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.

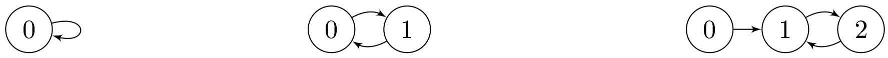

Figure 1: Valid number systems[2] without any condition on *next*

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) $\forall m \; \forall n \; next(m) = next(n) \implies m = n$

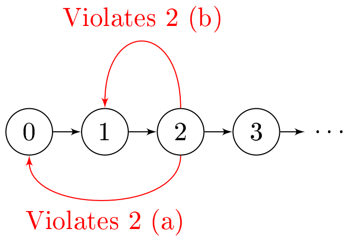

Figure 2: Diagrammatic explanation of why *next* always points to a new number

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. $\left\{0, \frac{1}{3}, \frac{2}{3}, \ldots\right\}$ 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 $0, next(0), next(next(0)), \ldots$ 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.

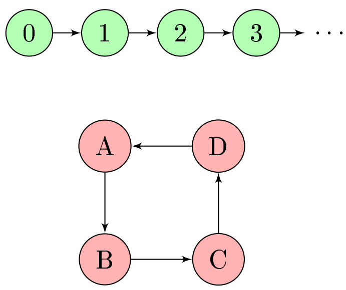

Figure 3: Our predicate is true for green cells and false for the red cells

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. $\forall n \ \forall m \ [\leq (next(n), next(m)) \ = \leq (n, m)]$

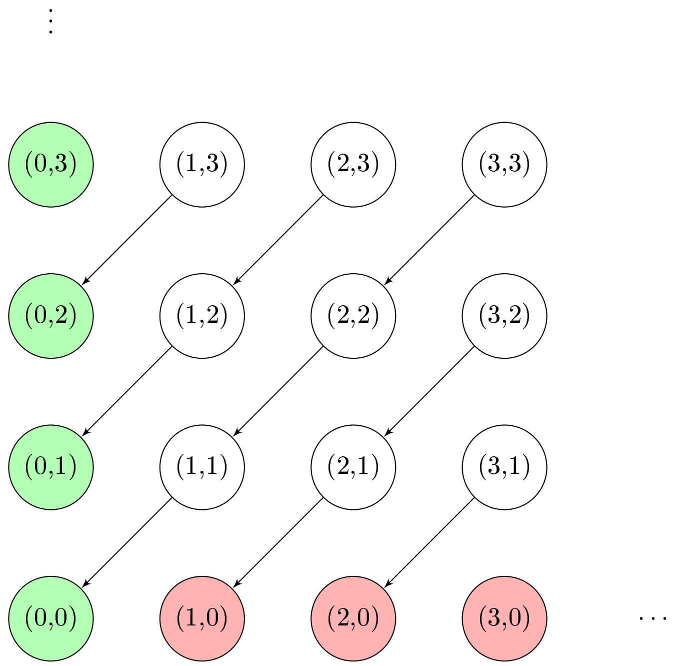

Figure 4: Diagrammatic representation of how $\leq$ is defined
$\leq$ is defined as true for green cells, false for red cells
$(A) \to (B)$ denotes (A) is defined by (B)

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 $\leq (a, b)$, $b = a$.

This exercise shows that there is no number in-between n and $next(n)$

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) $\forall n \; [n = 0] \lor [\exists m \; n = next(m)]$
3. $\exists \; \leq$
   (a) $\forall n \; \neg \leq (next(n), n)$
   (b) $\forall P \; [(\exists n \; P(n)) \implies \exists n \; (P(n) \; \land \; \forall m (P(m) \implies n \leq m))]$

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.

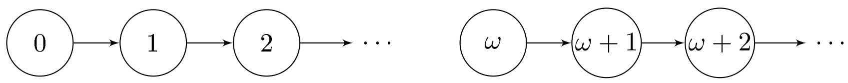

Figure 5: Valid number system without 2(c)

4 Lecture 04

The last lecture we saw the well-ordering principle, and showed how induction follows from it. Once that's true, we have basically confirmed that it also defines the natural numbers. Now let's try to prove the well-ordering principle from the induction axioms.

Proving 2(c) is not too hard using induction, actually the proof sounds silly. $P(0)$ is true as $0 = 0$[4]. And to prove $P(next(n))$ we need to find m such that $next(m) = next(n)$ and $m = n$ works for this.

Now for 3(a). Remember that for axiom 3, we just need to find one predicate $\leq$ which works, and we claim that the $\leq$ we defined in Lecture 02 works. 3(a) is also done by induction, take $P(n)$ to be $\leq (next(n), n)$ is false. $P(0)$ is true as $\leq (next(n), 0)$ is always false. $P(n) \implies P(next(n))$ is also clear as $\leq (next(next(n)), next(n)) \; = \leq (next(n), n)$.

