text{cons}(1, \text{cons}(1, \text{cons}(1, \text{cons}(1, \text{nil})))) \), where \text{cons} is a list constructor and \text{nil}, the empty list, a nullary constructor.

• Codata: The infinite list \( l_\infty = [1, 1, 1, \ldots] \) is defined by specifying 
\( \text{hd}(l_\infty) = 1 \) and \( \text{tl}(l_\infty) = l_\infty \), where \text{hd} and \text{tl} are destructors.

Recursion and corecursion

Recursion defines a function that maps values from a datatype by invoking itself on the components of the constructors used to build the datatype values. Corecursion defines a function to a codatatype by specifying the values of destructors on applications of the function. This is illustrated below using lists \( \mathbb{L} \) and colists \( \mathbb{L} \).

Let \( \mathbb{N} \) be the set of natural numbers, \( \mathbb{L} \) be the set of finite lists of numbers and \( \mathbb{L}_\infty \) the set of infinite lists of numbers. Let \( \mathbb{L} = \mathbb{L} \cup \mathbb{L}_\infty \) be the set of finite or infinite lists of numbers. The empty list is \text{nil}, \( \text{cons}(n, l) \) is the list constructed by adding the number \( n \) to the front of list \( l \), \text{hd}(l) \) is the first element of \( l \) and \( \text{tl}(l) \) is the list resulting from removing its first element, so \( \text{cons}(\text{hd}(l), \text{tl}(l)) = l \).

Example: the function Add1 that adds 1 to each element of a list of numbers is defined below both by recursion and corecursion. For the recursion one views Add1 as having type Add1 : \( \mathbb{L} \to X \) and for corecursion having type Add1 : \( X \to \mathbb{L} \). For the Add1 example \( X = \mathbb{L} \).

• Recursion:
\[
\text{Add1}(\text{nil}) = \text{nil} \quad \text{and} \quad \text{Add1}(\text{cons}(n, l)) = \text{cons}(n+1, \text{Add1}(l))
\]

• Corecursion:
\[
\text{null}(\text{Add1}(l)) = (l = \text{nil}) \quad \text{and} \quad \text{hd}(\text{Add1}(l)) = \text{hd}(l) + 1 \quad \text{and} \quad \text{tl}(\text{Add1}(l)) = \text{Add1}(\text{tl}(l))
\]

More generally, recursion defines functions from \( \mathbb{L} \), whereas corecursion defines functions to \( \mathbb{L} \).

• If \( X \) is a set, \( x_0 \in X \) and \( \theta : \mathbb{N} \times X \to X \), then recursion legitimates the definition of \( f : \mathbb{L} \to X \) by:
\[
f(\text{nil}) = x_0 \quad \text{and} \quad f(\text{cons}(n, l)) = \theta(n, f(l))
\]
which is equivalent to the single recursion equation:
\[
f(l) = \textbf{if } l = \text{nil} \textbf{ then } x_0 \textbf{ else } \theta(\text{hd}(l), f(\text{tl}(l)))
\]

• If \( X \) is a set, \( P \subseteq X \) and \( \phi : \{ x \mid x \in X \land x \notin P \} \to \mathbb{N} \times X \), then corecursion legitimates the definition of \( g : X \to \mathbb{L} \) by:
\[
\text{null}(g(x)) = (x \in P) \quad \text{and} \quad \text{hd}(g(x)) = \pi_1(\phi(x)) \quad \text{and} \quad \text{tl}(g(x)) = g(\pi_2(\phi(x)))
\]
which is equivalent to the single corecursion equation:
\[
g(x) = \textbf{if } x \in P \textbf{ then } \text{nil} \textbf{ else } \text{cons}(\pi_1(\phi(x)), g(\pi_2(\phi(x))))
\]
where \( \pi_1, \pi_2 \) extract the first and second elements of a pair.
A typical, though trivial, example of corecursion is:

\[ \text{CountFrom}(n) = \text{cons}(n, \text{CountFrom}(n+1)) \]
which defines \( \text{CountFrom}(n) \) to be the infinite list counting up from \( n \), i.e. \( \text{cons}(n, \text{cons}(n+1, \text{cons}(n+2, \ldots))) \). This corecursion is an instance of:

\[ g(x) = \begin{cases} x \in P & \text{nil} \\ \text{else} & \text{cons}(\pi_1(\phi(x)), g(\pi_2(\phi(x)))) \end{cases} \]
if \( X = \mathbb{N}, P \) is the empty set and \( \theta(n) = (n, n+1) \). The function \( g \) can also be specified by giving equations for the destructors:

\[ \text{hd}(\text{CountFrom}(n)) = n \text{ and } \text{tl}(\text{CountFrom}(n)) = \text{CountFrom}(n+1) \]
A less trivial version of this example of corecursion is:

\[ \text{CountUpTo}(m, n) = \begin{cases} m = n & \text{nil} \\ \text{else} & \text{cons}(m, \text{CountUpTo}(m+1, n)) \end{cases} \]
which defines \( \text{CountUpTo} \) to be the finite list consisting of successive numbers greater than or equal to \( m \) and less than \( n \), if \( m \leq n \), and the infinite list counting up from \( m \), if \( m > n \). This corecursion is an instance of:

\[ g(x) = \begin{cases} x \in P & \text{nil} \\ \text{else} & \text{cons}(\pi_1(\phi(x)), g(\pi_2(\phi(x)))) \end{cases} \]
if \( X = \mathbb{N} \times \mathbb{N}, P = \{(m, n) \mid m = n\} \) and \( \theta(m, n) = (m, (m+1, n)) \).
Returning to the equation for \( \text{Add1} \) discussed above:

\[ \text{Add1}(l) = \begin{cases} l = \text{nil} & \text{nil} \\ \text{else} & \text{cons}(\text{hd}(l)+1, \text{Add1}(\text{tl}(l))) \end{cases} \]
This can be viewed both as a definition by recursion by taking \( f = \text{Add1}, X = \mathbb{L}, x_0 = \text{nil} \) and \( \theta(n, l) = \text{cons}(n+1, l) \) in the recursion scheme for \( f \) in the first bullet point above, or as a definition by corecursion by taking \( g = \text{Add1}, X = \overline{\mathbb{L}}, P = \{\text{nil}\} \) and \( \phi(l) = (\text{hd}(l)+1, \text{tl}(l)) \) in corecursion scheme for \( g \) in the second bullet point. The definition by recursion maps \( \mathbb{L} \) to \( \mathbb{L} \), but the definition by corecursion maps \( \overline{\mathbb{L}} \) to \( \overline{\mathbb{L}} \), which allows infinite lists to be arguments and results.

**Fixed points, induction, coinduction and bisimulation**

If \( L \subseteq \overline{\mathbb{L}} \), define \( \mathcal{F}(L) \) by: \( \mathcal{F}(L) = \{\text{nil}\} \cup \{\text{cons}(n, l) \mid n \in \mathbb{N} \text{ and } l \in L\} \).
\( \mathbb{L} \) and \( \overline{\mathbb{L}} \) are both fixed points of \( \mathcal{F} \), i.e. \( \mathcal{F}(\mathbb{L}) = \mathbb{L} \) and \( \mathcal{F}(\overline{\mathbb{L}}) = \overline{\mathbb{L}} \). The least fixed point is \( \mathbb{L} \) and the greatest fixed point is \( \overline{\mathbb{L}} \).
\( \mathbb{L} \) is also the least pre-fixed point of \( \mathcal{F} \), that is the least \( L \) such that \( \mathcal{F}(L) \subseteq L \). Thus if \( \mathcal{F}(L) \subseteq L \) then by leastness \( \mathbb{L} \subseteq L \). This is the principle of induction for finite lists since \( \mathcal{F}(L) \subseteq L \) is equivalent to \( \text{nil} \in L \) (the base case of the induction) and \( \forall n \in \mathbb{N}. \forall l \in L. \text{cons}(n, l) \in L \) (the induction step). \( \mathbb{L} \subseteq L \) is equivalent to \( \forall l \in \mathbb{L}. l \in L \).
If \( R \subseteq \mathbb{L} \times \mathbb{L} \) is a binary relation on \( \mathbb{L} \), then define \( \mathcal{B}(R) \subseteq \mathbb{L} \times \mathbb{L} \) by:

\[ \mathcal{B}(R) = \{(\text{nil, nil}) \cup \{\text{cons}(n, l_1), \text{cons}(n, l_2) \mid n \in \mathbb{N} \wedge (l_1, l_2) \in R\} \]
The least fixed point of $\mathcal{B}$ is the equality relation on $\mathbb{L}$, i.e. $\{(l, l) \mid l \in \mathbb{L}\}$, and the greatest fixed point is the equality relation on $\mathbb{L}$, i.e. $\{(l, l) \mid l \in \mathbb{L}\}$.

The relation $\{(l, l) \mid l \in \mathbb{L}\}$ is also the greatest post-fixed point of $\mathcal{B}$, that is the greatest $R$ such that $R \subseteq \mathcal{B}(R)$. Thus if there exists an $R$ such that $R \subseteq \mathcal{B}(R)$, then by greatestness $R \subseteq \{(l, l) \mid l \in \mathbb{L}\}$.

The property $R \subseteq \mathcal{B}(R)$ means that if $(l_1, l_2) \in R$ then either $l_1 = \text{nil}$ and $l_2 = \text{nil}$ or else $l_1 = \text{cons}(n, l'_1)$ and $l_2 = \text{cons}(n, l'_2)$ and $(l'_1, l'_2) \in R$, for some $n \in \mathbb{N}$ and $l'_1, l'_2 \in \mathbb{L}$. Such an $R$ is called a bisimulation. The proof principle that if $R$ is a bisimulation, then $\forall l_1, l_2 \in \mathbb{L}. (l_1, l_2) \in R \Rightarrow l_1 = l_2$ is an example of coinduction.

Both the terms “bisimulation” and “coinduction” originate from Robin Milner. For further historical details see Section 4.3 of Sangiorgi’s paper On the Origins of Bisimulation and Coinduction and Milner and Tofte’s paper Co-induction in relational semantics.

Overview of the rest of this article

The rest of this paper consists of the following.

- A discussion of the traditional Peano axioms for numbers and their equivalence to another definition, which is based on the unique existence of functions and whose dual yields the conumbers.
- Numbers are fitted into the general framework of algebras and its dual, coalgebras, is introduced. Corecursion for conumbers is explained and some examples given.
- Lists are introduced as another example of algebras and colists as another example of coalgebras. Examples of corecursion for lists are given.
- Coinduction is explained and the way in which it is dual to induction discussed. Bisimulation relations are introduced and their central role in coinduction explained. Examples for numbers and lists are described.
- $\mathbb{F}$-algebras and $\mathbb{F}$-coalgebras are introduced as a uniform framework with numbers and lists being special cases. Algebra and coalgebra morphisms are defined. Initial and terminal algebras and coalgebras are explained as a general way of defining datatypes, with numbers and lists being examples.
- The roles of least and greatest fixed points in characterising numbers, conumbers, lists and colists are explained and so is the relation of fixed points to induction and coinduction.
- Some brief comments are made on how algebras and coalgebras relate to programming language datatypes, and how recursion and corecursion can be used to define function on data and codata.
Natural numbers, Peano’s axioms and Peano structures

The Wikipedia article says that coinduction is the “mathematical dual to structural induction”, so a good starting place is ordinary mathematical induction, which is structural induction applied to the natural number structure \((\mathbb{N}, 0, S)\), where \(\mathbb{N}\) is a set, \(0 \in \mathbb{N}\) a constant and \(S : \mathbb{N} \to \mathbb{N}\) a one-argument function.

The five Peano axioms define the set \(\mathbb{N}\) of natural numbers:

1. \(0 \in \mathbb{N}\)
2. \(\forall n \in \mathbb{N}. S(n) \in \mathbb{N}\)
3. \(\forall n \in \mathbb{N}. S(n) \neq 0\)
4. \(\forall m \in \mathbb{N}. \forall n \in \mathbb{N}. S(m) = S(n) \Rightarrow m = n\)
5. \(\forall M. 0 \in M \land (\forall n \in M. S(n) \in M) \Rightarrow \mathbb{N} \subseteq M\)

The structure \((\mathbb{N}, 0, S)\) is an instance of a class of structures \((A, z, s)\), where \(A\) is a set, \(z \in A\) and \(s : A \to A\). These structures seem to have several names, including discrete dynamical systems and Peano structures. The latter name is used here.

The existence of \((\mathbb{N}, 0, S)\) satisfying Peano’s axioms follows from the axioms of set theory, e.g. see this wikipedia article. Peano’s axioms entail the principle of recursive definition. This says that for any Peano structure \((A, z, s)\) there is exactly one function \(f : \mathbb{N} \to A\) such that \(f(0) = z\) and \(\forall n \in \mathbb{N}. f(S(n)) = s(f(n))\). Showing this is straightforward, but not entirely trivial (e.g. see here for a discussion and here for a detailed proof).

The principle of recursive definition is equivalent to Peano’s axioms because \((\mathbb{N}, 0, S)\) satisfies the five Peano axioms if and only if for all Peano structures \((A, z, s)\) there is exactly one function \(f : \mathbb{N} \to A\) such that: \(f(0) = z \land \forall n \in \mathbb{N}. f(S(n)) = s(f(n))\). \((\mathbb{N}, 0, S)\) an example of an initial algebra.

Algebras and coalgebras

A Peano structure is an example of an algebra. The dual of an algebra is a coalgebra. The dual of the natural numbers are the conatural numbers, also called the conumbers. These will be described using coalgebras.
It seems that algebras and coalgebras can be formulated in various ways. The simplest one I’ve found defines an algebra to be a structure consisting of a carrier set plus some number of distinguished elements and some number of functions, called constructors, whose range is the carrier set. An example of an algebra is a Peano algebra, which is just what was previously called a Peano structure. A Peano algebra \((A, z, s)\) has a carrier \(A\), only one distinguished element \(z \in A\) and only one constructor function \(s : A \to A\). The arity of a constructor is the number of arguments it takes. Distinguished elements like \(z\) are considered to be nullary constructors, i.e. to have arity 0.

