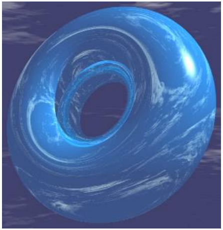
Introduction: Recursion and Circularity

Larry Moss
Indiana University, Bloomington

TACL'13 Summer School, Vanderbilt University



My intention is to present material on circularly defined objects and sets emphasizing

- the “big picture” ideas, including lots of examples of what we’ll eventually see in detail
- basic concepts from category theory and coalgebra
- Non-wellfounded sets covering much of what someone would need to know to use these (maybe)
- connections to modal logic (maybe)
- additional topics coming from one of the first three days (or extra time if I’m running late)

This course was intended for people with no prior exposure to the subject.
It would be good to have seen a bit of (standard) set theory, but this is not really needed.

Most of the emphasis is on the theory rather than the applications.

You may find versions of my lectures at

www.indiana.edu/~iulg/moss/TACL2013

In general, my slides have more stuff than I present in person.

I taught a somewhat-related course at the 2012 European Summer School in Logic, Language, and Information.

The material there was less mathematical than this course at TACL.

You may find versions of those lectures at

www.indiana.edu/~iulg/moss/ESSLLI2012

A very basic mathematical example: recursion

The factorial function is expressed by

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= (n+1) \times n! \end{aligned}$$

Compare this circular (or fixed-point) presentation with an explicit presentation

$$n! = 1 \times 2 \times \cdots \times n$$

Circular presentations are often very useful.

At the same time, circular presentations are sometimes problematic: $x = x + 1$.

A very basic mathematical example: recursion

The factorial function is expressed by

$$
\begin{aligned}
0! &= 1 \\
(n+1)! &= (n+1) \times n!
\end{aligned}
$$

Compare this circular (or fixed-point) presentation with an explicit presentation

$$
n! = 1 \times 2 \times \cdots \times n
$$

Circular presentations are often very useful.

At the same time, circular presentations are sometimes problematic: $x = x + 1$.

Other times, they are trivial:

$$
23 = 46 - 23
$$

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= (n+1) \times n! \end{aligned} \qquad \begin{aligned} 0? &= 1 \\ (n+1)? &= n? + (n \times n?) \end{aligned}$$

It just so happens that $n! = n?$ for all n.

Why?

$$
\begin{aligned}
0! &= 1 \\
(n+1)! &= (n+1) \times n!
\end{aligned}
\qquad
\begin{aligned}
0? &= 1 \\
(n+1)? &= n? + (n \times n?)
\end{aligned}
$$

It just so happens that $n! = n?$ for all n.

Why?

Circular definitions are mainly useful when they come with matching proof principles, such as induction.

It turns out to be very hard to say exactly what circularity is!

Here is a very preliminary definition, to be followed by a series of suggestive examples.

An object is circular if it involves itself in some interesting way.

Let X be some collection of objects,
and let R be a relation on X.

An element x of X is circular with respect to R
if $x\ R\ x$, or if there is a finite chain

$$x = x_0 \quad R \quad x_1 \quad R \quad x_2 \quad R \quad \cdots \quad R \quad x_n = x.$$

- This sentence is true.
- This sentence is false.
- This sentence is circular.
- This sentence is not circular.

I take it that these sentences refer to themselves and thus are circular.

At the same time, I take reference to be a deeply mysterious phenomenon.

- This sentence is true.
- This sentence is false.
- This sentence is circular.
- This sentence is not circular.

I take it that these sentences refer to themselves and thus are circular.

At the same time, I take reference to be a deeply mysterious phenomenon.

Accordingly, I won't have much to say on what it is.

But taking it as a given, we'll have quite a bit to say!

A comment on recursion, circularity, and mathematical logic

By and large, the tradition in mathematical logic is to be suspicious of circularity, due to the proximity of paradox.

In fact, the usual treatments of recursion suppress the connections to circularity that I would like to emphasize.

Recursion Principle for N

For every set X, every $x_0 \in X$, and every $f : X \to X$, there is a unique function $f^* : N \to X$ so that

$$
\begin{aligned}
f^*(0) &= x_0 \\
f^*(n+1) &= f(f^*(n))
\end{aligned}
$$

Recursion Principle for N

For every set X, every $x_0 \in X$, and every $f : X \to X$, there is a unique function $f^* : N \to X$ so that

$$\begin{aligned} f^*(0) &= x_0 \\ f^*(n+1) &= f(f^*(n)) \end{aligned}$$

In a course on set theory that emphasizes the foundational aspects of the subject, one has to prove this Recursion Principle.