3(b) is done by contradiction. So suppose there's a predicate P such that $P(n)$ is true for some n, but there's no smallest n for which $P(n)$ is true. How our contradiction will go is by showing $P(n)$ is false for all n. We will do this by showing if $P(0)$ is false, $P(1)$ is false, $\ldots$, $P(n)$ is false, this implies $P(next(n))$ is false[5].

We take $Q(n) : \forall m \; (m \leq n) \implies (\neg P(m))$ or in other words, $Q(n)$ says $P(k)$ is false for $0 \leq k \leq n$. What is $Q(0)$? $m \leq 0 \implies P(m)$ is false or simply, $P(0)$ is false. This is right as if $P(0)$ were true, 0 is clearly a smallest n for which $P(n)$ is true.

[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

[4] Where's my fields medal for observing this

[5] This is something called strong induction; for proving something for $next(n)$, instead of just assuming it for n, we assume it true for 0 to n. This is equivalent to induction actually

Now let's try to induct on $Q(n)$. Is it possible that $Q(n)$ is true and $Q(next(n))$ is false? This would mean there exists $m \leq next(n)$ such that $P(m)$ is true, at the same time $m \nleq n$, which means $m = next(n)$ (See exercise 2.3). But this m we found would then be a smallest k for which $P(k)$ is true. Why? Let k be such that $P(k)$ is true, we know $k \nleq n$ from $Q(n)$. So we have to show if $k \nleq n$, $m = next(n) \leq k$. This is equivalent to showing that $[k \leq n] \vee [next(n) \leq k]$ which can be shown by nested induction. So we got that it's impossible, $Q(n)$ has to imply $Q(next(n))$. This would then mean $Q(n)$ is true for all n which is the same thing as $P(n)$ is false for all n [6], which is a contradiction.

This proof does use a lot of English, but it's still correct and can be written in predicate logic, but that takes away the intuition.

Exercise 4.1. *Prove that* $[a \leq b] \vee [next(b) \leq a]$. *Is it possible for both of these to be true?*

Solution. Let $P(a)$ be $\forall b\ [a \leq b] \vee [next(b) \leq a]$.
$P(0)$ is true as $0 \leq b$. Now assume $P(a)$.
$P(next(a))$ is $\forall b\ [next(a) \leq b] \vee [b \leq a]$.

> Let $Q(b)$ be $[next(a) \leq b] \vee [b \leq a]$.
> $Q(0)$ is true as $0 \leq a$.
> $Q(next(b))$ is equivalent to $P(a)$ which is assumed to be true.

This completes the induction.

No it's not possible for both to be true.
$a \leq b$ and $b \leq next(b)$ implies $a \leq next(b)$.
This along with $next(b) \leq a$ means $a = next(b)$.
But $a = next(b) \leq b$ is clearly false, so we get a contradiction.

5 Lecture 05

We discuss some common mistakes made while doing induction proofs. Say you want to prove something for all objects which can have sizes 0, 1, 2, ... In the induction step, we can assume the property is true for all objects of size n. We must then show it's true for *all* objects of size $n+1$, not just *some* objects. Take the following example:
Every sequence of n numbers with sum $2n-1$ must contain an occurence of 1
$\forall n\ \forall S\ [L(s) = n] \wedge [sum(s) = 2n-1] \implies occurs(S, 1)$
This statement is clearly wrong, take the counterexample sequence $\{0, 3\}$. But here's a proof using induction which has a mistake. First let's define a sequence and define how induction works to prove something for all sequences.
Definition of sequence:

1. λ is a sequence which is an empty sequence
2. If S is a sequence, $insert(S, n)$ is a sequence for all numbers n

Induction for sequences:

1. $P(\lambda)$ is true
2. $\forall S\ [P(S)] \implies [\forall n\ P(insert(S, n))]$

[6] As $Q(n)$ implies $\neg P(n)$

Clearly, these aren't complete definitions, lot of details are assumed to be understood. But with enough conditions added, they will define sequences without any ambiguities.

So for our wrong proof we just do induction on n, not actually sequence induction. $P(0)$ is vacuously true as sum of sequence of length 0 is just 0. Now we do induction. Assume $P(n)$ is true. Now a sequence of length $n+1$ can be formed by $insert(S, 2)$ where S is a sequence of length n. Assuming our new sequence has sum $2(n+1)-1$, S will have sum $2(n+1)-1-2 = 2n-1$, so by induction 1 is in S, which means 1 is in our sequence of length $n+1$.

Why is this proof wrong? We haven't proved our statement for *all* sequences of length $n+1$, just for the sequences with ending element 2. We have only proved that there exists some sequence which has a 1, not all sequences have a 1.