**Numbers and conumbers**

The natural numbers are the Peano algebra \((\mathbb{N}, 0, S)\) with the property that for any Peano structure \((A, z, s)\) there’s exactly one function \(f : \mathbb{N} \to A\) such that \(f(0) = z\) and \(\forall n \in \mathbb{N}. f(S(n)) = s(f(n))\). The function \(f\) can also be defined by a single equation \(f(n) = \text{if } n=0 \text{ then } z \text{ else } s(f(n-1))\).

The dual of an algebra is a coalgebra. This also has a carrier set, but instead of constructor functions that build members of the carrier, a coalgebra has destructor functions that split members of the carrier into the components they are built from. Thus the carrier of an algebra is the range of its constructors, but the carrier of a coalgebra is the domain of its destructors.

A destructor is dual to a constructor in that it splits the results of a construction into its components. If \(c\) is an \(n\)-ary constructor and \(c(a_1, \ldots, a_n) = a\), then its dual destructor, \(d\) say, splits \(a\) into \((a_1, \ldots, a_n)\), i.e. \(d(a) = (a_1, \ldots, a_n)\). In general, the dual of a non-nullary constructor is a partial function – it’s only defined on those elements that are constructed by the dual constructor, these elements are the domain of the destructor. The domain of \(d\) is denoted by \(\text{Dom}(d)\).

The dual of the unary number constructor \(S\) is the predecessor function \(P\) defined by \(P(n) = n-1\), where \(P\) is the partial function only defined on non-zero numbers, so \(\text{Dom}(P) = \{n \mid n > 0\}\).

Nullary constructors represent distinguished elements of the carrier, so it’s not obvious what their corresponding destructors are, since there are no components of a corresponding constructor to return. To cope with this, destructors corresponding to nullary constructors return a ‘dummy value’ to represent ‘no components’. This value is traditionally denoted by \(\ast\), though \(()\) might be more mnemonic. This may seem like an odd way to represent the duals of nullary constructors, but it should become more motivated in the section on \(F\)-algebras and \(F\)-coalgebras below. In the summary section \(x \in d\) is an abbreviation for \(x \in \text{Dom}(d)\), where \(d\) is a nullary destructor.

The conumbers dual of the distinguished number 0 is the partial function \(\text{is}0 : \{0\} \to \{\ast\}\), and so necessarily \(\text{is}0(0) = \ast\) and \(\text{Dom}(\text{is}0) = \{0\}\).
The domain of a non-nullary destructor is the set of members of the carrier that are constructed using the dual constructor. The domain of a nullary operator is the set just containing it. The carrier of a coalgebra is required to be partitioned by the domains of its destructors. Thus each element of the carrier will be a member of the domain of exactly one destructor.

The relation between constructors and destructors described above is only intended to provide some intuition. I don’t know whether in general algebras and coalgebras come in pairs with each constructor in an algebra dual to a destructor in the coalgebra it’s paired with. Such a relationship may hold for some particular algebra-coalgebra pairs, like the Peano algebra and coalgebra described below (and maybe also for all initial \( \mathbb{F} \)-algebras and terminal \( \mathbb{F} \)-coalgebras). I’m ignorant of the full theory, but my guess is that such a relationship doesn’t hold in general.

If a coalgebra has more than one destructor, then all its destructors are partial functions. Here’s some useful notation. Writing \( \theta : X \rightarrow X \) means \( \theta \) is a partial function from set \( X \) to set \( Y \). The subset of \( X \) where \( \theta \) is defined – i.e. the domain of \( \theta \) – is denoted by \( \text{Dom}(\theta) \). If \( \theta : X \rightarrow Y \) – i.e. \( \theta \) is a total function – then \( \text{Dom}(\theta) = X \). If \( \theta : X \rightarrow Y \) or \( \theta : X \rightarrow Y \) and if \( U \subseteq X \) and \( V \subseteq Y \), then writing \( \theta : U \rightarrow V \) means that if \( x \in U \) then \( \theta(x) \in V \). In particular, if \( \theta : X \rightarrow Y \) then \( \theta : \text{Dom}(\theta) \rightarrow Y \).

The dual of a Peano algebra \( \langle A, z, s \rangle \) is a Peano coalgebra \( \langle C, isz, p \rangle \) where \( isz \) and \( p \) are destructors: \( isz : C \rightarrow \{\ast\} \) is a nullary destructor and \( p : C \rightarrow C \) is a unary destructor. The domains of \( isz \) and \( p \) partition \( C \), so if \( x \in C \) then either \( x \in \text{Dom}(isz) \) or \( x \in \text{Dom}(p) \), but not both.

The \textit{conatural numbers} are the Peano coalgebra \( \langle \mathbb{N}, is0, P \rangle \) with the property that for any Peano coalgebra \( \langle C, isz, p \rangle \) there is exactly one function \( g : C \rightarrow \mathbb{N} \) such that for all \( x \in C \):

- if \( x \in \text{Dom}(isz) \) then \( g(x) \in \text{Dom}(is0) \) and \( is0(g(x)) = isz(x) \);
- if \( x \in \text{Dom}(p) \) then \( g(x) \in \text{Dom}(P) \) and \( P(g(x)) = g(p(x)) \).

The coalgebra \( \langle \mathbb{N}, is0, P \rangle \) is an example of a \textit{terminal coalgebra}.

It turns out that the unique existence of \( g \) property in the preceding paragraph determines the Peano coalgebra \( \langle \mathbb{N}, is0, P \rangle \) to have carrier set \( \mathbb{N} = \mathbb{N} \cup \{\infty\} \), the nullary destructor \( is0 : \{0\} \rightarrow \{\ast\} \) satisfying \( is0(0) = \ast \) and the unary destructor \( P \) to be the predecessor function \( n \mapsto n - 1 \) extended by defining \( P(\infty) = \infty \), thus \( P : \{ n \mid (n \in \mathbb{N} \land n > 0) \lor n = \infty \} \rightarrow \mathbb{N} \).

It’s useful to \textit{extend the addition operator} to conumbers \( \mathbb{N} \) by specifying that if either argument is \( \infty \) then so is the result. For example, \( \infty + 1 = \infty \). Note that \(+ \) extended to \( \mathbb{N} \) is associative and commutative. With this extension, \( m = P(n) \iff m + 1 = n \) for all \( m \) and \( n \) in \( \mathbb{N} \).
With this extended definition of +, the function $g$ is defined by the single equation:

$$g(x) = \text{if } isz(x) = \ast \text{ then } 0 \text{ else } g(p(x)) + 1.$$ 

Note the ways in which natural numbers are dual to conatural numbers:

- Constructors $0 \in \mathbb{N}$, $S : \mathbb{N} \to \mathbb{N}$ versus destructors $iz0 : \mathbb{N} \to \{\ast\}$, $P : \mathbb{N} \to \mathbb{N}$;
- Unique $f : \mathbb{N} \to A$ versus unique $g : C \to \mathbb{N}$;
- Define $f$ on constructed values: $f(0) = z \land f(S(n)) = s(f(n))$ versus define destructors on values of $g$: $iz0(g(x)) = isz(x) \land P(g(x)) = g(p(x))$;
- Recursion $f(n) = \text{if } n = 0 \text{ then } z \text{ else } s(f(n-1))$ versus corecursion $g(x) = \text{if } isz(x) = \ast \text{ then } 0 \text{ else } g(p(x)) + 1$.
- Simple recursion on natural numbers always terminates versus corecursion on conumbers sometimes doesn’t terminate (see example below).

**Example of corecursion for numbers**

The notation $[x_1 \mapsto v_1, \ldots, x_k \mapsto v_k]$ denotes the function $\theta$ with domain $\{x_1, \ldots, x_k\}$ defined by $\theta(x_i) = v_i$. Using this notation, consider the Peano coalgebra $(C, isz, p)$ where:

$\begin{align*}
C &= \{A, B, C, D, E, F, G, H, I, J\}, \\
isz &= [F \mapsto \ast, J \mapsto \ast], \\
p &= [A \mapsto A, B \mapsto C, C \mapsto B, D \mapsto E, E \mapsto F, G \mapsto H, H \mapsto I, I \mapsto J].
\end{align*}$

$\text{Dom}(isz) = \{F, J\}$ and $\text{Dom}(p) = \{A, B, C, D, E, G, H, I\}$, so $\text{Dom}(isz)$ and $\text{Dom}(p)$ partition $C$.

This coalgebra is diagrammed in Figure 1 below: an arrow from $x$ to $x'$ means that if $x \in \text{Dom}(p)$ then $p(x) = x'$, and if $x \in \text{Dom}(isz)$ then $isz(x) = \ast$.

Consider now the definition of $g : C \to \mathbb{N}$ specified for $x \in C$ by $g(x) = \text{if } isz(x) = \ast \text{ then } 0 \text{ else } g(p(x)) + 1$.

Rewriting $g(A)$ with this equation yields:

$g(A) = g(p(A)) + 1 = g(A) + 1$

The only way this can be satisfied is with $g(A) = \infty$.

Rewriting $g(B)$ and $g(C)$ yields:

$g(B) = g(p(B)) + 1 = g(C) + 1 = (g(p(C)) + 1) + 1 = (g(B) + 1) + 1 = g(B) + 2$

$g(C) = g(p(C)) + 1 = g(B) + 1 = (g(p(B)) + 1) + 1 = (g(C) + 1) + 1 = g(C) + 2$

The only way these can be satisfied is with $g(B) = \infty$ and $g(C) = \infty$. 

11
Thus evaluating $g(x)$ by rewriting with the equation for $g$ loops if $x \in \{A, B, C\}$.

On other arguments the rewriting terminates:

- $g(F) = 0$
- $g(E) = g(p(E))+1 = g(F)+1 = 0+1 = 1$
- $g(D) = g(p(D))+1 = g(E)+1 = 1+1 = 2$
- $g(J) = 0$
- $g(I) = g(p(I))+1 = g(J)+1 = 0+1 = 1$
- $g(H) = g(p(H))+1 = g(I)+1 = 1+1 = 2$
- $g(G) = g(p(G))+1 = g(H)+1 = 2+1 = 3$

These rewriting calculations show that:

$$g = \{A \mapsto \infty, B \mapsto \infty, C \mapsto \infty, D \mapsto 2, E \mapsto 1, F \mapsto 0, G \mapsto 3, H \mapsto 2, I \mapsto 1, J \mapsto 0\}$$

For an arbitrary Peano coalgebra $(C, \text{isz}, p)$, the function $g : C \rightarrow \mathbb{N}$ satisfying the equation $g(x) = \text{if } isz(x) = \ast \text{ then } 0 \text{ else } g(p(x))+1$ is described by:

$$g(x) = \begin{cases} n & \exists x_0 \cdots x_n. x = x_0 \land isz(x_n) = \ast \land \forall i < n. p(x_i) = x_{i+1} \\ \infty & \text{otherwise} \end{cases}$$

The example just given illustrates this.

**Lists and colists**

If $\mathcal{A}$ is a set – the name “$\mathcal{A}$” for “alphabet” – then the set $L_{\mathcal{A}}$ of finite lists (or strings) of members of $\mathcal{A}$ is defined by two constructors: the empty list $\text{nil} \in L_{\mathcal{A}}$
and the function $\text{cons} : \mathbb{A} \times L_{\mathbb{A}} \rightarrow L_{\mathbb{A}}$ which constructs the new list $\text{cons}(a, l)$ that results from adding the element $a \in \mathbb{A}$ to the front of list $l \in L_{\mathbb{A}}$.

Peano-style axioms for lists are:

1. $\text{nil} \in L_{\mathbb{A}}$
2. $\forall a \in \mathbb{A}. \forall l \in L_{\mathbb{A}}. \text{cons}(a, l) \in L_{\mathbb{A}}$
3. $\forall a \in \mathbb{A}. \forall l \in L_{\mathbb{A}}. \text{cons}(a, l) \neq \text{nil}$
4. $\forall a_1, a_2 \in \mathbb{A}. \forall l_1, l_2 \in L_{\mathbb{A}}. \text{cons}(a_1, l_1) = \text{cons}(a_2, l_2) \Rightarrow a_1 = a_2 \land l_1 = l_2$
5. $\forall M. \text{nil} \in M \land (\forall a \in \mathbb{A}. \forall l \in M. \text{cons}(a, l) \in M) \Rightarrow L_{\mathbb{A}} \subseteq M$

Axiom 5 entails that if $l \in L_{\mathbb{A}}$ then $l = \text{nil}$ or $l = \text{cons}(a, l')$ for some $a \in \mathbb{A}$ and $l' \in L_{\mathbb{A}}$ (proof: specialise $M$ to $\{l \mid l = \text{nil} \lor \exists a \in \mathbb{A}. \exists l' \in L_{\mathbb{A}}. l = \text{cons}(a, l')\}$ in Axiom 5). This and Axiom 4 shows that there are destructors $\text{hd} : L_{\mathbb{A}} \rightarrow \mathbb{A}$ and $\text{tl} : L_{\mathbb{A}} \rightarrow L_{\mathbb{A}}$, which satisfy $\forall l \in L_{\mathbb{A}}. l = \text{nil} \lor l = \text{cons}(\text{hd}(l), \text{tl}(l))$.

These five Peano-style axioms for lists are equivalent to the single property that if $\mathbb{A}$ is a set, $\text{nil} \in \mathbb{A}$ and $\text{cs} : \mathbb{A} \times \mathbb{A} \rightarrow \mathbb{A}$, then there is a unique function $f : L_{\mathbb{A}} \rightarrow \mathbb{A}$ such that $\forall l \in L_{\mathbb{A}}. f(l) = \text{if } l = \text{nil} \text{ then } \text{nil} \text{ else } \text{cs}(\text{hd}(l), f(\text{tl}(l)))$.