It follows from the Axiom of Infinity (and some other basic axioms), but one could take the Recursion Principle to be the Axiom of Infinity!

Use the Recursion Principle as we stated in to prove that the factorial function exists.

You should use more basic functions like

$$\begin{array}{lcl} s(n) & = & n+1 \\ p(n,m) & = & n+m \\ t(n,m) & = & n \times m \\ \pi((n,m)) & = & n \end{array}$$

But there is still more to do.

More circularity: common knowledge and social conventions

Countries differ as to which side of the road one drives a car;
the matter is one of social and legal convention.
In Kenya, they follow British custom and drive on the left.

Suppose that in Kenya, the government decides to change the driving side.

But suppose that the change is made in a quiet way,
so that only one person in the country, say Silvanos,
finds out about it.
After this, what should Silvanos do?

More circularity: common knowledge and social conventions

Countries differ as to which side of the road one drives a car;
the matter is one of social and legal convention.
In Kenya, they follow British custom and drive on the left.

Suppose that in Kenya, the government decides to change the driving side.

But suppose that the change is made in a quiet way,
so that only one person in the country, say Silvanos,
finds out about it.
After this, what should Silvanos do?

From the point of view of safety, it is clear that
he should not obey the law:
since others will be disobeying it, he puts his life at risk.

More circularity: common knowledge and social conventions

Suppose further that the next day the government decides to make an announcement to the press that the law was changed. What should happen now?

Suppose further that the next day the government decides to make an announcement to the press that the law was changed. What should happen now?

The streets are more dangerous and more unsure this day, because many people will still not know about the change. Even the ones that have heard about it will be hesitant to change, since they do not know whether the other drivers know or not.

More circularity: common knowledge and social conventions

Eventually, after further announcements, we reach a state where:

The law says drive on the right and everyone knows (1). (1)

Note that (1) is a circular statement. The key point is not that everyone know what the law says, but that they in addition know this very fact, the content of the sentence you are reading.

A hawk is someone who

- usually acts aggressively towards a dove
- usually avoids conflict with another hawk.

A dove is someone who

- usually shares with another dove
- usually avoids conflict with a hawk.

This sort of example comes from
games of imperfect information,
and the specific concept there is called (Harsanyi) types.

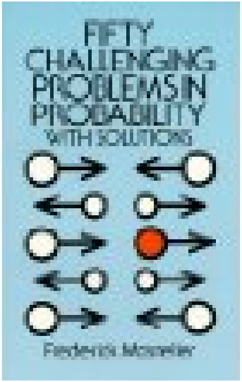
The point is that to say what a type is,
we need to say how it interacts with agents of
other types.

Adding some sort of expected payoffs, we might want

$$\begin{array}{lcl} \text{dove} & = & \{(\text{dove}, 3), (\text{hawk}, 1)\} \\ \text{hawk} & = & \{(\text{dove}, 5), (\text{hawk}, 0)\} \end{array}$$

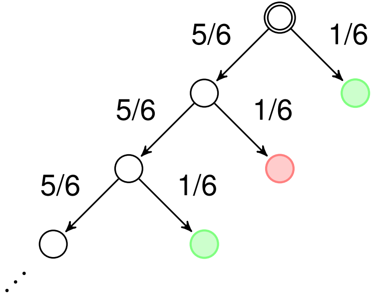
And so we are very quickly facing a mathematical problem
involving circularity.

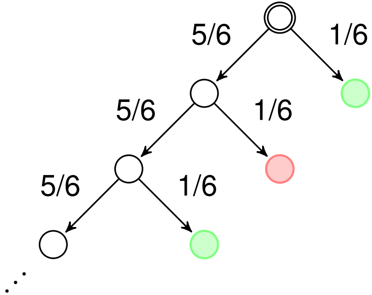
Frederick Mosteller,
Fifty Challenging Problems in Probability With Solutions



Problem 4: If one throws a die repeatedly, starting with roll 1, what is the probability that the first 6 is on an odd numbered roll?

