1 Lecture 01

This course deals with *abstract mathematical objects*, which are defined by the properties they satisfy.

Properties: defined by propositions/statements which are either true or false. Here are a few examples of propositions:

1. 7 is a prime number.
2. All natural numbers are even.
3. All even numbers greater than 2 can be written as the sum of 2 primes.

We shall try to define the natural numbers themselves using the properties they satisfy. Let's start with these 2 axioms:

1. 0 is a natural number. [1]
2. For every natural number n, there exists a natural number $n + 1$.

The first axiom tells us that there is a starting number (which we call 0), and the second axiom tells us that for every natural number there is a *next* natural number.

It might be a bit weird to use the addition symbol in our axioms when we haven't even defined numbers yet. Note that this is just a notation; to make it clear we can write $next(n)$ instead of $n + 1$ to indicate the next natural number. It's best to think of $next(n)$ as a function which just spits out a new natural number for each input n.

Predicates: a statement which involves variables, which can take any value in some domain. Think of a predicate $P(x)$ as a function which assign true or false to each value x. For example, $P(x)$ could denote *x is the square of an integer.*

There are 3 ways to make a predicate into a proposition:

1. Substitute a constant for x, for example $P(18)$ is a proposition.
2. $\exists x\ P(x)$: this proposition is true if there is some object a for which $P(a)$ is true.
3. $\forall x\ P(x)$: this proposition is true if $P(x)$ is true for all objects x.

Using this notation, we can precisely write our previous 2 axioms for natural numbers:

1. $\exists n\ n = 0$
2. $\forall n\ \exists m\ (m = next(n))$

Let's think more about the second axiom. We need to place more restrictions on this *next* function to get our natural numbers. For example, if we allow $next(0) = 0$, our natural

[1] Whether we add 0 or not to the set of natural numbers is simply a matter of convention. For this course, it is convenient to add it to the set.

numbers just becomes the set $\{0\}$, and it satisfies the axioms we have so far. We could also have $next(0) = 1, next(1) = 0$. So one restriction we could think of to avoid this is to keep $next(n) \neq 0$ for all n.

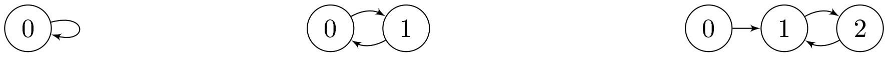

Figure 1: Valid number systems[2] without any condition on *next*

Is this enough? Not really, as we can still think of counterexamples, like $next(0) = 1, next(1) = 2, next(2) = 1$. Basically we have ensured that *next* doesn't loop back to 0. But we must ensure that it doesn't loop back at all (or even to the same number). How we shall do this is to add the restriction that *next* should not point to a number which has already been mapped to i.e. we make it a one-one function. Let's now add these conditions to our axioms:

1. $\exists n \ n = 0$
2. $\forall n \ \exists m \ (m = next(n))$
   (a) $\forall n \ next(n) \neq 0$
   (b) $\forall m \ \forall n \ next(m) = next(n) \implies m = n$

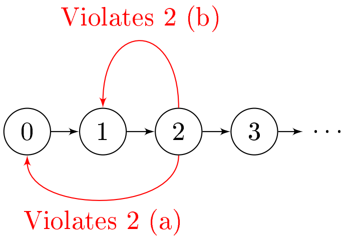

Figure 2: Diagrammatic explanation of why *next* always points to a new number

It turns out our axioms are still not complete. We have ensured that *next* always points to a new number, but we haven't really ensured that every natural number can be formed by applying *next* to 0 a finite number of times. Here are some counterexamples:

1. $\{0, \frac{1}{3}, \frac{2}{3}, \dots\}$ where $next(n) = n + 1$
2. $[0, \infty)$ where $next(n) = n + 1$

By repeatedly applying *next* to our growing chain, we should end up with the set of all natural numbers. A neat way of stating this is to just keep an axiom that induction itself works i.e. if a statement is true for $0, next(0), next(next(0)), \dots$ it must be true for all natural numbers. So here is our final set of axioms, which does lead only to our natural numbers:

[2] It's important to keep in mind what makes one number system different from another is how the nodes are linked, it's not about what symbol we keep for each node like 0, 1, 2