A structure $(\mathbb{A}, \text{nil}, \text{cs})$ where $\text{nil} \in \mathbb{A}$ and $\text{cs} : \mathbb{A} \times \mathbb{A} \rightarrow \mathbb{A}$ will be called an $\mathbb{A}$-list algebra. The dual concept is an $\mathbb{A}$-list coalgebra $(C, \text{test}, \text{dest})$ where $C$ is the carrier set and $\text{test} : C \rightarrow \{\ast\}$ and $\text{dest} : C \rightarrow \mathbb{A} \times C$ are destructors whose domains partition the carrier $C$.

Some notation is useful when discussing the dual of the $\mathbb{A}$-list algebra $(L_{\mathbb{A}}, \text{nil}, \text{cons})$.

- For any sets $X_1$, $X_2$, if $(x_1, x_2) \in X_1 \times X_2$ then $\pi_1(x_1, x_2) = x_1$ and $\pi_2(x_1, x_2) = x_2$. The functions $\pi_1 : X_1 \times X_2 \rightarrow X_1$ and $\pi_2 : X_1 \times X_2 \rightarrow X_2$ are called projections.

- If $\theta_1 : X_1 \rightarrow Y_1$ and $\theta_2 : X_2 \rightarrow Y_2$, then $\theta_1 \times \theta_2 : X_1 \times X_2 \rightarrow Y_1 \times Y_2$ is defined by $(\theta_1 \times \theta_2)(x_1, x_2) = (\theta_1(x_1), \theta_2(x_2))$. The function $\theta_1 \times \theta_2$ is called the product of functions $\theta_1$ and $\theta_2$. Note that $(\theta_1 \times \theta_2)(x) = (\theta_1(\pi_1(x)), \theta_2(\pi_2(x)))$.

- If $E$ is an expression containing a variable $n$ (e.g. $E = \sigma(n+1)$), then $\lambda n. E$ denotes the function that when applied to an argument returns the value obtained by evaluating $E$ after the argument has been substituted for $n$, so $\lambda n. \sigma(n+1)$ denotes the function $n \mapsto \sigma(n+1)$.

The dual of the $\mathbb{A}$-list algebra $(L_{\mathbb{A}}, \text{nil}, \text{cons})$ is the $\mathbb{A}$-list coalgebra $(L_{\mathbb{A}}, \text{null}, \text{destcons})$ with the property that for any $\mathbb{A}$-list coalgebra $(C, \text{test}, \text{dest})$, there is exactly one function $g : C \rightarrow L_{\mathbb{A}}$ such that for all $x \in C$: 

13
if \( x \in \text{Dom}(\text{test}) \) then
\[ g(x) \in \text{Dom}(\text{null}) \text{ and } \text{null}(g(x)) = \text{test}(x); \]

if \( x \in \text{Dom}(\text{dest}) \) then
\[ g(x) \in \text{Dom}(\text{destcons}) \text{ and } \text{destcons}(g(x)) = (\text{id} \times g)(\text{dest}(x)). \]

It turns out that the unique existence of \( g \) determines the \( \mathcal{A} \)-list coalgebra \((\mathbb{L}_\mathcal{A}, \text{null}, \text{destcons})\) to have carrier set \( \mathbb{L}_\mathcal{A} = \mathbb{L}_\mathcal{A} \cup \mathbb{A}^N \), where \( \mathbb{A}^N \) is the set of infinite lists of members of \( \mathcal{A} \). Formally \( \mathbb{A}^N = \{ \sigma \mid \sigma : \mathbb{N} \to \mathcal{A} \} \), i.e. infinite lists are represented as functions \( \sigma \) from the natural numbers to \( \mathcal{A} \), with \( \sigma(n) \) being the \( n \)th element of the list \( \sigma \), counting from 0, so \( \sigma(0) \) is the first element. The nullary destructor \( \text{null} : \{ \text{nil} \} \to \{ * \} \) satisfies \( \text{null}(\text{nil}) = * \) and the unary destructor \( \text{destcons} : \{ l \mid l \neq \text{nil} \} \to \mathbb{L}_\mathcal{A} \) is the function that returns the pair \((\text{hd}(l), \text{tl}(l))\) when applied to a non-empty finite list \( l \), and returns the pair \((\sigma(0), \lambda n. \sigma(n+1))\) when applied to an infinite list \( \sigma \).

It is useful to extend \( \text{cons} \), \( \text{hd} \) and \( \text{tl} \) from \( \mathbb{L}_\mathcal{A} \) to all of \( \mathbb{L}_\mathcal{A} \cup \mathbb{A}^N \). For \( \sigma \in \mathbb{A}^N \) define:

\[
\begin{align*}
\text{cons}(a, \sigma) &= \lambda n. \text{if } n = 0 \text{ then } a \text{ else } \sigma(n-1) \\
\text{hd}(\sigma) &= \sigma(0) \\
\text{tl}(\sigma) &= \lambda n. \sigma(n+1)
\end{align*}
\]

With these definitions, the unique function \( g : \mathcal{C} \to \mathbb{L}_\mathcal{A} \) is defined by the single equation:

\[ g(x) = \text{if } \text{test}(x) = * \text{ then } \text{nil} \text{ else } \text{cons}((\text{id} \times g)(\text{dest}(x))) \]

which can also be written as:

\[ g(x) = \text{if } \text{test}(x) = * \text{ then } \text{nil} \text{ else } \text{cons}(\pi_1(\text{dest}(x)), g(\pi_2(\text{dest}(x)))) \]

and is equivalent to:

\[ \text{null}(g(x)) = \text{test}(x) \land \text{hd}(g(x)) = (\pi_1(\text{dest}(x)) \land \text{tl}(g(x)) = g(\pi_2(\text{dest}(x))) \]

Note the ways in which colists are dual to lists:

- constructors \( \text{nil} \in \mathbb{L}_\mathcal{A} \), \( \text{cons} : \mathcal{A} \times \mathbb{L}_\mathcal{A} \to \mathbb{L}_\mathcal{A} \) versus
destackers \( \text{null} : \mathbb{L}_\mathcal{A} \to \{ * \} \), \( \text{destcons} : \mathbb{L}_\mathcal{A} \to \mathcal{A} \times \mathbb{L}_\mathcal{A} \);
- unique \( f : \mathbb{L}_\mathcal{A} \to \mathcal{A} \) versus
unique \( g : \mathcal{C} \to \mathbb{L}_\mathcal{A} \);
- define \( f \) on constructors: \( f(\text{nil}) = \text{nil} \land f(\text{cons}(a, l)) = cs(a, f(l)) \) versus
define destructors on \( g \): \( g(\text{null}(x)) = \text{test}(x) \land g(\text{destcons}(g(x))) = (\text{id} \times g)(\text{dest}(x)) \);
- recursion \( f(l) = \text{if } l = \text{nil} \text{ then } \text{nil} \text{ else } cs(\text{hd}(l), f(\text{tl}(l))) \) versus
corecursion \( g(x) = \text{if } \text{test}(x) = * \text{ then } \text{nil} \text{ else } \text{cons}((\text{id} \times g)(\text{dest}(x))) \).
- recursion always terminates versus
corecursion sometimes doesn’t terminate (see example below).
Example of corecursion for lists

The Peano coalgebra example used above can be reinterpreted as a $\mathbb{L}_\epsilon$ coalgebra.

$\mathfrak{A} = \{A, B, C, D, E, F, G, H, I, J\}$,
$\mathcal{C} = \{A, B, C, D, E, F, G, H, I, J\}$,
$\text{test} = [F \mapsto *, J \mapsto *]$,
$\text{dest} = [A \mapsto (A, A), B \mapsto (B, C), C \mapsto (C, B), D \mapsto (D, E), E \mapsto (E, F),
G \mapsto (G, H), H \mapsto (H, I), I \mapsto (I, J)]$.

$\text{Dom} (\text{test}) = \{F, J\}$ and $\text{Dom} (\text{dest}) = \{A, B, C, D, E, G, H, I\}$, so $\text{Dom} (\text{test})$ and $\text{Dom} (\text{dest})$ partition $\mathcal{C}$.

In the diagram in Figure 1 below: an arrow from $x$ to $x'$ means that if $x \in \text{Dom} (\text{dest})$ then $\text{dest} (x) = (x, x')$, and if $x \in \text{Dom} (\text{test})$ then $\text{test} (x) = *$.

![Diagram of corecursion](image)

Figure 2:

Consider now the definition of $g : \mathcal{C} \rightarrow \mathbb{L}_\epsilon$ specified for $x \in \mathcal{C}$ by $g(x) = \text{if test}(x) = * \text{ then nil else } \text{cons}((\text{id} \times g)(\text{dest}(x)))$.

The notation $[a_0, a_1, \ldots, a_n]$ abbreviates $\text{cons}(a_0, \text{cons}(a_1, \ldots, \text{cons}(a_n, \text{nil}) \ldots))$ and $[\ ]$ is used as a synonym for nil.

Rewriting $g(A)$ with the equation defining $g$ yields:

$g(A) = \text{cons}((\text{id} \times g)(\text{dest}(A))) = \text{cons}((\text{id} \times g)(A, A)) = \text{cons}(A, g(A)) = [A, g(A)]$

The only way this can be satisfied is with $g(A)$ being the infinite list of $A$s, i.e. $g(A) = [A, A, A, \ldots]$. Formally this is the function $\lambda n. A$.

Rewriting $g(B)$ and $g(C)$ yields:
The example just given illustrates this.

\[ g(B) = \text{cons}((\text{id} \times g)(\text{dest}(B))) \]
\[ = \text{cons}((\text{id} \times g)(B, C)) \]
\[ = \text{cons}((\text{id} \times g)(B, g(C))) \]
\[ = \text{cons}([B, C, g(B)]) \]

\[ g(C) = \text{cons}((\text{id} \times g)(\text{dest}(C))) \]
\[ = \text{cons}((\text{id} \times g)(C, B)) \]
\[ = \text{cons}([C, g(B)]) \]
\[ = \text{cons}([C, \text{cons}((\text{id} \times g)(\text{dest}(B)))]) \]
\[ = \text{cons}([C, \text{cons}([B, g(C)])]) \]
\[ = [C, B, g(C)] \]

The only way these can be satisfied is with \( g(B) \) being the infinite list that repeats \( B \) followed by \( C \), i.e. \( g(B) = [B, C, B, C, B, C, B, C, \ldots] \) and \( g(C) \) being the infinite list that repeats \( C \) followed by \( B \), i.e. \( g(C) = [C, B, C, B, C, B, C, B, \ldots] \).

Thus if \( x \in \{A, B, C\} \), then evaluating \( g(x) \) by rewriting with the equation for \( g \) returns an infinite list, i.e. a member of \( \mathbb{A}^\infty \).

On other arguments the rewriting results in a finite list, i.e. a member of \( \mathbb{L}_\mathbb{A} \).

The rewriting calculations below take bigger steps than the ones above (the expansion of \((\text{id} \times g)(\cdot \cdot \cdot)\) is omitted).

\[ g(F) = \text{nil} = [\ ] \]
\[ g(E) = \text{cons}(E, g(F)) = \text{cons}(E, \text{nil}) = [E] \]
\[ g(D) = \text{cons}(D, g(E)) = \text{cons}(D, \text{cons}(E, \text{nil})) = [D, E] \]
\[ g(J) = \text{nil} = [\ ] \]
\[ g(I) = \text{cons}(I, g(J)) = \text{cons}(I, \text{nil}) = [I] \]
\[ g(H) = \text{cons}(H, g(I)) = \text{cons}(H, \text{cons}(I, \text{nil})) = [H, I] \]
\[ g(G) = \text{cons}(G, g(H)) = \text{cons}(G, \text{cons}(H, \text{cons}(I, \text{nil}))) = [G, H, I] \]

These rewriting calculations show that:

\[ g = [A \mapsto [A, A, A, \ldots], B \mapsto [B, C, B, C, B, C, B, C, B, C, B, C, \ldots], C \mapsto [C, B, C, B, C, B, C, B, C, \ldots], D \mapsto [D, E], E \mapsto [E], F \mapsto [\ ], G \mapsto [G, H, I], H \mapsto [H, I], I \mapsto [I], J \mapsto [\ ]] \]

For an arbitrary \( \mathbb{A} \)-list coalgebra \((C, \text{test}, \text{dest})\), the function \( g : C \rightarrow \prod_\mathbb{A} \) satisfying the equation \( g(x) = \text{if test}(x) = * \text{ then nil else cons}((\text{id} \times g)(\text{dest}(x))) \) is described by:

\[
g(x) = \begin{cases} 
[a_0, \ldots, a_{n-1}] \exists x_0 \cdots x_n. \\
\quad x = x_0 \land \text{test}(x_n) = * \land \forall i < n. \text{dest}(x_i) = (a_i, x_{i+1}) \\
[a_0, a_1, a_2, \ldots] \exists \sigma : \mathbb{N} \rightarrow C. x = \sigma(0) \land \forall i. \text{dest}(\sigma(i)) = (a_i, \sigma(i+1))
\end{cases}
\]

The example just given illustrates this.
Coinduction and bisimulation

Induction for natural numbers is the fifth Peano axiom. For lists, it is the fifth of the Peano-like axioms given at the start of the section on Lists and colists above. Both of these are equivalent to the uniqueness of the functions resulting from the principle of recursive definition from \( \mathbb{N} \) or \( \mathbb{L}_\alpha \) to the carriers of the appropriate algebras.