We have a Markov chain with success and fail nodes at the end





So the total probability for a success is

$$\frac{1}{6} + \left(\frac{5}{6}\right)^2 \frac{1}{6} + \left(\frac{5}{6}\right)^4 \frac{1}{6} + \cdots \quad = \quad \frac{6}{11}$$

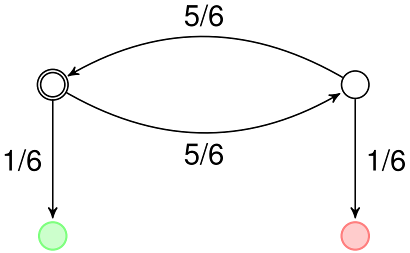
"But a beautiful way to solve the problem is as follows:
To get the first 6 on an odd numbered roll,
one can either get it on the first roll,
or else fail to get a 6 on the first roll, and
then get the first 6 on an *even* numbered roll after that."

Let p be the probability of success,
So $1 - p$ is the chance that the first 6 is on an even numbered roll.

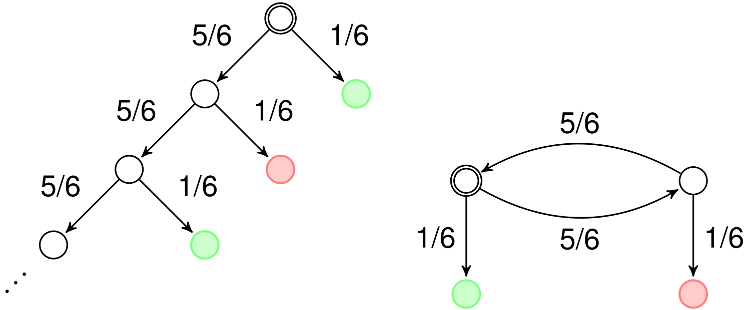
$$p = \frac{1}{6} + \frac{5}{6}q$$

$$q = 1 - p$$

The point: one in effect one is looking at



But what exactly is the relation between the two pictures?



For us, this is the important question.

Is the relationship describable as a form of induction,
or is it something else entirely?

We have seen a number of examples of circular presentations:

- recursion
- $(23 = 46 - 23)$
- self-referential sentences
- common knowledge/tacit consensus
- game-theoretic types
- (equilibrium notions)
- numbers, in the probability problem

The point so far has been to
situate recursion inside a broader class of useful phenomena
and to suggest mathematical questions.

Streams, with a circular example

A stream of numbers is an ordered pair whose first coordinate is a number and whose second coordinate is again a stream of numbers.

The first coordinate is called the head, and the second the tail.

The tail of a given stream might be different from it, but again, it might be the very same stream.

For example, consider the stream s whose head is 0 and whose tail is s again.

Thus the tail of the tail of s is s itself,
and in this sense, s is circular.

We have $s = \langle 0, s \rangle$, $s = \langle 0, \langle 0, s \rangle \rangle$, etc.

$s = \langle 0, s \rangle$

This stream s exhibits object circularity.

It is natural to "unravel" its definition as

$$(0, 0, \ldots, 0, \ldots).$$

We are purposely using different notation from $s = \langle 0, s \rangle$.
We do this to emphasize the conceptual difference.

We defined streams in a circular way.

The classical way to "straighten out" the circularity is to identify Nat^∞ with $N \to N$.

So we can take the unraveled form to be the constant function with value 0.

And the constant function doesn't seem to be circular at all!

One way to define streams is with systems of equations.

For example, here is such a system:

$$\begin{array}{lcl} x & \approx & \langle 0, y \rangle \\ y & \approx & \langle 1, z \rangle \\ z & \approx & \langle 2, x \rangle \end{array}$$

We use the $\approx$ sign for equations we would like to solve.

For the solution to an equation or a system of them, we will use a “dagger” to refer to the solution.

One way to define streams is with systems of equations.

For example, here is such a system:

$$\begin{array}{rcl} x & \approx & \langle 0, y \rangle \\ y & \approx & \langle 1, z \rangle \\ z & \approx & \langle 2, x \rangle \end{array}$$

In an arithmetic setting, we could write

$$w \approx \frac{1}{2} w + 1 \qquad\qquad w^{\dagger} = 2$$

for example.

One way to define streams is with systems of equations.