1. $\exists n \; n = 0$
2. $\forall n \; \exists m \; (m = next(n))$
   (a) $\forall n \; next(n) \neq 0$
   (b) $\forall m \; \forall n \; next(m) = next(n) \implies m = n$
3. $[P(0)][\forall n \; \{P(n) \implies P(next(n))\}] \implies [\forall n \; P(n)]$

Exercise 1.1. *Prove that $\forall n \; next(n) \neq n$. Can we have this statement instead of 2 (b) to define natural numbers?*

Solution. Proof by induction
Define $P(n)$ to be $next(n) \neq n$. $P(0)$ is true from 2 (a).
Also, $next(n) \neq n \implies next(next(n)) \neq next(n)$ as *next* is one- one (or contrapositive of 2 (b)). This is basically $P(n) \implies P(next(n))$.
From this we conclude $P(n)$ i.e. $next(n) \neq n$ for all n.
This can't be used instead of 2 (b). Counterexample: $next(0) = 1, next(1) = 2, next(2) = 1$.

Exercise 1.2. *Instead of keeping induction as an axiom, we could ensure that there are no other starting points for a chain other than 0. This might ensure that all numbers are part of the chain starting from 0.*

Can we replace axiom 3 with the following:
$\forall n \; n \neq 0 \iff \exists m \; next(m) = n$

Solution. No, we have a counterexample, take the set
$\{0, 1, 2, \dots\} \cup \{\dots, -1.5, -0.5, 0.5, 1.5, \dots\}$ where $next(n)$ is the standard $n + 1$.
It satisfies the new set of 3 axioms but aren't equivalent to natural numbers.

Exercise 1.3. *Is there a more concrete way to show that from axiom 3 that all natural numbers can be obtained composing next to 0 a finite (including 0) number of times?*

Solution. Let $P(n)$ denote n obtained composing $($next) to 0 a finite (including 0) number of times. $P(0)$ is obviously true. It's also clear that $P(n) \implies P(next(n))$, as if n can be written as $next(next(\dots(next(0))\dots))$, $next(n)$ can also be written that way by just composing one more *next* to the expression. This completes our proof.

Another way we can do this question is proof by contradiction. Assume there are some numbers not in the infinite chain starting from 0. We define our predicate to be true for values in the infinite chain starting from 0, and false for every other value.

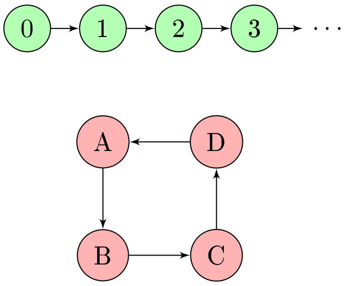

Figure 3: Our predicate is true for green cells and false for the red cells

This predicate satisfies $P(0)$ is true. It also satisfies $P(n) \implies P(next(n))$, because if $P(n)$ is true only for the green cells, and green cells point to only green cells. So induction steps are done, but $P(n)\forall n$ is false. So we have a contradiction.

2 Lecture 02

To extend our definition, let's define $\leq$ operator.

1. $\exists n \ \leq (0, n)$ is true
2. $\forall n \ \leq (next(n), 0)$
3. $\forall n \ \forall m \ [\leq (next(n), next(m)) \ = \leq (n, m)]$

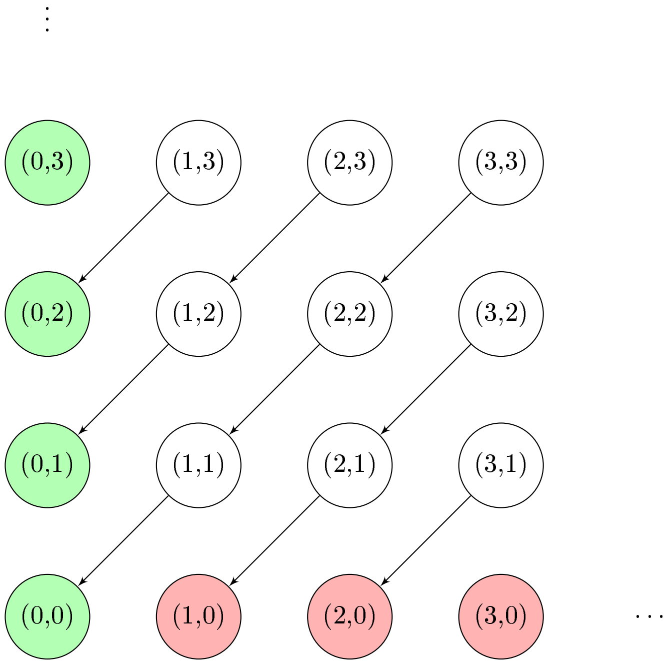

Figure 4: Diagrammatic representation of how $\leq$ is defined
$\leq$ is defined as true for green cells, false for red cells
$(A) \to (B)$ denotes (A) is defined by (B)