As far as I can discover there is no canonical notion of coinduction for the dual of natural numbers or lists. The term “coinduction” (actually “co-induction”) is generally attributed to Milner and Tofte in their 1991 paper Co-induction in relational semantics whose abstract is:

An application of the mathematical theory of maximum fixed points of monotonic set operators to relational semantics is presented. It is shown how an important proof method which we call co-induction, a variant of Park’s (1969) principle of fixpoint induction, can be used to prove the consistency of the static and the dynamic relational semantics of a small functional programming language with recursive functions.

Milner and Tofte’s paper is based on fixed points, but other more recent work on coinduction is based on terminal algebras, which is the approach taken here (see the sections below entitled least and greatest fixed points and Initial and terminal algebras).

The coinduction principle described here is called here bisimulation coinduction, where a bisimulation is a relation \( R \subseteq \mathbb{N} \times \mathbb{N} \) such that

\[
\text{if } (n_1, n_2) \in R \text{ then either } n_1 = 0 \text{ and } n_2 = 0 \text{ or else } n_1 \neq 0 \text{ and } n_2 \neq 0 \text{ and } (P(n_1), P(n_2)) \in R.
\]

The bisimulation coinduction principle for \( \mathbb{N} \) states that if \( R \) is any bisimulation, then \( R \subseteq \{ (n, n) \mid n \in \mathbb{N} \} \).

Example of bisimulation coinduction for numbers It’s hard to come up with examples for \( \mathbb{N} \) that illustrate useful applications of coinduction. This is because coinduction is actually not much use in practice. The rather contrived example that follows is inspired by part of a more convincing example used later.
to illustrate coinduction on lists. In the example even(n) means that n is an even number (even(0) is considered true) and odd(n) that n is odd.

Consider the unique function $g : \mathbb{N} \to \mathbb{N}$ determined by the Peano coalgebra $\langle \mathbb{N}, \text{isz}, p \rangle$ where $\text{Dom}(\text{isz}) = \{ n \mid \text{even}(n) \}$ and $\text{Dom}(p) = \{ n \mid \text{odd}(n) \}$, and the destructors are defined by $p(n) = \ast \iff \text{even}(n)$ and $s(n) = n+2$. This function $g$ satisfies:

$$g(x) = \text{if } \text{isz}(x) = \ast \text{ then } 0 \text{ else } g(p(x)) + 1$$

With the particular isz and $p$ just specified, this is equivalent to:

$$g(n) = \text{if } \text{even}(n) \text{ then } 0 \text{ else } g(n+2) + 1$$

Intuitively this function returns 0 on even numbers and loops on odd numbers, so is equal to $h : \mathbb{N} \to \mathbb{N}$ defined by: $h(n) = \text{if even}(n) \text{ then } 0 \text{ else } \infty$.

This can be proved by showing that $R = \{ (g(n), h(n)) \mid n \in \mathbb{N} \}$ is a bisimulation.

Suppose $(n_1, n_2) \in R$, then $n_1 = g(n)$ and $n_2 = h(n)$ for some $n \in \mathbb{N}$.

If $n$ is even then $n_1 = g(n) = 0$ and $n_2 = h(n) = 0$.

If $n$ is not even, then $n_1 = g(n+2)+1$ and $n_2 = \infty$, so $n_1 \neq 0$ and $n_2 \neq 0$. Also, if $n$ is not even then $n+2$ is not even, so $P(n_1) = P(g(n)) = P(g(n+2)+1) = g(n+2)$ and $P(n_2) = P(h(n)) = P(\infty) = \infty = h(n+2)$, and so $(P(n_1), P(n_2)) \in R$.

Thus either $n_1 = 0$ and $n_2 = 0$ or $n_1 \neq 0$ and $n_2 \neq 0$ and $(P(n_1), P(n_2)) \in R$, so $R$ is a bisimulation, hence by the bisimulation coinduction principle it follows that $\forall n \in \mathbb{N}, g(n) = h(n)$.

Justification of bisimulation coinduction for numbers  To establish that the uniqueness of corecursively specified functions entails the principle of bisimulation coinduction, let $R \subseteq \mathbb{N} \times \mathbb{N}$ be a bisimulation. Consider the Peano coalgebra $\langle R, \text{isz}_R, p_R \rangle$, where $\text{isz}_R(n_1, n_2) = \ast \iff n_1 = 0 \land n_2 = 0$ and $p_R(n_1, n_2) = (P(n_1), P(n_2))$. The definition of a bisimulation ensures that the domains of $\text{isz}_R$ and $p_R$ partition the coalgebra carrier set $R$. By the defining property of $\langle \mathbb{N}, \text{isz}_0, P \rangle$, there is a unique function $g : R \to \mathbb{N}$ such that for all $(n_1, n_2) \in R$:

$$g(n_1, n_2) = \text{if } \text{isz}_R(n_1, n_2) = \ast \text{ then } 0 \text{ else } g(p_R(n_1, n_2)) + 1$$

i.e. for all $(n_1, n_2) \in R$:

$$g(n_1, n_2) = \text{if } n_1 = 0 \land n_2 = 0 \text{ then } 0 \text{ else } g(P(n_1), P(n_2)) + 1$$

Recall the projection functions: $\pi_1(\sigma_1, \sigma_2) = \sigma_1$ and $\pi_2(\sigma_1, \sigma_2) = \sigma_2$. It is easy to verify the equation for $g$ is satisfied with both $g = \pi_1$ and $g = \pi_2$.

Taking $g = \pi_1$:

$$\pi_1(n_1, n_2) = \text{if } n_1 = 0 \land n_2 = 0 \text{ then } 0 \text{ else } \pi_1(P(n_1), P(n_2)) + 1$$

which simplifies to:
\[ n_1 = \text{if } n_1 = 0 \land n_2 = 0 \text{ then } 0 \text{ else } P(n_1) + 1 \]

which holds for all \((n_1, n_2) \in R\), since if \((n_1, n_1) \in R\) and \(n_1 = 0\) then as \(R\) is a bisimulation \(n_2 = 0\).

Now take \(g = \pi_2\):

\[
\pi_2(n_1, n_2) = \text{if } n_1 = 0 \land n_2 = 0 \text{ then } 0 \text{ else } \pi_2(P(n_1), P(n_2)) + 1
\]

which simplifies to:

\[
 n_2 = \text{if } n_1 = 0 \land n_2 = 0 \text{ then } 0 \text{ else } P(n_2) + 1
\]

which also holds for all \((n_1, n_2) \in R\).

Since \(g\) is unique, \(\pi_1 : R \to \mathbb{N}\) and \(\pi_2 : R \to \mathbb{N}\) must be the same function, so if \((n_1, n_2) \in R\) then \(n_1 = \pi_1(n_1, n_2) = \pi_2(n_1, n_2) = n_2\).

The argument just given shows that the bisimulation coinduction principle follows from the uniqueness of the function \(g : C \to \mathbb{N}\) corecursively specified by:

\[
g(x) = \text{if } \text{isz}(x) = * \text{ then } 0 \text{ else } g(p(x)) + 1
\]

To prove that the bisimulation coinduction principle entails the uniqueness of corecursively specified functions, suppose that:

\[
g_1(x) = \text{if } \text{isz}(x) = * \text{ then } 0 \text{ else } g_1(p(x)) + 1
\]
\[
g_2(x) = \text{if } \text{isz}(x) = * \text{ then } 0 \text{ else } g_2(p(x)) + 1
\]

then it’s easy to see that \(R\), where \(R = \{(g_1(x), g_2(x)) \mid x \in C\}\), is a bisimulation.

If \((n_1, n_2) \in R\) then \(n_1 = g_1(x)\) and \(n_2 = g_2(x)\) for some \(x \in C\).

If \(\text{isz}(x) = \ast\), then \(n_1 = g_1(x) = 0\) and \(n_2 = g_2(x) = 0\).

If \(\text{isz}(x) \neq \ast\), then \(n_1 = g_1(x) = g_1(p(x)) + 1\) and \(n_2 = g_2(x) = g_2(p(x)) + 1\), so \(n_1 \neq 0\) and \(n_2 \neq 0\). Also, if \(\text{isz}(x) \neq \ast\), then \(P(n_1) = P(g_1(x)) = P(g_1(p(x)) + 1) = g_1(p(x))\) and \(P(n_2) = P(g_2(x)) = P(g_2(p(x)) + 1) = g_2(p(x))\), and so \((P(n_1), P(n_2)) \in R\).

Thus either \(n_1 = 0\) and \(n_2 = 0\) or \(n_1 \neq 0\) and \(n_2 \neq 0\) and \((P(n_1), P(n_2)) \in R\), so \(R\) is a bisimulation, hence by the bisimulation coinduction principle: \(\forall x \in C. g_1(x) = g_2(x)\).

**Bisimulation coinduction for lists**

A bisimulation on \(\Sigma_N\) is a relation \(R \subseteq \Sigma_N \times \Sigma_N\) such that if \((\sigma_1, \sigma_2) \in R\) then either \(\sigma_1 = \text{nil}\) and \(\sigma_2 = \text{nil}\) or else \(\sigma_1 \neq \text{nil}\) and \(\sigma_2 \neq \text{nil}\) and \(hd(\sigma_1) = hd(\sigma_2)\) and \((\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R\).

The bisimulation coinduction principle for \(\Sigma_N\) states that if \(R\) is any bisimulation, then \(R \subseteq \{(\sigma, \sigma) \mid \sigma \in \Sigma_N\}\).
Examples of bisimulation coinduction for lists  

The examples here are adapted from similar ones in *An introduction to (co)algebra and (co)induction* by Bart Jacobs and Jan Rutten, except here lists can be finite or infinite, but in Jacobs & Rutten they are only infinite.

If $\sigma \in \mathbb{L}_A$ — i.e. $\sigma$ is a finite or infinite list — then $g_{\text{even}}(\sigma)$ is the sublist consisting of those elements at even numbered positions and $g_{\text{odd}}(\sigma)$ is the sublist consisting of those elements at odd numbered positions.

\[
\begin{align*}
\sigma &: \ a_0 \ a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a_6 \ a_7 \ a_8 \ a_9 \ a_{10} \ a_{11} \ \cdots \\
g_{\text{even}}(\sigma) &: \ a_0 \ a_2 \ a_4 \ a_6 \ a_8 \ a_{10} \ a_{12} \ \cdots \\
g_{\text{odd}}(\sigma) &: \ a_1 \ a_3 \ a_5 \ a_7 \ a_9 \ a_{11} \ \cdots 
\end{align*}
\]

The functions $g_{\text{even}}$ and $g_{\text{odd}}$ are defined by corecursion below, and then two lemmas are proved by bisimulation coinduction:

**Lemma 1.** $\forall \sigma \in \mathbb{L}_A. \ g_{\text{odd}}(\sigma) = g_{\text{even}}(\text{tl}(\sigma))$

**Lemma 2.** $\forall \sigma \in \mathbb{L}_A. \ \sigma \neq \text{nil} \Rightarrow \ \text{tl}(g_{\text{even}}(\sigma)) = g_{\text{odd}}(\text{tl}(\sigma))$

Next $\text{merge}(\sigma_1, \sigma_2)$ is defined by corecursion to be the interleaving of $\sigma_1$ and $\sigma_2$. Using these two lemmas, it is then shown by bisimulation coinduction that $\text{merge}(g_{\text{even}}(\sigma), g_{\text{odd}}(\sigma)) = \sigma$.

To define $g_{\text{even}}$ and $g_{\text{odd}}$ consider the following $\mathbb{A}$-list coalgebras:

\[
\begin{align*}
C_{\text{even}} &= (\mathbb{L}_A, \text{test}_{\text{even}}, \text{dest}_{\text{even}}) \\
C_{\text{odd}} &= (\mathbb{L}_A, \text{test}_{\text{odd}}, \text{dest}_{\text{odd}})
\end{align*}
\]

where

\[
\begin{align*}
\text{test}_{\text{even}}(\sigma) &= * \Leftrightarrow \sigma = \text{nil} \\
\text{test}_{\text{odd}}(\sigma) &= * \Leftrightarrow \sigma = \text{nil} \text{ or } \text{tl}(\sigma) = \text{nil}
\end{align*}
\]

and

\[
\begin{align*}
\text{dest}_{\text{even}}(\sigma) &= (\text{hd}(\sigma), \text{if } \text{tl}(\sigma) = \text{nil} \text{ then } \text{nil} \text{ else } \text{tl}(\text{tl}(\sigma)))) \\
\text{dest}_{\text{odd}}(\sigma) &= (\text{hd}(\text{tl}(\sigma)), \text{tl}(\text{tl}(\sigma)))
\end{align*}
\]

Recall the general form of the unique corecursively specified function $g : C \rightarrow \mathbb{L}_A$ from the carrier of a coalgebra $(C, \text{test}, \text{dest})$ to the carrier of $(\mathbb{L}_A, \text{null}, \text{destcons})$:

\[
g(x) = \text{if } \text{test}(x) = * \text{ then } \text{nil} \text{ else } \text{cons}((\text{id} \times g)(\text{dest}(x)))
\]

For the coalgebras $C_{\text{even}}$ and $C_{\text{odd}}$, this general schema instantiates, respectively, to:

\[
\begin{align*}
g_{\text{even}}(\sigma) &= \text{if } \sigma = \text{nil} \\
& \quad \text{ then } \text{nil} \\
& \quad \text{ else } \text{cons}(\text{hd}(\sigma), g_{\text{even}}(\text{if } \text{tl}(\sigma) = \text{nil} \text{ then } \text{nil} \text{ else } \text{tl}(\text{tl}(\sigma)))))
\end{align*}
\]

\[
\begin{align*}
g_{\text{odd}}(\sigma) &= \text{if } \sigma = \text{nil} \text{ or } \text{tl}(\sigma) = \text{nil} \\
& \quad \text{ then } \text{nil} \\
& \quad \text{ else } \text{cons}(\text{hd}(\text{tl}(\sigma)), g_{\text{odd}}(\text{tl}(\text{tl}(\sigma))))
\end{align*}
\]

20
These equations look intuitively correct.

To prove Lemma 1: \( \forall \sigma \in \mathbb{L}_A. g_{\text{odd}}(\sigma) = g_{\text{even}}(\text{tl}(\sigma)) \), let \( R = \{(g_{\text{odd}}(\sigma), g_{\text{even}}(\text{tl}(\sigma))) \mid \sigma \in \mathbb{L}_A\} \). It is shown below that \( R \) is a bisimulation.