For example, here is such a system:

$$\begin{array}{rcl} x & \approx & \langle 0, y \rangle \\ y & \approx & \langle 1, z \rangle \\ z & \approx & \langle 2, x \rangle \end{array}$$

The system defines streams $x^\dagger$, $y^\dagger$, and $z^\dagger$.

These streams satisfy real equations:
$x^\dagger = \langle 0, y^\dagger \rangle$, $y^\dagger = \langle 1, z^\dagger \rangle$, and $z^\dagger = \langle 2, x^\dagger \rangle$.
These streams then have unraveled forms.

For example, the unraveled form of $y^\dagger$ is $(1, 2, 0, 1, 2, 0, \ldots)$.

One way to define streams is with systems of equations.

For example, here is such a system:

$$\begin{array}{lcl} x & \approx & \langle 0, y \rangle \\ y & \approx & \langle 1, z \rangle \\ z & \approx & \langle 2, x \rangle \end{array}$$

It might be better to think of circularity as a property of the definition, rather than of the object being defined.

There is a natural operation of "zipping" two streams.

For example, if $s = \langle 0, s \rangle$ and $t = \langle 1, t \rangle$, then

$$\text{zip}(s, t) \quad = \quad (0, 1, 0, 1, \ldots)$$

Also called "merging", the function zip is defined by

$$\text{zip}(s, t) \quad = \quad \langle \text{head}(s), \text{zip}(t, \text{tail}(s)) \rangle$$

So to zip two streams *s* and *t* one starts with the head of *s*, and then begins the same process of zipping all over again, but this time with *t* first and the tail of *s* second.

There is a natural operation of "zipping" two streams.

For example, if $s = \langle 0, s \rangle$ and $t = \langle 1, t \rangle$, then

$$\text{zip}(s, t) \quad = \quad (0, 1, 0, 1, \ldots)$$

Note that the definition of zip is circular!

There is a natural operation of “zipping” two streams.

For example, if $s = \langle 0, s\rangle$ and $t = \langle 1, t\rangle$, then

$$\text{zip}(s, t) \quad = \quad (0, 1, 0, 1, \ldots)$$

Please note that our definition of zip does not work by recursion as one might expect; for on thing, there are no “base cases” of streams.

A famous stream defined in terms of zip

$$x \quad \approx \quad \mathsf{zip}(x, x)$$

has all constant streams as its solutions.

$$x \quad \approx \quad \langle \mathsf{head}(x) + 1, x \rangle$$

has no solutions whatsoever.

A famous stream defined in terms of zip

$$\begin{array}{rcl} x & \approx & \langle 1, \mathsf{zip}(x, y) \rangle \\ y & \approx & \langle 0, \mathsf{zip}(y, x) \rangle \end{array}$$

The system has a unique solution.

$$\begin{array}{rcl} x & \approx & \langle 1, \mathrm{zip}(x, y)\rangle \\ y & \approx & \langle 0, \mathrm{zip}(y, x)\rangle \end{array}$$

The system has a unique solution.
The unraveled form of $x^\dagger$, $y^\dagger$, and $\mathrm{zip}(x^\dagger, y^\dagger)$ begin as

$$\begin{array}{lcl} x^\dagger & = & (1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,\ldots) \\ y^\dagger & = & (0,0,1,0,1,1,0,0,1,1,0,1,0,0,1,0,1,\ldots) \\ \mathrm{zip}(x^\dagger, y^\dagger) & = & (1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,\ldots) \end{array}$$

$\langle 0, x^\dagger\rangle$ is the Thue-Morse sequence.

Circularity is more a quality of presentations of objects than of the objects themselves.

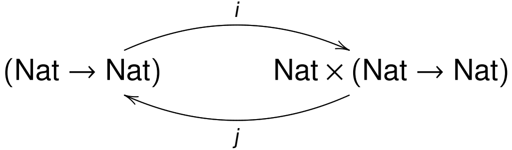
Often very interesting objects have circular presentations.

Let Nat^{∞} be the set of streams of numbers.
What equation does Nat^{∞} satisfy?

$$\mathsf{Nat}^{\infty} \quad = \quad \mathsf{Nat} \times \mathsf{Nat}^{\infty}.$$

Actually, the question of whether we mean $=$ (actual identity)
or just $\cong$ (isomorphic in some relevant sense)
is interesting!