From the figure it's intuitive (hopefully) that $\leq (m, n)$ is defined for all m and n, (3) kind of gives a recursive definition. But how do we prove this? Since our predicate has 2 input variables, there is some sort of nested induction.
Take $P(m)$ to be $\forall n \ \leq (m, n)$ is defined.
$P(0)$ is defined from (1).
Now assume $\forall n \ \leq (m, n)$ is defined (which is $P(m)$)
We have to prove $\forall n \ \leq (next(m), n)$ is defined (which is $P(next(m))$)
The thing is, there's no direct way to proceed from here. It's clear that we somehow want to use (3) but we can't as we have $\leq (next(m), n)$ instead of $\leq (next(m), next(n))$. How we proceed is we take $Q(n)$ as $\leq (next(m), n)$ is defined, which is want we want to prove to complete the induction, and prove $Q(n)$ using induction itself! (Note that for the $Q(n)$ statement, m is fixed!) $Q(0)$ is true as $\leq (next(m), 0)$ is defined as false.
Now assume $Q(n)$ is true i.e. $\leq (next(m), n)$ is defined.
$Q(next(n))$ is $\leq (next(m), next(n))$ which is $\leq (m, n)$ which is defined, as it is $P(m)$. So we proved $\forall n \ Q(n)$, which is the inner induction complete.
This also completes the outer induction.

Exercise 2.1. *Prove that* $\leq(a,b) \wedge \leq(b,a) \implies a=b$

Solution. Nested induction on a, b.
Let $P(a)$ be $\forall b \ \leq(a,b) \wedge \leq(b,a) \implies a=b$
First we need to show that $P(0)$ is true. $\leq(0,b)$ is always true, also we can see that $\leq(b,0)$ is true implies b is 0 as if it's not the case, b can be written as $next(k)$ and $\leq(next(k),0)$ is false.
Now for the induction, assume $\leq(a,b) \wedge \leq(b,a) \implies a=b \quad (*)$
To prove: $\leq(next(a),b) \wedge \leq(b,next(a)) \implies next(a)=b$
Nested induction now, take the above as $P(b)$.

> $P(0)$ is a vacuous truth as $\leq(next(a),0)$ is false.
> Now assuming $P(b)$ we have to prove $P(next(b))$, which is
> $\leq(next(a),next(b)) \wedge \leq(next(b),next(a)) \implies next(a)=next(b)$
> But this is just equivalent to $(*)$, as LHS of the implication can be simplified by the recursive definition of $\leq$ and RHS of the implication can be simplified with one-oneness of *next*.
> So inner induction is complete.

This also completes outer induction as we have proved $\forall b \ P(b)$

Exercise 2.2. *Prove that* $\leq(a,b) \wedge \leq(b,c) \implies \leq(a,c)$

Solution. Nested induction again...
Let $P(a)$: $\forall b \, \forall c \ \leq(a,b) \wedge \leq(b,c) \implies \leq(a,c)$
$P(0)$ is true as RHS of implication is always true.
Now assume $P(a)$: $\forall b \, \forall c \ \leq(a,b) \wedge \leq(b,c) \implies \leq(a,c) \quad (*)$
To prove $P(next(a))$: $\forall b \, \forall c \ \leq(next(a),b) \wedge \leq(b,c) \implies \leq(next(a),c)$

> Let $Q(b)$: $\forall c \ \leq(next(a),b) \wedge \leq(b,c) \implies \leq(next(a),c)$
> $Q(0)$ is true as first term of LHS of implication is false.
> Now assuming $Q(b)$ we have to prove $Q(next(b))$, which is:
> $\forall c \ \leq(next(a),next(b)) \wedge \leq(next(b),c) \implies \leq(next(a),c)$
>
> > Let $R(c)$: $\leq(next(a),next(b)) \wedge \leq(next(b),c) \implies \leq(next(a),c)$
> > $R(0)$ is true as second term of LHS of implication is false.
> > Now assume $R(c)$, we have to prove $R(next(c))$, which is:
> > $\leq(next(a),next(b)) \wedge \leq(next(b),next(c)) \implies \leq(next(a),next(c))$
> > This can be reduced by the recursive definition to $(*)$ which is assumed as true.