If \((\sigma_1, \sigma_2) \in R\), then \(\sigma_1 = g_{\text{odd}}(\sigma)\) and \(\sigma_2 = g_{\text{even}}(\text{tl}(\sigma))\) for some \(\sigma \in \mathbb{L}_A\). Two cases needed to be considered.

1. If \(\sigma = \text{nil}\) or \(\text{tl}(\sigma) = \text{nil}\) then \(\sigma_1 = \sigma_2 = \text{nil}\) by the definitions of \(g_{\text{even}}\) and \(g_{\text{odd}}\).

2. If \(\sigma \neq \text{nil}\) and \(\text{tl}(\sigma) \neq \text{nil}\) then \(\sigma_1 = g_{\text{odd}}(\sigma) = \text{cons}(\text{hd}(\text{tl}(\sigma)), g_{\text{odd}}(\text{tl}(\text{tl}(\sigma))))\)
   and \(\sigma_2 = g_{\text{even}}(\text{tl}(\sigma)) = \text{cons}(\text{hd}(\text{tl}(\sigma)), g_{\text{even}}(\text{tl}(\text{tl}(\sigma))))\)
   by the definitions of \(g_{\text{odd}}\) and \(g_{\text{even}}\), respectively. Hence \(\text{hd}(\sigma_1) = \text{hd}(\sigma_2)\)
   and \(\text{tl}(\sigma_1) = g_{\text{odd}}(\text{tl}(\sigma))\) and \(\text{tl}(\sigma_2) = g_{\text{even}}(\text{tl}(\text{tl}(\sigma)))\).
   Thus \((\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R\).

As \((\sigma_1, \sigma_2) \in R\) if either \(\sigma_1 = \sigma_2 = \text{nil}\) or else \(\sigma_1 \neq \text{nil}\) and \(\sigma_2 \neq \text{nil}\) and \(\text{hd}(\sigma_1) = \text{hd}(\sigma_2)\) and \((\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R\), it follows that \(R\) is a bisimulation.

To prove Lemma 2: \(\sigma \neq \text{nil} \Rightarrow \text{tl}(g_{\text{even}}(\sigma)) = g_{\text{odd}}(\text{tl}(\sigma))\), let \( R = \{(\text{tl}(g_{\text{even}}(\sigma)), g_{\text{odd}}(\text{tl}(\sigma))) \mid \sigma \in \mathbb{L}_A \land \sigma \neq \text{nil}\} \). It is shown below that \(R\) is a bisimulation.

If \((\sigma_1, \sigma_2) \in R\), then \(\sigma_1 = \text{tl}(g_{\text{even}}(\sigma))\) and \(\sigma_2 = g_{\text{odd}}(\text{tl}(\sigma))\) for some \(\sigma \neq \text{nil}\). Three cases needed to be considered.

1. If \(\text{tl}(\sigma) = \text{nil}\) then \(\sigma_1 = \sigma_2 = \text{nil}\) by the definitions of \(g_{\text{even}}\) and \(g_{\text{odd}}\).

2. If \(\text{tl}(\sigma) \neq \text{nil}\) and \(\text{tl}(\text{tl}(\sigma)) = \text{nil}\) then \(\sigma_1 = \text{tl}(g_{\text{even}}(\sigma)) = g_{\text{even}}(\text{tl}(\text{tl}(\sigma))) = \text{nil}\)
   and \(\sigma_2 = g_{\text{odd}}(\text{tl}(\sigma)) = \text{nil}\) by the definitions of \(g_{\text{odd}}\) and \(g_{\text{even}}\), respectively.

3. If \(\text{tl}(\sigma) \neq \text{nil}\) and \(\text{tl}(\sigma) \neq \text{nil}\) and \(\text{tl}(\sigma) \neq \text{nil}\) then
   \(\sigma_1 = \text{tl}(g_{\text{even}}(\sigma)) = g_{\text{even}}(\text{tl}(\text{tl}(\sigma))) = \text{cons}(\text{hd}(\text{tl}(\text{tl}(\sigma))), g_{\text{even}}(\text{if} - \text{then} - \text{else}))\)
   and \(\sigma_2 = g_{\text{odd}}(\text{tl}(\sigma)) = \text{cons}(\text{hd}(\text{tl}(\text{tl}(\sigma))), g_{\text{odd}}(\text{tl}(\text{tl}(\sigma))))\)
   by the definitions of \(g_{\text{odd}}\) and \(g_{\text{even}}\). Hence \(\text{hd}(\sigma_1) = \text{hd}(\sigma_2)\) and \(\text{tl}(\sigma_1) = \text{tl}(g_{\text{even}}(\text{tl}(\sigma)))\)
   and \(\text{tl}(\sigma_2) = g_{\text{odd}}(\text{tl}(\text{tl}(\sigma)))\). Thus \((\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R\).

As \((\sigma_1, \sigma_2) \in R\) if either \(\sigma_1 = \sigma_2 = \text{nil}\) or else \(\sigma_1 \neq \text{nil}\) and \(\sigma_2 \neq \text{nil}\) and \(\text{hd}(\sigma_1) = \text{hd}(\sigma_2)\) and \((\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R\), it follows that \(R\) is a bisimulation.

The function \(\text{merge} : \mathbb{L}_A \times \mathbb{L}_A \to \mathbb{L}_A\) interleaves two lists. It will be proved by bisimulation coinduction that \(\forall \sigma \in \mathbb{L_A}. \text{merge}(g_{even}(\sigma), g_{odd}(\sigma)) = \sigma\). Before proving this, the function \(\text{merge}\) needs to be defined. The natural recursion to achieve this is:
merge(σ₁, σ₂) =
if σ₁ = nil
  then σ₂
else
  if tl(σ₁) = nil
    then cons(hd(σ₁), σ₂)
  else cons(hd(σ₁), merge(σ₂, tl(σ₁)))

To make this fit the corecursion format:

\[ g(x) = \begin{cases} \text{nil} & \text{if } test(x) = \ast \\ \text{cons}(\text{id} \times g)(dest(x)) & \text{else} \end{cases} \]

where, \( x \) ranges over pairs \( (σ₁, σ₂) \) of lists, the destructors \( test \) and \( dest \) need to be defined. To achieve this the equation for \( merge \) can be reformulated to:

merge(σ₁, σ₂) =
if σ₁ = nil and σ₂ = nil
  then nil
else
  if σ₁ = nil
    then cons(hd(σ₂), merge(σ₁, tl(σ₂)))
  else cons(hd(σ₁), merge(σ₂, tl(σ₁)))

This reformulated equation is shown equivalent to the original equation below.

The reformulated version becomes an instance of

\[ g(x) = \begin{cases} \text{nil} & \text{if } test(x) = \ast \\ \text{cons}(\text{id} \times g)(dest(x)) & \text{else} \end{cases} \]

if \( g = \text{merge} \) and \( test : \{\text{nil}\} \times \{\text{nil}\} \rightarrow \{\ast\} \) is defined by:

\[ test(σ₁, σ₂) = \ast \iff σ₁ = \text{nil} \text{ and } σ₂ = \text{nil} \]

and \( dest : \{(σ₁, σ₂) | σ₁ \neq \text{nil} \text{ or } σ₂ \neq \text{nil}\} \rightarrow \mathcal{A} \times (\mathcal{L}_\mathbb{A} \times \mathcal{L}_\mathbb{A}) \) by:

\[ dest(σ₁, σ₂) = \begin{cases} (\text{nil}, (σ₁, \text{tl}(σ₂))) & \text{if } σ₁ = \text{nil} \\ (\text{hd}(σ₂), (σ₁, \text{tl}(σ₂))) & \text{else} \end{cases} \]

The reformulated equation for \( merge \) is then the unique function from the carrier of the coalgebra \( (\mathcal{L}_\mathbb{A} \times \mathcal{L}_\mathbb{A}, test, dest) \) to the carrier of the coalgebra \( (\mathcal{L}_\mathbb{A}, \text{null}, dests) \).

The original recursion for \( merge \) can be derived from the reformulated equation using \( σ₂ = \text{cons}(\text{hd}(σ₂), \text{tl}(σ₂)) \) and \( merge(\text{nil}, \text{tl}(σ₂)) = \text{tl}(σ₂) \), where the latter is an instance of \( \forall σ \in \mathcal{L}_\mathbb{A}. \text{merge}(\text{nil}, σ) = σ \), which is proved by bisimulation coinduction by showing the \( R = \{(\text{merge}(\text{nil}, σ), σ) | σ \in \mathcal{L}_\mathbb{A}\} \) is a bisimulation. To show this let \( (σ₁, σ₂) \in R \), then \( σ₁ = \text{merge}(\text{nil}, σ) \) and \( σ₂ = σ \) for some \( σ \in \mathcal{L}_\mathbb{A} \).

If \( σ = \text{nil} \), then \( σ₁ = σ₂ = \text{nil} \). If \( σ \neq \text{nil} \) then \( σ₁ = \text{cons}(\text{hd}(σ), \text{merge}(\text{nil}, \text{tl}(σ))) \), so \( \text{hd}(σ₁) = \text{hd}(σ) \) and \( \text{tl}(σ₁) = \text{merge}(\text{nil}, \text{tl}(σ)) \). Thus either \( σ₁ = σ₂ = \text{nil} \) or else \( σ₁ \neq \text{nil} \) and \( σ₂ \neq \text{nil} \) and \( \text{hd}(σ₁) = \text{hd}(σ₂) \) and \( (\text{tl}(σ₁), \text{tl}(σ₂)) \in R \), so \( R \) is a bisimulation.
To prove $\text{merge}(g_{\text{even}}(\sigma), g_{\text{odd}}(\sigma)) = \sigma$ for arbitrary $\sigma \in \mathbb{I}_\mathcal{A}$, it is sufficient to show that $R = \{(\text{merge}(g_{\text{even}}(\sigma), g_{\text{odd}}(\sigma)), \sigma) | \sigma \in \mathbb{I}_\mathcal{A}\}$ is a bisimulation. The argument follows.

If $(\sigma_1, \sigma_2) \in R$, then $\sigma_1 = \text{merge}(g_{\text{even}}(\sigma), g_{\text{odd}}(\sigma))$ and $\sigma_2 = \sigma$ for some $\sigma \in \mathbb{I}_\mathcal{A}$.

If $\sigma = \text{nil}$ then $\sigma_1 = \text{merge}(\text{nil}, \text{nil}) = \text{nil}$ and $\sigma_2 = \sigma = \text{nil}$.

If $\sigma \neq \text{nil}$ then $g_{\text{even}}(\sigma) \neq \text{nil}$ and $\text{hd}(\sigma_1) = \text{hd}(g_{\text{even}}(\sigma)) = \text{hd}(\sigma) = \text{hd}(\sigma_2)$. Also, $\text{tl}(\sigma_1) = \text{merge}(g_{\text{odd}}(\sigma), \text{tl}(g_{\text{even}}(\sigma))) = \text{merge}(g_{\text{even}}(\text{tl}(\sigma)), g_{\text{even}}(\text{tl}(\sigma)))$. As $\sigma \neq \text{nil}$, $\text{tl}(g_{\text{even}}(\sigma)) = g_{\text{odd}}(\sigma)$, so $\text{tl}(\sigma_1) = \text{merge}(g_{\text{even}}(\text{tl}(\sigma)), g_{\text{odd}}(\text{tl}(\sigma)))$. Clearly $\text{tl}(\sigma_2) = \text{tl}(\sigma)$, thus $\text{hd}(\sigma_1) = \text{hd}(\sigma_2)$ and $(\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R$, so $R$ is a bisimulation.

**Justification of bisimulation coinduction for lists** A bisimulation on $\mathbb{I}_\mathcal{A}$ is a relation $R \subseteq \mathbb{I}_\mathcal{A} \times \mathbb{I}_\mathcal{A}$ such that $(\sigma_1, \sigma_2) \in R$ if either $\sigma_1 = \text{nil}$ and $\sigma_2 = \text{nil}$ or else $\sigma_1 \neq \text{nil}$ and $\sigma_2 \neq \text{nil}$ and $\text{hd}(\sigma_1) = \text{hd}(\sigma_2)$ and $(\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R$.

To establish that the uniqueness of corecurvably specified functions entails the principle of bisimulation coinduction, let $R \subseteq \mathbb{I}_\mathcal{A} \times \mathbb{I}_\mathcal{A}$ be a bisimulation. Define the $\mathcal{A}$-list coalgebra $(R, \text{test}_R, \text{dest}_R)$ by: $\text{test}_R(\sigma_1, \sigma_2) = * \iff \sigma_1 = \text{nil} \land \sigma_2 = \text{nil}$ and $\text{dest}_R(\sigma_1, \sigma_2) = (\text{hd}(\sigma_1), (\text{tl}(\sigma_1), \text{tl}(\sigma_2)))$. Note that if $(\sigma_1, \sigma_2) \in R$ then $\text{hd}(\sigma_1) = \text{hd}(\sigma_2)$, so in the definition of $\text{dest}_R$ in the last sentence $\text{hd}(\sigma_1)$ could have been $\text{hd}(\sigma_2)$.