So let's explore it.



Here $i(f) = \langle f(0), \lambda m.f(m+1)\rangle$
and $j(n, f) = \lambda m.$if $m = 0$, then n, otherwise $f(n-1)$.

One should check that the two composites are the identities.

$$(\text{Nat} \to \text{Nat}) \underset{j}{\overset{i}{\rightleftarrows}} \text{Nat} \times (\text{Nat} \to \text{Nat})$$

The way we defined Nat^∞, we had $\text{Nat}^\infty = N \times \text{Nat}^\infty$, so that

$$\text{Nat}^\infty \underset{id}{\overset{id}{\rightleftarrows}} \text{Nat} \times \text{Nat}^\infty$$

The maps this time are strictly the identity.

Writing

$$\mathsf{Nat}^\infty \quad = \quad \mathsf{Nat} \times \mathsf{Nat}^\infty$$

exhibits the set of streams in a circular way.

An object is circular if it involves itself in some interesting way.

Frequently this is interesting regarding collections of objects.

Again, Nat^∞ satisfies $X \approx \mathsf{Nat} \times X$.
But this equation has other solutions, such as $\emptyset$.

And up to isomorphism, the function set

$$\mathsf{Nat} \to \mathsf{Nat}$$

solves it.

Exercise 2

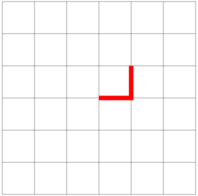
Find a set $X \subseteq \mathsf{Nat}^\infty$ and an isomorphism $X \approx \mathsf{Nat} \times X$ such that X is not closed under zip.

The importance of this is that the principle implying the existence/uniqueness of zip must use more than just the equation $X \approx \mathsf{Nat} \times X$.

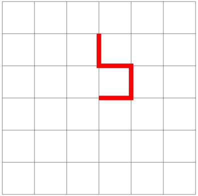
With 90 minute lectures, I like to vary the style of the presentation at some points.

I think it will be good to do a group exercise that will also present some issues that we'll explore further later on.

(And for readers in the future,
please get out a strip of paper and follow along.
You need to successively fold right over left,
and you need to understand how I'm using the words
clockwise and counter-clockwise.)

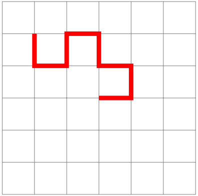


one fold	1

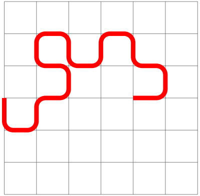


one fold	1		
two folds	1	1	-1

1 for counterclockwise.
-1 for clockwise.



one fold	1						
two folds	1	1	−1				
three folds	1	1	−1	1	1	−1	−1



one fold	1														
two folds	1	1	−1												
three folds	1	1	−1	1	1	−1	−1								
four folds	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

Although we can't fold a real piece of paper onto itself seven times, we can imagine doing it an arbitrary number of times.

Mathematically, we can even study the infinite sequence that we would get by folding it forever.

It starts out

$$1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1,$$
$$1, 1, 1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, -1, -1, \ldots$$

This is the regular paperfolding sequence which I'll write as p.

I'll start the indexing of all sequences in this talk with the number 0.

What is p_{2013}?

s_0	1														
s_1	1	1	−1												
s_2	1	1	−1	1	1	−1	−1								
s_3	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

There are at least two different ways to go from s_n to s_{n+1}.

Can you find one?

How can we go from one finite sequence to the next?

s_n is $p_0, \ldots, p_{2^{n+1}-1}$

s_0	1														
s_1	1	1	−1												
s_2	1	1	−1	1	1	−1	−1								
s_3	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

There are at least two different ways to go from s_n to s_{n+1}.

Hint 1

Imagine the folded paper after n folds.
What does fold $n+1$ do to the sequence?

Hint 2

Imagine the paper after $n+1$ folds.
Cut it open on the middle fold,
to find two copies of the paper after n folds.

FOLLOWING HINT 1

Take s_n and interleave (zip) a sequence of alternating 1's and -1's, starting with 1 before the first term in s_n.

For example:

s_2	1	1	−1	1	1	−1	−1								
s_2 spread		1		1		−1		1		1		−1		−1	
zip	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1
s_3	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

Following Hint 1

Take s_n and interleave (zip) a sequence of alternating 1's and -1's, starting with 1 before the first term in s_n.