That completes all the induction layers.

Exercise 2.3. *Prove that* $\leq(a,next(b)) \implies [\leq(a,b)] \vee [a=next(b)]$
Use this to prove $[\leq(a,b)] \wedge [\leq(b,next(a))] \implies [b=a] \vee [b=next(a)]$

Solution. Let $P(a)$: $\forall b \ \leq(a,next(b)) \implies [\leq(a,b)] \vee [a=next(b)]$
$P(0)$ is true as $\leq(0,b)$ is always true.
Now assuming $P(a)$, we have to prove $P(next(a))$.

> Let $Q(b)$: $\leq(next(a),next(b)) \implies [\leq(next(a),b)] \vee [next(a)=next(b)]$
> $Q(0)$: $\leq(a,1) \implies [\leq(a,0)] \vee [a=1]$
> We can first simplify $\leq(a,0)$ to $a=0$ using Exercise 2.1's property.
> Let's take $Q(0)$ as $R(a)$ and prove that using induction.

$R(0)$ is true as $\leq (a, 0)$ is true.
Now assuming $R(a)$ we have to prove $R(next(a))$.
$\leq (next(a), 1) \implies \leq (a, 0) \implies a = 0 \implies next(a) = 1$ so $R(next(a))$ is true
So $R(a)$ is true for all a.

Now assuming $Q(b)$ we have to prove $Q(next(b))$
But that can be reduced to just $P(a)$ which is assumed as true.
This completes the induction.

For the second part, we know :
$\leq (b, next(a)) \implies [\leq (b, a)] \vee [b = next(a)]$
And if $\leq (b, a)$ since we also know $\leq (a, b)$, $b = a$

We now define the addition function $add(m, n)$:

1. $add(0, m) = m$
2. $add(next(n), m) = next(add(n, m))$

It's not too hard to show this sufficiently defines addition by taking $P(n)$ as [$add(n, m)$ is defined] and using induction.

Exercise 2.4. *Prove that* $add(add(a, b), c) = add(a, add(b, c))$ *which is the associative property*

Solution. We can somehow avoid nested induction for once :)
Let $P(a)$ be $\forall b\ \forall c\ add(add(a, b), c) = add(a, add(b, c))$
To prove $P(0)$, $LHS = add(add(0, b), c) = add(b, c)$ and $RHS = add(0, add(b, c)) = add(b, c)$
To prove $P(next(a))$, assuming $P(a)$ is true:
$LHS = add(add(next(a), b), c) = add(next(add(a, b)), c) = next(add(add(a, b), c))$
$RHS = add(next(a), add(b, c)) = next(add(a, add(b, c)))$
And from $P(a)$ these both are equal.

Exercise 2.5. *Prove that* $add(a, b) = add(b, a)$ *which is the commutative property*

Solution. Lot of induction again :(
Let $P(a)$ be $\forall b\ add(a, b) = add(b, a)$
$P(0)$ is $\forall b\ add(0, b) = b = add(b, 0)$, this itself has to be done by induction on b.
Now assume $P(a)$ which is $\forall b\ add(a, b) = add(b, a) \quad (*)$
Basically whenever we have a in the add function we can swap stuff.
To prove: $P(next(a))$ which is $\forall b\ add(next(a), b) = add(b, next(a))$
We can simplify LHS a bit: $add(next(a), b) = next(add(a, b)) = next(add(b, a))$ from $(*)$

Let $Q(b)$ be $add(b, next(a)) = next(add(b, a)) \quad (**)$
$Q(0)$ is true as we get $LHS = RHS = next(a)$
Now assume $Q(b)$, we have to prove $Q(next(b))$
LHS for this is $add(next(b), next(a)) = next(add(b, next(a)))$
RHS is $next(add(next(b, a)))$ which is $next(next(add(b, a)))$
And from $(**)$ both of these are equal

This completes all the induction.