The definition of a bisimulation ensures that the domains of $\text{test}_R$ and $\text{dest}_R$ partition the coalgebra carrier set $R$. By the defining property of $(\mathbb{I}_\mathcal{A}, \text{null}, \text{destcons})$, there is a unique function $g : R \to \mathbb{I}_\mathcal{A}$ such that for all $(\sigma_1, \sigma_2) \in R$:

$$g(\sigma_1, \sigma_2) = \text{if} \ test_R(\sigma_1, \sigma_2) = * \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}((\text{id} \times g)(\text{dest}_R(\sigma_1, \sigma_2)))$$

i.e. for all $(\sigma_1, \sigma_2) \in R$:

$$g(\sigma_1, \sigma_2) = \text{if} \ \sigma_1 = \text{nil} \ \land \ \sigma_2 = \text{nil} \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}(\text{hd}(\sigma_1), g(\text{tl}(\sigma_1), \text{tl}(\sigma_2)))$$

It is easy to verify the equation for $g$ is satisfied with both $g = \pi_1$ and $g = \pi_2$. Taking $g = \pi_1$:

$$\pi_1(\sigma_1, \sigma_2) = \text{if} \ \sigma_1 = \text{nil} \ \land \ \sigma_2 = \text{nil} \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}(\text{hd}(\sigma_1), \pi_1(\text{tl}(\sigma_1), \text{tl}(\sigma_2)))$$

which simplifies to:

$$\sigma_1 = \text{if} \ \sigma_1 = \text{nil} \ \land \ \sigma_2 = \text{nil} \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}(\text{hd}(\sigma_1), \text{tl}(\sigma_1))$$

which holds for all $(\sigma_1, \sigma_2) \in R$. Now take $g = \pi_2$:

$$\pi_2(\sigma_1, \sigma_2) = \text{if} \ \sigma_1 = \text{nil} \ \land \ \sigma_2 = \text{nil} \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}(\text{hd}(\sigma_1), \pi_2(\text{tl}(\sigma_1), \text{tl}(\sigma_2)))$$

which – since if $(\sigma_1, \sigma_2) \in R$ then $\text{hd}(\sigma_1) = \text{hd}(\sigma_2)$ – simplifies to:

$$\sigma_2 = \text{if} \ \sigma_1 = \text{nil} \ \land \ \sigma_2 = \text{nil} \ \text{then} \ \text{nil} \ \text{else} \ \text{cons}(\text{hd}(\sigma_2), \text{tl}(\sigma_2))$$

which also holds for all $(\sigma_1, \sigma_2) \in R$. 

23
Since \( g \) is unique, \( \pi_1 : R \to \Sigma_\mathcal{A} \) and \( \pi_2 : R \to \Sigma_\mathcal{A} \) must be the same function, so if \( (\sigma_1, \sigma_2) \in R \) then \( \sigma_1 = \pi_1(\sigma_1, \sigma_2) = \pi_2(\sigma_1, \sigma_2) = \sigma_2 \).

The argument just given shows that the bisimulation coinduction principle follows from the uniqueness of the function \( g : \mathcal{C} \to \Sigma_\mathcal{A} \) corecursively specified by:

\[
g(x) = \begin{cases} 
\text{if } test(x) = \ast & \text{then nil} \\
\text{else } \text{cons}((\text{id} \times g)(\text{dest}(x))) 
\end{cases}
\]

To prove that the bisimulation coinduction principle entails the uniqueness of corecursively specified functions, suppose that:

\[
g_1(x) = \begin{cases} 
\text{if } test(x) = \ast & \text{then nil} \\
\text{else } \text{cons}((\text{id} \times g_1)(\text{dest}(x))) 
\end{cases}
\]

\[
g_2(x) = \begin{cases} 
\text{if } test(x) = \ast & \text{then nil} \\
\text{else } \text{cons}((\text{id} \times g_2)(\text{dest}(x))) 
\end{cases}
\]

then it’s easy to see that \( R \), where \( R = \{(g_1(x), g_2(x)) \mid x \in \mathcal{C}\} \), is a bisimulation.

If \( (\sigma_1, \sigma_2) \in R \) then \( \sigma_1 = g_1(x) \) and \( \sigma_2 = g_2(x) \) for some \( x \in \mathcal{C} \).

If \( test(x) = \ast \), then \( \sigma_1 = g_1(x) = \text{nil} \) and \( \sigma_2 = g_2(x) = \text{nil} \).

If \( test(x) \neq \ast \), then \( \sigma_1 = g_1(x) = \text{cons}((\text{id} \times g_1)(\text{dest}(x))) = \text{cons}(\pi_1(\text{dest}(x)), g_1(\pi_2(\text{dest}(x)))) \)
and \( \sigma_2 = g_2(x) = \text{cons}((\text{id} \times g_2)(\text{dest}(x))) = \text{cons}(\pi_1(\text{dest}(x)), g_2(\pi_2(\text{dest}(x)))) \),
so \( \sigma_1 \neq \text{nil} \) and \( \sigma_2 \neq \text{nil} \). Also, if \( \text{hd}(\sigma_1) = \text{hd}(g_1(x)) = \pi_1(\text{dest}(x)) \) and \( \text{hd}(\sigma_2) = \text{hd}(g_2(x)) = \pi_1(\text{dest}(x)) \), so \( \text{hd}(\sigma_1) = \text{hd}(\sigma_2) \) and \( \text{tl}(\sigma_1) = \text{tl}(g_1(x)) = g_1(\pi_2(\text{dest}(x))) \)
and \( \text{tl}(\sigma_2) = \text{tl}(g_2(x)) = g_2(\pi_2(\text{dest}(x))) \), hence \( (\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R \).

Thus either \( \sigma_1 = \text{nil} \) and \( \sigma_2 = \text{nil} \) or else \( \sigma_1 \neq \text{nil} \) and \( \sigma_2 \neq \text{nil} \) and \( \text{hd}(\sigma_1) = \text{hd}(\sigma_2) \)
and \( (\text{tl}(\sigma_1), \text{tl}(\sigma_2)) \in R \), so \( R \) is a bisimulation.

\section*{\( \mathbb{F} \)-algebras and \( \mathbb{F} \)-coalgebras}

\( \mathbb{F} \)-algebras and \( \mathbb{F} \)-coalgebras are a uniform framework with numbers and lists being special cases. \textit{An introduction to (co)algebra and (co)induction} by Bart Jacobs and Jan Rutten is a great tutorial, so only an outline of some of the core ideas is given here – just enough to explain how the particular number and list algebras and coalgebras described above fit into the framework.

The \( \mathbb{F} \) in \( \mathbb{F} \)-algebras and \( \mathbb{F} \)-coalgebras is an operator that maps a set \( X \), the algebra or coalgebra carrier, to a disjoint union of sets that represents the arities of the operators – constructors for algebras and destructors for coalgebras.

\section*{Set theory notation}

The examples of \( \mathbb{F} \) below use the following set theory concepts and notation.

- The function \( \text{id}_X : X \to X \) is the identity: \( \forall x \in X, \text{id}_X(x) = x \).
• If \( \theta_1 : X \to Y \) and \( \theta_2 : Y \to Z \), then \( \theta_2 \circ \theta_1 : X \to Z \) is the function composition defined by \( \forall x \in X. (\theta_2 \circ \theta_1)(x) = \theta_2(\theta_1(x)) \). Note that \( \text{id}_Y \circ \theta_1 = \theta_1 \) and \( \theta_1 \circ \text{id}_X = \theta_1 \).

• The disjoint union of sets \( X \) and \( Y \) is just the union \( X \cup Y \) when \( X \) and \( Y \) are disjoint. This is the case for the examples here. If \( X \) and \( Y \) have elements in common, then they are ‘forced’ to be disjoint ... but details of how this is done are not needed here.

• \( X + Y \) denotes the disjoint union of \( X \) and \( Y \). If \( x \in X + Y \) then either \( x \in X \) or \( x \in Y \), but not both. \( X + Y \) is sometimes called the sum of \( X \) and \( Y \).

• If \( \theta_1 : X_1 \to Y_1 \) and \( \theta_2 : X_2 \to Y_2 \), then \( \theta_1 + \theta_2 : X_1 + X_2 \to Y_1 + Y_2 \) is defined by: \( (\theta_1 + \theta_2)(x) = \text{if } x \in X_1 \text{ then } \theta_1(x) \text{ else } \theta_2(x) \).

• \( 1 \) denotes the single-element set \( \{ \ast \} \). It’s assumed that \( \ast \) isn’t a member of any of the carrier sets in the examples, so that the sums in the definitions of \( \mathbb{F}_N \) and \( \mathbb{F}_{L_a} \) below are between disjoint sets.

**Numbers and lists**

The particular \( \mathbb{F}s \) for natural numbers and lists are \( \mathbb{F}_N \) and \( \mathbb{F}_{L_a} \), defined by:

\[
\begin{align*}
\mathbb{F}_N(X) &= 1 + X \\
\mathbb{F}_{L_a}(X) &= 1 + (\mathfrak{A} \times X)
\end{align*}
\]

The \( \mathbb{F} \) lists that are only infinite is:

\[
\mathbb{F}_{\mathbb{N}^\omega}(X) = \mathfrak{A} \times X
\]

In general, \( \mathbb{F}(X) \) is a ‘polynomial’ built out of \( X \) and other sets (e.g. \( 1 \) and \( \mathfrak{A} \) in the examples above) using disjoint sum and Cartesian product.

An \( \mathbb{F} \)-algebra is a pair \((\mathcal{A},a)\) where \( a : \mathbb{F}(\mathcal{A}) \to \mathcal{A} \).

The \( \mathbb{F}_N \)-algebra \( a : \mathbb{F}_N(\mathcal{A}) \to \mathcal{A} \) represents the Peano algebra \((\mathcal{A}, z, s)\) where \( a \) is the function defined by: \( a(\ast) = z \) and \( a(x) = s(x) \) when \( x \in \mathcal{A} \).

The \( \mathbb{F}_{L_a} \)-algebra \( a : \mathbb{F}_{L_a}(\mathcal{A}) \to \mathcal{A} \) represents the \( \mathfrak{A} \)-list algebra \((\mathcal{A}, \text{nl}, \text{cs})\) where \( a \) is the function defined by: \( a(\ast) = \text{nl} \) and \( a(a,x) = \text{cs}(a,x) \) when \( (a,x) \in \mathfrak{A} \times \mathcal{A} \).

Note how the nullary operators – the distinguished elements \( z \) and \( \text{nl} \) – are represented as function from \( 1 \) to the carrier.

An \( \mathbb{F} \)-coalgebra is a pair \((\mathcal{C},c)\) where \( c : \mathcal{C} \to \mathbb{F}(\mathcal{C}) \).

The \( \mathbb{F}_N \)-coalgebra \( c : \mathcal{C} \to \mathbb{F}_N(\mathcal{C}) \) represents the Peano coalgebra \((\mathcal{C}, \text{isz}, p)\) where \( c \) is the function defined by: \( c(x) = \ast \) when \( x \in \text{Dom}(\text{isz}) \) – i.e. \( \text{isz}(x) = \ast \) – and \( c(x) = p(x) \) when \( x \in \text{Dom}(p) \). This works because the domains of the destructors \( \text{isz} \) and \( p \) partition the carrier set \( \mathcal{C} \).
The $F_{\mathbb{N}}$-coalgebra $c : C \rightarrow F_{\mathbb{N}}(C)$ represents the $\mathbb{N}$-list algebra $(C, test, dest)$ where $c$ is the function defined by: $c(x) = \star$ when $x \in \text{Dom}(test)$ – i.e. $test(x) = \star$ – and $c(x) = dest(x)$ when $x \in \text{Dom}(dest)$. This works because the domains of the destructors $test$ and $dest$ partition the carrier set $C$.

Notice the duality: algebra $a : F(A) \rightarrow A$ versus coalgebra $c : C \rightarrow F(C)$.

**Morphisms**

The concept of a *morphism* is needed to generalise the unique function properties characterising conumbers and colists. To say what a morphism is, $F$ operators are defined on functions as well as on sets.

If $\theta : X \rightarrow Y$ then $F(\theta) : F(X) \rightarrow F(Y)$ is the natural extension of $\theta$ as illustrated by the following examples.

- If $X = Y = 1$ then necessarily $\theta = \text{id}_1$ and then $F(\theta) = F(\text{id}_1) = \text{id}_1$.
- If $F(X) = 1 + X$ then $F(\theta) : 1 + X \rightarrow 1 + Y$ and $F(\theta) = \text{id}_1 + \theta$.
- If $F(X) = 1 + (\mathbb{N} \times X)$ then $F(\theta) : 1 + (\mathbb{N} \times X) \rightarrow 1 + (\mathbb{N} \times Y)$ and $F(\theta) = \text{id}_1 + (\text{id}_N \times \theta)$.

A function $f : A_1 \rightarrow A_2$ is a morphism from an $F$-algebra $(A_1, a_1)$ to an $F$-algebra $(A_2, a_2)$ if and only if $f \circ a_1 = a_2 \circ F(f)$.

To illustrate the definition of an $F$-algebra morphism, consider an $F_N$-algebra morphism $f : A_1 \rightarrow A_2$ from an $F_N$-algebra $(A_1, a_1)$ corresponding to the Peano algebra $(A_1, z_1, s_1)$ to an $F_N$-algebra $(A_2, a_2)$ corresponding to the Peano algebra $(A_2, z_2, s_2)$.

The condition for $f$ to be an $F_N$-algebra morphism is $f \circ a_1 = a_2 \circ F_N(f)$.

Expanding the definition of $F_N(f)$ converts this equation to $f \circ a_1 = a_2 \circ (\text{id}_1 + f)$, which means $\forall x \in (1 + A_1). f(a_1(x)) = a_2((\text{id}_1 + f)(x))$.