For example:

s_2	1	1	-1	1	1	-1	-1								
s_2 spread		1		1		-1		1		1		-1		-1	
zip	1	1	-1	1	1	-1	-1	1	1	1	-1	-1	1	-1	-1
s_3	1	1	-1	1	1	-1	-1	1	1	1	-1	-1	1	-1	-1

Let alt_n be the alternating sequence of length 2^n, starting with 1.
We have

$$\begin{aligned} s_0 &= 1 \\ s_{n+1} &= zip(alt_{n+1}, s_n) \end{aligned}$$

Following Hint 2

Take s_n, append 1, and then append at the end
the same sequence s_n,
but *written backwards* and *with all signs changed*.

For example:

s_2	1	1	−1	1	1	−1	−1								
add 1	1	1	−1	1	1	−1	−1	1							
$rev(s_2)$	−1	−1	1	1	−1	1	1								
$-rev(s_2)$	1	1	−1	−1	1	−1	−1								
append	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1
s_3	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

Following Hint 2

Take s_n, append 1, and then append at the end
the same sequence s_n,
but *written backwards* and *with all signs changed*.

For example:

s_2	1	1	−1	1	1	−1	−1								
add 1	1	1	−1	1	1	−1	−1	1							
$rev(s_2)$	−1	−1	1	1	−1	1	1								
$-rev(s_2)$	1	1	−1	−1	1	−1	−1								
append	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1
s_3	1	1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	−1

We have

$$s_0 = 1$$
$$s_{n+1} = s_n \cdot 1 \cdot -rev(s_n)$$

We have two formulations of the finite sequences s_n

$$\begin{aligned} s_1 &= 1 \\ s_{n+1} &= zip(alt_n, s_n) \end{aligned} \qquad \begin{aligned} s_1 &= 1 \\ s_{n+1} &= s_n \cdot 1 \cdot -rev(s_n) \end{aligned}$$

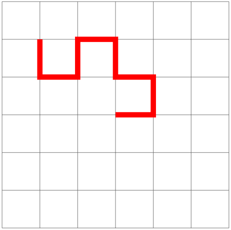
Exercise 3 for today

Suppose someone just gave you two definitions, without telling you where they came from.

$$\begin{aligned} s_1 &= 1 \\ s_{n+1} &= zip(alt_n, s_n) \end{aligned} \qquad \begin{aligned} t_1 &= 1 \\ t_{n+1} &= t_n \cdot 1 \cdot -rev(t_n) \end{aligned}$$

Prove that $s_n = t_n$ for all $n \geq 1$.

Earlier, we saw pictures like



Here are two videos related to our two methods:

Click here for an illustration of Method 1.
Click here for a similar one for Method 2.

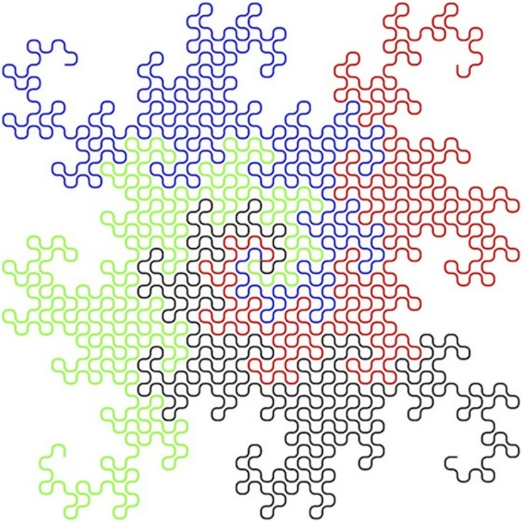
It turns out that if we run the process forever,
without shrinking things the way the videos do,
we get an infinite dragon curve.

The most startling feature of dragon curves is that
four such curves (starting together, but in different directions)
will fill all of the segments in the infinite grid,
with no repeats and nothing missing.

This results was proven by Chandler Davis and Donald Knuth
in a paper from 1970.

The dragon itself seems to have been discovered by
NASA physicist John Heighway in the 1960's.

Is this a circular object?