Exercise 2.6. *Prove that* $\leq (a, b) \implies \exists c$ *such that* $add(a, c) = b$

Solution. Let $P(a)$ be the above statement for all b.
$P(0)$ is true as $c = b$ works.
Now assume $P(a)$ is true. $(*)$
We have to prove $P(next(a))$, take this as $Q(b)$.

> $Q(0)$ is vacuously true as $\leq (next(a), 0)$ is false.
> Now assuming $Q(b)$ we have to prove $Q(next(b))$
> $\leq (next(a), next(b)) \implies \leq (a, b)$
> So from $(*)$ we know $\exists c$ such that $add(a, c) = b$
> But this also implies $add(next(a), c) = next(b)$
> This proves $Q(next(b))$ which completes all the induction.

3 Lecture 03

Rather than using induction, there's an equivalent way to define natural numbers called well-ordering principle. Here are the axioms:

1. $\exists n \; n = 0$
2. $\forall n \; \exists m \; (m = next(n))$
   (a) $\forall n \; next(n) \neq 0$
   (b) $\forall m \; \forall n \; next(m) = next(n) \implies m = n$
   (c) $\forall n \; [n = 0] \vee [\exists m \; n = next(m)]$
3. $\exists \; \leq$
   (a) $\forall n \; \neg \leq (next(n), n)$
   (b) $\forall P \; [(\exists n \; P(n)) \implies \exists n \; (P(n) \; \wedge \; \forall m (P(m) \implies n \leq m))]$

This might look like it's very complicated using predicate logic, so let's try to see what all this means. So the beginning is pretty much like the previous axioms, but 2(c) is new. It basically says every number is either 0 or is the *next* of some other number. We'll later see how this axiom helps in proving induction itself.

What does the third axiom say? It says there exists **some** predicate $\leq$, which is not necessarily the $\leq$ we saw in Lecture 02. But anyways there's some predicate $\leq$ which 'orders' the natural numbers. What exactly do we mean by that? 3(a) says *next* of any number is greater than it. 3(b) says that for all predicates P, if there is at least one number for which P is true, there will a 'smallest' number for which it is true. How we write this formally is that there is some n for which $P(n)$ is true and for every other m for which it is true, $n \leq m$.

Let's see how induction is true from these axioms. We prove induction by contradiction. Assume there is a predicate P such that $P(0)$ is true, and $P(n) \implies P(next(n))$. But $\forall n \; P(n)$ is false, that is there's some n for which $\neg P(n)$ is true. Let the smallest n that satisfies this be n_0 (we're using 3(b) here). $n_0 \neq 0$ as $P(0)$ is true. So from 2(c) there's m such that $next(m) = n_0$. Is $P(m)$ true? If it was, $P(m) \implies P(next(m))$, which would make $P(n_0)$ true.

So $P(m)$ is false, but haven't we just found a number smaller than n_0 which satisfies $\neg P(n)$, which contradicts well-ordering? From 3(a) we know $\leq (n, m)$ is false[3]. So from 3(b) we can get our contradiction, but remember the predicate we are using is $\neg P$ instead of P. We have n such that $\neg P(n)$, so 3(b) guarantees there exists n_0 such that $\neg P(n)$ is true, and for all other m that satisfies $\neg P(n)$, $\leq (n, m)$. So 3(a) and 3(b) form our contradiction.

Exercise 3.1. *We have seen how 2(c) was used in proving induction, but maybe even without it maybe we get only natural numbers? Is there a number system which isn't natural numbers but satisfies everything except 2(c)?*

Solution. In fact there are. $\{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$ form a number system.
Here $\leq$ is what you'd expect it to be, the numbers are arranged in order already, and ω is greater than all the natural numbers. $\leq$ satisfies all the properties it needs to, even things like the transitive property. But 2(c) forbids such things are there is no n such that $next(n) = \omega$. These are actually called the ordinal numbers. Thing is, we get many useful number systems if we make small changes to our axioms, for example if we remove $next(n) \neq 0$ we get modular arithmetic.

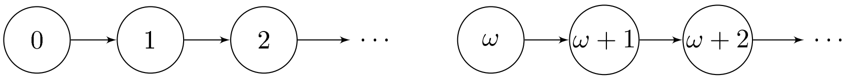

Figure 5: Valid number system without 2(c)

[3] Without 3(a) we can't actually conclude this, remember this isn't our familiar $\leq$, this is just an arbitrary predicate which satisfies well-ordering