Now, if $x \in (1 + A_1)$ then either $x \in 1$ or $x \in A_1$, so there are two cases to consider.

i. If $x \in 1$ then $x = \star$ and $a_1(x) = z_1$ so $f(a_1(x)) = f(z_1)$. If $x = \star$ then $(\text{id}_1 + f)(x) = \text{id}_1(x) = x = \star$, so $a_2((\text{id}_1 + f)(x)) = a_2(\star) = z_2$. Thus the equation $f(a_1(x)) = a_2((\text{id}_1 + f)(x))$ reduces to $f(z_1) = z_2$.

ii. If $x \in A_1$ then $a_1(x) = s_1(x)$, so $f(a_1(x)) = f(s_1(x))$. If $x \in A_1$ then $(\text{id}_1 + f)(x) = f(x)$, so $a_2((\text{id}_1 + f)(x)) = a_2(f(x)) = s_2(f(x))$. Thus the equation $f(a_1(x)) = a_2((\text{id}_1 + f)(x))$ reduces to $f(s_1(x)) = s_2(f(x))$. 

26
Thus a morphism from the $\mathbb{F}_\mathbb{N}$-algebra corresponding to the natural numbers $(\mathbb{N}, 0, S)$ to an $\mathbb{F}_\mathbb{N}$-algebra corresponding to $(\mathcal{A}, z, s)$ is a function $f : \mathbb{N} \to \mathcal{A}$ such that $f(0) = z$ and $\forall n \in \mathbb{N}. f(S(n)) = s(f(n))$, i.e.: $f(n) = \text{if } n=0 \text{ then } z \text{ else } s(f(n-1))$. This is the recursive equation characterising the natural numbers.

A function $g : C_1 \to C_2$ is a morphism from an $\mathbb{F}$-coalgebra $(C_1, c_1)$ to an $\mathbb{F}$-coalgebra $(C_2, c_2)$ if and only if $c_2 \circ g = \mathbb{F}(g) \circ c_1$.

To see what morphisms between coalgebras are, consider $\mathbb{F}_\mathbb{N}$-coalgebras. Recall: $\mathbb{F}_\mathbb{N}(X) = 1 + X$.

Suppose $g : C_1 \to C_2$ is a morphism from an $\mathbb{F}_\mathbb{N}$-coalgebra $c_1 : C_1 \to \mathbb{F}_\mathbb{N}(C_1)$ corresponding to a Peano coalgebra $(C_1, isz_1, p_1)$ to an $\mathbb{F}_\mathbb{N}$-coalgebra $c_2 : C_2 \to \mathbb{F}_\mathbb{N}(C_2)$ corresponding to a Peano coalgebra $(C_2, isz_2, p_2)$. There are two cases:

- if $x \in \text{Dom}(isz_1)$ then $c_1(x) = *$; if $x \in \text{Dom}(p_1)$ then $c_1(x) \in C_1$ and $c_1(x) = p_1(x)$;
- if $x \in \text{Dom}(isz_2)$ then $c_2(x) = *$; if $x \in \text{Dom}(p_2)$ then $c_2(x) \in C_2$ and $c_2(x) = p_2(x)$.

If $g : C_1 \to C_2$ is a morphism then $c_2(g(x)) = \mathbb{F}_\mathbb{N}(g)(c_1(x))$ holds. As $\mathbb{F}_\mathbb{N}(g) = \text{id}_1 + g$, the right hand side of the morphism equation can be simplified corresponding to the two cases above:

- if $x \in \text{Dom}(isz_1)$ then $\mathbb{F}_\mathbb{N}(g)(c_1(x)) = (\text{id}_1 + g)(*) = \text{id}_X(*) = *$;
- if $x \in \text{Dom}(p_1)$ then $\mathbb{F}_\mathbb{N}(g)(c_1(x)) = \mathbb{F}_\mathbb{N}(g)(p_1(x)) = g(p_1(x))$;

so for these two cases the morphism equation simplifies to:

- if $x \in \text{Dom}(isz_1)$ then $c_2(g(x)) = *$;
- if $x \in \text{Dom}(p_1)$ then $c_2(g(x)) = g(p_1(x))$.

Now $c_2(g(x)) = *$ if and only if $isz_2(g(x)) = *$ and $c_2(g(x)) = g(p_1(x))$ if and only if $g(x) \not\in \text{Dom}(isz_2)$ and hence $g(x) \in \text{Dom}(p_2)$ and then $c_2(g(x)) = p_2(g(x))$, so the two cases of the morphism equation further simplify to:

- if $x \in \text{Dom}(isz_1)$ then $isz_2(g(x)) = *$;
- if $x \in \text{Dom}(p_1)$ then $p_2(g(x)) = g(p_1(x))$.

Specialising the above discussion: a morphism from an $\mathbb{F}_\mathbb{N}$-coalgebra corresponding to $(\mathcal{C}, isz, p)$ to the $\mathbb{F}_\mathbb{N}$-coalgebra corresponding to the conatural numbers $(\mathbb{N}, is0, P)$ is a function $g : \mathcal{A} \to \mathbb{N}$ such that
• if \(isz(x) = \ast\) then \(g(x) = 0\);
• if \(x \in \text{Dom}(p)\) then \(P(g(x)) = g(p(x))\).

Thus a morphism to the \(F_N\)-colgebra corresponding to the conatural numbers \((\mathbb{N}, \text{isz}, P)\) from \(F_N\)-colgebra corresponding to \((C, isz, p)\) is a function \(g : C \rightarrow \mathbb{N}\) such that: \(g(x) = \text{if } isz(x) = \ast \text{ then } 0 \text{ else } g(p(x)) + 1\). This is the corecursion equation characterising the conatural numbers.

**Initial and terminal algebras**

An *initial* \(F\)-algebra is one for which there is a unique morphism from it to any other \(F\)-algebra. The natural numbers are characterised as being the unique initial \(F_N\)-algebra and the finite lists of members of \(A\) are characterised as being the unique initial \(F_L\)-algebra.

A *terminal* \(F\)-coalgebra is one for which there is a unique morphism to it from any other \(F\)-coalgebra. Terminal coalgebras are sometimes called *final* coalgebras. The conatural numbers are characterised as being the unique terminal \(F_N\)-coalgebra, and the finite and infinite lists of elements of \(A\) are characterised as being the unique terminal \(F_L\)-coalgebra.

**Least and greatest fixed points**

Some presentations of induction and coinduction are based around least and greatest fixed points (e.g. *A Tutorial on Co-induction and Functional Programming* by A.D. Gordon) whilst others are based on initial and terminal algebras (e.g. *An introduction to (co)algebra and (co)induction* by Jacobs & Rutten). The algebra-coalgebra view has been taken here, but in this section its relation to fixed points is superficially sketched.

There are at least two ways that fixed points arise. The first is to provide a uniform way to construct initial \(F\)-algebras and terminal \(F\)-coalgebras for a wide class of \(F\)s. Very roughly, the idea is that a least fixed point of \(F\) yields an initial \(F\)-algebra and a greatest fixed point yields a terminal \(F\)-coalgebra. These algebras and coalgebras can be explicitly constructed using a generalisation (dualised for coalgebras) of the proof of the Tarski-Knaster fixed point theorem. The mathematics of this generalisation is way beyond my comfort zone and I don’t attempt to explain it here (further discussion can be found in Section 14 starting on Page 55 of Rutten’s paper *Universal coalgebra: a theory of systems*).

**Fixed points, numbers and conumbers**

A hint of the idea can be glimpsed by looking at numbers. If the mapping \(F_N\) from subsets of \(\mathbb{N}\) to subsets of \(\mathbb{N}\) is defined by:
\[ \mathcal{F}_\mathbb{N}(X) = \{0\} \cup \{S(x) \mid x \in X\} \]

then \(\mathbb{N}\) and \(\overline{\mathbb{N}}\) are both fixed points of \(\mathcal{F}_\mathbb{N}\), but \(\mathbb{N}\) is the least fixed point and is the greatest fixed point.

\(\mathbb{N}\) is also the least pre-fixed point of \(\mathcal{F}_\mathbb{N}\), that is the least \(X\) such that \(\mathcal{F}_\mathbb{N}(X) \subseteq X\) and hence \(\mathbb{N} = \bigcap\{X \mid \mathcal{F}_\mathbb{N}(X) \subseteq X\}\).

Dually \(\overline{\mathbb{N}}\) is the greatest post-fixed point of \(\mathcal{F}_\mathbb{N}\), that is the greatest \(X\) such that \(X \subseteq \mathcal{F}_\mathbb{N}(X)\) and hence \(\overline{\mathbb{N}} = \bigcup\{X \mid X \subseteq \mathcal{F}_\mathbb{N}(X)\}\).

The second way fixed points arise is as a justification of induction and coinduction proof principles.

To illustrate this, compare proving \(\forall n \in \mathbb{N}. \theta_1(n) = \theta_2(n)\) by induction, where \(\theta_1 : \mathbb{N} \rightarrow A\) and \(\theta_2 : \mathbb{N} \rightarrow A\), with proving \(\forall x \in C. \phi_1(x) = \phi_2(x)\) by coinduction, where \(\phi_1 : C \rightarrow B\) and \(\phi_2 : C \rightarrow B\).

To prove \(\forall n \in \mathbb{N}. \theta_1(n) = \theta_2(n)\) by induction, let \(P = \{n \mid \theta_1(n) = \theta_2(n)\}\), then the proof of \(\forall n \in \mathbb{N}, n \in P\) by induction on \(n\) consists of the base case \(0 \in P\) and the induction step \(\forall n. n \in P \Rightarrow S(n) \in P\).

This induction argument can be seen as an application of least fixed points because the base and induction correspond to proving that \(\mathcal{F}_\mathbb{N}(P) \subseteq P\), i.e. that \(P\) is a pre-fixed point of \(\mathcal{F}_\mathbb{N}\), so as \(\mathbb{N}\) is the least pre-fixed point of \(\mathcal{F}_\mathbb{N}\) it follows that \(\mathbb{N} \subseteq P\), hence \(\forall n \in \mathbb{N}, n \in P\).

To prove \(\forall x \in C. \phi_1(x) = \phi_2(x)\) by coinduction, let \(R = \{((\phi_1(x)), \phi_2(x)) \mid x \in C\}\), then the proof by coinduction consists in \(R\) is a bisimulation, i.e. that for all \(x\): either \(\phi_1(x) = 0\) and \(\phi_2(x) = 0\) or else \(\phi_1(x) \neq 0\) and \(\phi_2(x) \neq 0\) and \((P(\phi_1(x)), P(\phi_2(x))) \in R\), i.e. \(\exists x' \in C. P(\phi_1(x)) = \phi_1(x') \land P(\phi_2(x)) = \phi_2(x')\).

This coinductive argument can be seen as an application of greatest fixed points because the set of pairs \(\mathit{EQ} = \{(n, n) \mid n \in \overline{\mathbb{N}}\}\) is the greatest post-fixed point of \(B : \mathcal{P}(\overline{\mathbb{N}} \times \overline{\mathbb{N}}) \rightarrow \mathcal{P}(\overline{\mathbb{N}} \times \overline{\mathbb{N}})\) defined by:

\[ B_{\overline{\mathbb{N}}}(R) = \{(n_1, n_2) \mid n_1 = 0 \land n_2 = 0 \lor n_1 \neq 0 \land n_2 \neq 0 \land (P(n_1), P(n_2)) \in R\} \]

\[ B_{\mathbb{N}}(R) = \{(0, 0)\} \cup \{(S(n_1), S(n_2)) \mid (n_1, n_2) \in R\} \]

Clearly \(\mathit{EQ} \subseteq B_{\overline{\mathbb{N}}}(\mathit{EQ})\) hence: \(\mathit{EQ} = \bigcup\{R \mid R \subseteq B_{\overline{\mathbb{N}}}(R)\}\). \(R\) being a bisimulation is just \(R \subseteq B_{\overline{\mathbb{N}}}(R)\), so \(R\) is less than the greatest such post-fixed point, so \(R \subseteq \mathit{EQ}\), hence if \((n_1, n_2) \in R\) then \((n_1, n_2) \in \mathit{EQ}\) and so \(n_1 = n_2\).

**Summary of fixed point proof rules for numbers and conumbers**

If \(\theta_1, \theta_2 : \mathbb{N} \rightarrow A\) then \(\forall n \in \mathbb{N}. \theta_1(n) = \theta_2(n)\) is proved by induction using the rule:

if \(P = \{n \mid \theta_1(n) = \theta_2(n)\}\) and \(\mathcal{F}_\mathbb{N}(P) \subseteq P\) then \(\mathbb{N} \subseteq P\)
This expands to:

\[ \theta_1(0) = \theta_2(0) \land (\forall n \in \mathbb{N}. \theta_1(n) = \theta_2(n)) \Rightarrow \theta_1(S(n)) = \theta_2(S(n)) \]

If \( \phi_1, \phi_2 : C \to \mathbb{N} \) then \( \forall x \in C. \phi_1(x) = \phi_2(x) \) is proved by coinduction using:

\[
\text{if } R = \{ (\phi_1(x), \phi_2(x)) \mid x \in C \} \text{ and } R \subseteq B_{\mathbb{N}}(R) \text{ then } R \subseteq EQ
\]

This expands to:

\[
\begin{align*}
\forall x \in C. & \ (\phi_1(x) = 0 \land \phi_2(x) = 0) \\
\lor & \ (\phi_1(x) \neq 0 \land \phi_2(x) \neq 0 \land (\exists x'. P(\phi_1(x)) = \phi_1(x') \land P(\phi_2(x)) = \phi_2(x')))) \\
\Rightarrow & \ \forall x \in C. \phi_1(x) = \phi_2(x)
\end{align*}
\]

**Fixed points, lists and colists**

The details of how fixed points relate to lists and colists are analogous to numbers, so are only briefly summarised here.