We have two formulations of the finite sequences s_n

$$\begin{aligned} s_0 &= 1 \\ s_{n+1} &= zip(alt_{n+1}, s_n) \end{aligned} \qquad \begin{aligned} s_0 &= 1 \\ s_{n+1} &= s_n \cdot 1 \cdot -rev(s_n) \end{aligned}$$

The second formulation shows that $\lim_n s_n$ exists;
it's p by definition.

The first formulation leads to a direct characterization of p.

Consider the infinite sequence

$$alt = 1, -1, 1, -1, 1, -1, \cdots$$

Then $alt_n \to alt$, and $s_n \to p$.

By continuity, and/or other principles that are my main interest in bringing up this topic,

FIXED-POINT CHARACTERIZATION OF THE PAPERFOLDING SEQUENCE p

$$p = zip(alt, p)$$

We have

$$p = zip(alt, p) \qquad head(p) = 1$$

Let's introduce a variable *a* for *alt*.
While we're at it, let's also introduce *b* and *c* for the constants.

$$\begin{array}{rclcrcr} a & = & zip(b, c) & \quad & head(alt) & = & 1 \\ b & = & zip(b, b) & & head(b) & = & 1 \\ c & = & zip(c, c) & & head(c) & = & -1 \end{array}$$

We have

$$p = zip(alt, p) \qquad head(p) = 1$$

Let's introduce a variable *a* for *alt*.
While we're at it, let's also introduce *b* and *c* for the constants.

$$\begin{array}{rclrcl} a & = & zip(b,c) & head(alt) & = & 1 \\ b & = & zip(b,b) & head(b) & = & 1 \\ c & = & zip(c,c) & head(c) & = & -1 \end{array}$$

Going back to *p*, we get

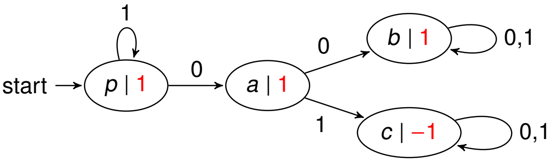
$$\begin{array}{rclrcl} p & = & zip(a,p) & head(p) & = & 1 \\ a & = & zip(b,c) & head(a) & = & 1 \\ b & = & zip(b,b) & head(b) & = & 1 \\ c & = & zip(c,c) & head(c) & = & -1 \end{array}$$

This is a second characterization of *p*, as part of the solution to a stream system involving *zip*.

We have seen a presentation of the paperfolding sequence

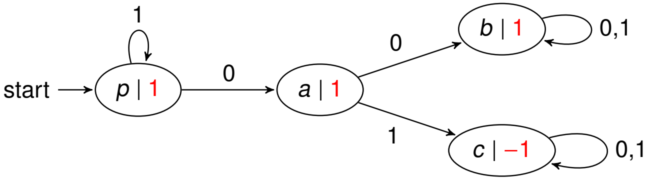
$$\begin{array}{rclrcr} p & = & zip(a,p) & head(p) & = & 1 \\ a & = & zip(b,c) & head(a) & = & 1 \\ b & = & zip(b,b) & head(b) & = & 1 \\ c & = & zip(c,c) & head(c) & = & -1 \end{array}$$

We convert this into a finite automaton with output:



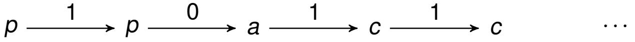
To find p_n, the nth term of the paperfolding sequence,

- write n in binary
- start with the least significant digit in the "start state"
- follow the arrows as you process the binary digits
- answer is the red value on the last node



The base 2 representation of 2013 is 11111011101.

Feed this into the automaton, starting in state p
with the 0 on the right end of 11111011101 and going leftward.



It's the output at state c, namely -1.

(Of course I didn't say why this weird procedure works.
That's one of our questions!)

1. Take the unit interval $[0, 1]$, then remove the open middle third $(\frac{1}{3}, \frac{2}{3})$, leaving two disconnected pieces.
   For each of those, remove the open middle third.
   Keep going for infinitely many steps.
   Then c is what remains "at the end".
2. c is the set of numbers possessing a ternary (base 3) decimal expansion with no 1's.
3. c is the unique non-empty compact subset of $[0, 1]$ with

$$c = \frac{1}{3}c \; \cup \; \left(\frac{2}{3} + \frac{1}{3}c\right) .$$

This last equation defines c in terms of itself.

It is the presentation of the Cantor set coming from the theory of iterated function systems.
(cf. my talk at TACL on Monday).

We have see a number of examples of circular presentations:

- recursion
- $(23 = 46 - 23)$
- self-referential sentences
- common knowledge/tacit consensus
- game-theoretic types
- (equilibrium notions)
- numbers, in the probability problem
- $s = \langle 0, s \rangle$ and more involved systems
- the definition of zip
- $\mathrm{Nat}^\infty = \mathrm{Nat} \times \mathrm{Nat}^\infty$
- $p = \mathrm{zip}(alt, p)$
- fractal sets of reals

Circularity is more a matter of presentations than of objects.

At this point, we have seen three examples of

1. Objects presented as the solution of systems of various kinds.
2. The solution spaces themselves giving rise to problematic forms of circularity.

The goal of the course is to make sense of this phenomenon in a general, and mathematically insightful manner.

At this point, we have seen three examples of

1. Objects presented as the solution of systems of various kinds.
2. The solution spaces themselves giving rise to problematic forms of circularity.

The goal of the course is to make sense of this phenomenon in a general, and mathematically insightful manner.
The way it will work:

system of some sort	coalgebra of some functor F
solution space for those systems	final coalgebra for F

algebraic concepts	coalgebraic concepts
set with algebraic operations	set with transitions and observations
algebra for a functor	coalgebra for a functor
initial algebra	final coalgebra
least fixed point	greatest fixed point
congruence relation	bisimulation equivalence rel'n
equational logic	modal logic
recursion: map out of an initial algebra	corecursion: map into a final coalgebra
Foundation Axiom	Anti-Foundation Axiom
iterative conception of set	coiterative conception of set
typical for syntactic objects	typical for semantic spaces
bottom-up	top-down

Exercise 1

Use the Recursion Principle as we stated in to prove that the factorial function exists.

Let $X = N \times N$,
let $x_0 = (0, 1)$,
and let $f : N \times N \to N \times N$ be

$$(m, n) \mapsto (m + 1, (m + 1) \times n)$$

By initiality, we get $f^* : N \to N \times N$ so that

$$\begin{array}{rcl} f^*(0) & = & (0, 1) \\ f^*(n+1) & = & (pi(f^*(n)) + 1, (pi(f^*(n)) + 1) \times f^*(n)) \end{array}$$

An easy induction on N shows that $pi(f^*(n)) = n$ for all n.
And so

$$\begin{array}{rcl} f^*(0) & = & (0, 1) \\ f^*(n+1) & = & (n + 1, (n + 1) \times f^*(n)) \end{array}$$

To get factorial, we take $\pi_2 \cdot f$.

Exercise 2

Find a set $X \subseteq \mathsf{Nat}^{\infty}$ and an isomorphism $X \approx \mathsf{Nat} \times X$ such that X is not closed under zip.

The set of streams which are eventually constant does it.

Solution to Exercise 3

Exercise 3 for today

Suppose someone just gave you two definitions, without telling you where they came from.

$$s_1 = 1 \qquad\qquad t_1 = 1$$
$$s_{n+1} = zip(alt_n, s_n) \qquad\qquad t_{n+1} = t_n \cdot 1 \cdot -rev(t_n)$$

Prove that $s_n = t_n$ for all $n \geq 1$.

We show by induction that $s_n = t_n$ and $s_{n+1} = t_{n+1}$.
Here is the main step:

$$
\begin{aligned}
& s_{n+2} \\
= \;& zip(alt_{n+1}, s_{n+1}) \\
= \;& zip(alt_{n+1}, t_{n+1}) \\
= \;& zip(alt_n \cdot alt_n, t_n \cdot 1 \cdot -rev(t_n)) \\
= \;& zip(alt_n, t_n) \cdot 1 \cdot zip(-rev(alt_n), -rev(t_n)) \\
= \;& zip(alt_n, s_n) \cdot 1 \cdot -rev(zip(alt_n, t_n)) \\
= \;& zip(alt_n, s_n) \cdot 1 \cdot -rev(zip(alt_n, s_n)) \\
= \;& s_{n+1} \cdot 1 \cdot -rev(s_{n+1}) \\
= \;& t_{n+1} \cdot 1 \cdot -rev(t_{n+1}) \\
= \;& t_{n+2}
\end{aligned}
$$