If the mapping \( F_{L_{\mathbb{A}}} \) from subsets of \( L_{\mathbb{A}} \) to subsets of \( L_{\mathbb{A}} \) is defined by:

\[
F_{L_{\mathbb{A}}}(X) = \{ \text{nil} \} \cup \{ \text{cons}(a, x) \mid (a \in \mathbb{A} \land x \in X) \}
\]

then \( L_{\mathbb{A}} \) and \( \overline{L}_{\mathbb{A}} \) are both fixed points of \( F_{L_{\mathbb{A}}} \), but \( L_{\mathbb{A}} \) is the least fixed point and \( \overline{L}_{\mathbb{A}} \) is the greatest fixed point.

\( \overline{L}_{\mathbb{A}} \) is also the least pre-fixed point of \( F_{L_{\mathbb{A}}} \), that is the least \( X \) such that \( F_{L_{\mathbb{A}}}(X) \subseteq X \) and hence \( L_{\mathbb{A}} = \bigcap \{ X \mid F_{L_{\mathbb{A}}}(X) \subseteq X \} \).

Dually \( \overline{L}_{\mathbb{A}} \) is the greatest post-fixed point of \( F_{L_{\mathbb{A}}} \), that is the greatest \( X \) such that \( X \subseteq F_{L_{\mathbb{A}}}(X) \) and hence \( \overline{L}_{\mathbb{A}} = \bigcup \{ X \mid X \subseteq F_{L_{\mathbb{A}}}(X) \} \).

The second way fixed points arise is as a justification of induction and coinduction proof principles.

To illustrate this, compare proving \( \forall l \in L_{\mathbb{A}}. \theta_1(l) = \theta_2(l) \) by induction, where \( \theta_1 : L_{\mathbb{A}} \to A \) and \( \theta_2 : L_{\mathbb{A}} \to A \), with proving \( \forall x \in C. \phi_1(x) = \phi_2(x) \) by coinduction, where \( \phi_1 : C \to L_{\mathbb{A}} \) and \( \phi_2 : C \to L_{\mathbb{A}} \).

To prove \( \forall l \in L_{\mathbb{A}}. \theta_1(l) = \theta_2(l) \) by induction, let \( P = \{ l \mid \theta_1(l) = \theta_2(l) \} \), then the proof of \( \forall l \in L_{\mathbb{A}}. l \in P \) by induction on \( l \) consists of the base case \( \text{nil} \in P \) and the induction step \( \forall l. l \in P \Rightarrow \forall a \in \mathbb{A}. \text{cons}(a, l) \in P \).

This induction argument can be seen as an application of least fixed points because the base and induction correspond to proving that \( F_{L_{\mathbb{A}}}(P) \subseteq P \), i.e. that
P is a pre-fixed point of $F_{L^{\infty}}$, so as $L^{\infty}$ is the least pre-fixed point of $F_{L^{\infty}}$ it follows that $L^{\infty} \subseteq P$, hence $\forall l \in L^{\infty}. l \in P$.

To prove $\forall x \in C. \phi_1(x) = \phi_2(x)$ by coinduction, let $R = \{(\phi_1(x), \phi_2(x)) \mid x \in C\}$, then the proof by coinduction consists of showing that $R$ is a bisimulation, i.e. that for all $x$: either $\phi_1(x) = \text{nil}$ and $\phi_2(x) = \text{nil}$ or else $\phi_1(x) \neq \text{nil}$ and $\phi_2(x) \neq \text{nil}$ and $\text{hd}(\phi_1(x)) = \text{hd}(\phi_2(x))$ and $(\text{tl}(\phi_1(x)), \text{tl}(\phi_2(x))) \in R$, i.e. $\exists x'. \in C. \text{tl}(\phi_1(x)) = \phi_1(x') \land \text{tl}(\phi_2(x)) = \phi_2(x')$.

This coinductive argument can be seen as an application of greatest fixed points because the set of pairs $\text{EQ} = \{(l, l) \mid l \in L^{\infty}\}$ is the greatest post-fixed point of $B_{L^{\infty}} : \mathcal{P}(L^{\infty} \times L^{\infty}) \to \mathcal{P}(L^{\infty} \times L^{\infty})$ defined by:

$B_{L^{\infty}}(R) = \{(l_1, l_2) \mid l_1 = \text{nil} \land l_2 = \text{nil} \lor l_1 \neq \text{nil} \land l_2 \neq \text{nil} \land \text{hd}(l_1) = \text{hd}(l_2) \land (\text{tl}(l_1), \text{tl}(l_2)) \in R\}$

Clearly $\text{EQ} \subseteq B_{L^{\infty}}(\text{EQ})$ hence: $\text{EQ} = \bigcup\{R \mid R \subseteq B_{L^{\infty}}(R)\}$. $R$ being a bisimulation is just $R \subseteq B_{L^{\infty}}(R)$, so $R$ is less than the greatest such post-fixed point, so $R \subseteq \text{EQ}$, hence if $(l_1, l_2) \in R$ then $(l_1, l_2) \in \text{EQ}$ and so $l_1 = l_2$.

Summary of fixed point proof rules for lists and colists

If $\phi_1, \phi_2 : L^{\infty} \to A$ then $\forall l \in L^{\infty}. \phi_1(l) = \phi_2(l)$ is proved by induction using the rule:

\[\text{if } P = \{l \mid \phi_1(l) = \phi_2(l)\} \text{ and } F_{L^{\infty}}(P) \subseteq P \text{ then } L^{\infty} \subseteq P\]

This expands to:

\[\phi_1(\text{nil}) = \phi_2(\text{nil}) \land (\forall l \in L^{\infty}. \phi_1(l) = \phi_2(l)) \Rightarrow \forall a \in A. \phi_1(\text{cons}(a, l)) = \phi_2(\text{cons}(a, l))\]

\[\Rightarrow \forall l \in L^{\infty}. \phi_1(l) = \phi_2(l)\]

If $\phi_1, \phi_2 : C \to L^{\infty}$ then $\forall x \in C. \phi_1(x) = \phi_2(x)$ is proved by coinduction using:

\[\text{if } R = \{(\phi_1(x), \phi_2(x)) \mid x \in C\} \text{ and } R \subseteq B_{L^{\infty}}(R) \text{ then } R \subseteq \text{EQ}\]

This expands to:

\[(\forall x \in C.\)
\[\left(\phi_1(x) = \text{nil} \land \phi_2(x) = \text{nil}\right)\]
\[\lor\]
\[\left(\phi_1(x) \neq \text{nil} \land \phi_2(x) \neq \text{nil} \land \text{hd}(\phi_1(x)) = \text{hd}(\phi_2(x)) \land \exists x'. \text{tl}(\phi_1(x)) = \phi_1(x') \land \text{tl}(\phi_2(x)) = \phi_2(x'))\right)\]
\[\Rightarrow \forall x \in C. \phi_1(x) = \phi_2(x)\]

31
Use in programming

Initial $F$-algebras correspond to programming language datatypes. Compare the ingredients of the initial $F_N$-algebra of numbers:

$$F_N(\mathbb{N}) = 1 + \mathbb{N}, \quad 0 \in \mathbb{N}, \quad S : \mathbb{N} \to \mathbb{N}$$

with functional programming pseudocode for a datatype declaration on numbers:

```haskell
data N = 0 | S of N
```

These contain essentially the same specifications. The `of` indicates that the thing before it is a constructor of data taking arguments of the type shown after it. If there is no `of`, then the element is a nullary constructor, i.e. a distinguished element of the datatype.

The ingredients of the initial $F_LA$-algebra of lists of members of $A$ are:

$$F_{LA}(L_A) = 1 + (\mathbb{A} \times L_A), \quad \text{null} \in L_A, \quad \text{cons} : \mathbb{A} \times L_A \to L_A$$

and the pseudocode for a corresponding datatype declaration:

```haskell
data L_A = nil | cons of (A × L_A)
```

The values specified by `data` declarations consists of finite structures built from the distinguished elements by applying constructors, e.g. $S(S(S(0)))$ or $[a_0, a_1, a_2]$, i.e. $\text{cons}(a_0, \text{cons}(a_1, \text{cons}(a_2, \text{nil})))$. Recursion is used to construct data, for example the list $[n, n-1, \ldots, 1]$ would be constructed by executing `downfrom(n)`, where: $\text{downfrom}(n) = \text{if } n = 0 \text{ then nil else cons}(n, \text{downfrom}(n-1))$.

Codatatypes are less common, but compare the ingredients of the terminal $F$-coalgebras for conumbers and colists.

$$F_N(\overline{\mathbb{N}}) = 1 + \overline{\mathbb{N}}, \quad \text{is} : \overline{\mathbb{N}} \to 1, \quad P : \overline{\mathbb{N}} \to \overline{\mathbb{N}}, \quad F_{LA}(\overline{L_A}) = 1 + (\mathbb{A} \times \overline{L_A}), \quad \text{null} : \overline{L_A} \to 1, \quad \text{destcons} : \overline{L_A} \to \mathbb{A} \times \overline{L_A}$$

with the made up pseudocode:

```haskell
codata \overline{\mathbb{N}} = \text{null} & P to \overline{\mathbb{N}}
codata \overline{L_A} = \text{null} & \text{destcons to (A × L_A)}
```

The $F$-coalgebra specifications also contain essentially the same material as the pseudocode. The `to` indicates that the thing before it is a destructor that decomposes data into components of the type shown after it. If there is no `to`, then the element is a nullary destructor, i.e. a test for a distinguished element of the datatype.

For lists, `hd` and `tl` would normally be specified, rather than `destcons`. The made up pseudocode corresponding to:

$$F_{LA}(\overline{L_A}) = 1 + (\mathbb{A} \times \overline{L_A}), \quad \text{null} : \overline{L_A} \to 1, \quad \text{hd} : \overline{L_A} \to \mathbb{A}, \quad \text{tl} : \overline{L_A} \to \overline{L_A}$$
would be:

```
codata L = null & hd to A & tl to L
```

The values specified by `codata` declarations may not be finite, so can’t necessarily be represented explicitly in finite computer memories. However, these values can be implicitly represented and accessed incrementally by destructors, i.e. by lazy evaluation.

One way to define codata is by corecursion, for example

```
CountFrom(n) = cons(n, CountFrom(n+1))
```

defines `CountFrom(n)` to be the infinite list starting from `n`, i.e. `[n, n+1, ...]`. This corecursion is the instance of:

```
g(x) = if test(x) = * then nil else cons(((id × g)(dest(x)))
```

where `A = N`, `test(n) = *` is always false and `dest(n) = (n, n+1)`. It is is the unique morphism from the $F_N$-coalgebra $(N, ∅, λn.(n, n+1))$ to the final $F_N$-coalgebra $(L_N, null, destcons)$, where $Dom(∅)$ is the empty set, so $∅(n) = *$ is never true.

Another way codata is specified is by giving equations for the destructors, for example `CountFrom(n)` could be specified by:

```
hd(CountFrom(n)) = n ; tl(CountFrom(n)) = CountFrom(n+1)
```

This style can be used to define codata corresponding to automata as already suggested by the discussion of the function `g` in the example of corecursion for lists used above and repeated in Figure 2 below.

---

**Figure 3:**
The function $g$ defined by this could be specified by:

$$\text{hd}(g(A)) = A; \text{hd}(g(B)) = B; \text{hd}(g(C)) = C; \text{hd}(g(D)) = D; \text{hd}(g(E)) = E;$$
$$\text{hd}(g(F)) = F; \text{hd}(g(G)) = G; \text{hd}(g(H)) = H; \text{hd}(g(I)) = I; \text{hd}(g(J)) = J;$$

$$\text{tl}(g(A)) = g(A); \text{tl}(g(B)) = g(C); \text{tl}(g(C)) = g(B); \text{tl}(g(D)) = g(E);$$
$$\text{tl}(g(E)) = g(F); \text{tl}(g(G)) = g(H); \text{tl}(g(H)) = g(I); \text{tl}(g(I)) = g(JA);$$
$$\text{null}(g(F)); \text{null}(g(J))$$

Unlike `CountFrom`, which only creates infinite lists, the function $g$ creates both infinite and finite lists: $g(A)$, $g(B)$ and $g(C)$ are infinite and $g(x)$ for $x \in \{D, E, F, G, H, I, J\}$ are finite, with $g(F)$ and $g(J)$ being nil.

There’s an illuminating blog post that discusses Data vs Codata.

I’ve read that infinite data imported from external sources, e.g. from an analog-to-digital converter or a Twitter stream, can be considered to be codata. Presumably this view considers reading inputs as applying destructors, like `hd` and `tl`, so that coalgebra inspired programming methods can be used to process such imported data streams. Due to my near total ignorance, more will not be said on this now!

**Concluding thoughts**

I wrote this article as a way to learn about coinduction. Did I succeed? Essentially yes: I now feel – tentatively – that I understand the core ideas of coinduction and how it is dual to induction. I’ve also hope I now have a rough idea of the elementary parts of the general theory of algebras and coalgebras – at least the part that lives in set theory – and how this theory relates to recursion induction, corecursion and coinduction. The most general formulations live in category theory, which is territory in which I struggle to survive … but Google finds plenty of stuff, a random example being Worrell’s PhD thesis.

Most articles on coinduction aim to evangelise its use for applications. This is something I’ve pretty much ignored here. Particularly important applications are to reasoning about concurrent systems, indeed the Wikipedia article on coinduction starts with the sentence “In computer science, coinduction is a technique for defining and proving properties of systems of concurrent interacting objects”. In such applications the bisimulations that arise are often between labelled transition system. As far as I am aware there are no significant applications of coinduction to reasoning about numbers and only a few to lists. The bulk of applications are to systems modelled with transition systems, so perhaps I should add something about these … but I’m burned out on coinduction and the tutorials cited at the beginning of this article are excellent, so I probably won’t ever get around to adding anything on this.
First complete draft: February 03, 2017.