So let's modify our statement to be true and then prove it properly by induction. Let's add the restriction that our sequence contains only *non-zero* numbers. Now our statement is true, because if it didn't contain a 1, the sum would be at least $2+2+\cdots+2 = 2n$. So we should be able to prove this by induction.

For $n=0$ again the statement is vacuously true. For $n=1$ it must be true as well because the only sequence with sum $2 \times 1 - 1$ is $\{1\}$. So let's assume it's true for sequences of length n. Every sequence of length $n+1$ is formed by inserting a number x to a sequence of length n, let's go case by case.

$x \neq 0$ from our conditions. If $x = 1$ we are done, our sequence has a 1. If $x = 2$, the rest of the sequence with length n has sum $2n-1$ so it has a 1 by induction, so far so good. But what if $x > 2$? Intuitively it's still true that the rest of the sequence should contain a 1 right, because the sum should be smaller than $2n-1$, but we can't exactly proceed by induction as our statement says nothing about such sequences. So to prove our statement, we actually make a stronger claim:

Every non-empty sequence S of length n with $sum(S) \leq 2n-1$ contains a 1

If we prove this statement by induction, we also solve the question as this is a stronger statement i.e. it is claiming something about a larger set of sequences. So let's just modify our proof to prove this statement. Again $P(0)$ is vacuously true.

$x \neq 0$ from our conditions. If $x = 1$ we are done, our sequence has a 1. If $x \geq 2$, the sum of the rest of the sequence is $\leq 2(n+1)+1-x \leq 2n-1$. So the rest of the sequence must contain a 1 by our induction assumption, this completes the induction.

The take away message is that in order to prove a statement by induction, sometimes we have to make a stronger statement which is easier to prove by induction.

Homework: Consider a set of $n+1$ positive numbers each of which is atmost $2n$. Prove that there exist 2 numbers such that one divides the other.

6 Lecture 06

We solve the homework question using well-ordering principle and proof by contradiction. It turns out that this method is more useful than direct induction for solving decently challenging questions, but is equivalent to induction. We assume n is the smallest number for which $P(n)$ is false (where $P(n)$ is what we want to prove), and use the fact that $P(k)$ is true for all $k < n$ to get some sort of contradiction showing that $P(n)$ is in fact true. Remember it's important to show a base case, here $n = 1$. In this case the only sets are {1, 1}, {1, 2} and {2, 2} so our statement is true.

So let n the smallest number for which $P(n)$ is false. Let the sequence for which it is false be $\{a_1, a_2, \ldots, a_n, a_{n+1}\}$ and also assume the numbers are in ascending order. What can we say about this sequence? Obviously none of the numbers are the same, if so they divide each other. Also look at the subsequence of this, $\{a_1, a_2, \ldots, a_n\}$. If all of the numbers were atmost $2n - 2$, the conditions for $P(n - 1)$ would be satisfied, which would mean two numbers divide each other. And if this is true for our subsequence, it's also true for the whole sequence, so we have a contradiction.

a_n must be greater than $2n-2$, and since all terms of are sequence are atmost $2n$ and distinct, $a_n = 2n - 1, a_{n+1} = 2n$. But we can actually still get a contradiction, if we consider the subsequence $\{a_1, a_2, \ldots, a_{n-1}, n\}$ [7]. Here all terms are atmost $2n-2$ as $a_{n-1} < a_n = 2n-1$ and $n \leq 2n - 2$. So we can apply $P(n - 1)$, x and y exist in the sequence such that $x|y$. Is it possible that neither of x, y are n? No, because then we would have 2 numbers in our original sequence which divide each other. So n is one of x, y. We can also say $y = n$, because x can't be n, there's no term in the sequence big enough for n to divide (except n itself). So some x divides n. We're not done though, as n is not part of our original sequence, but $a_{n+1} = 2n$ is! And if x divides n, x divides $2n$. So we still have 2 numbers in our original sequence which divide each other, so we have a contradiction.

Let's move to an even more challenging example.

Erdös-Ginzburg-Ziv Theorem: Any sequence of $2n - 1$ integers contains a subsequence of n elements, with their sum being a multiple of n.

Let n be the smallest number for which the statement is not true. Assume n is composite and $n = pq$ where $p, q > 1$. We show by contradiction that if the statement is true for p, q it is true for n (we take care of the case where n is prime later).

We have $2pq - 1$ numbers. Choose $2p - 1$ numbers from these. Now from our assumption, we can choose p numbers out of these with sum divisible by p. Take these numbers away and put them in a group G_1. And for the rest of the $p - 1$ numbers, put them back into our original sequence, to recycle them. Now again choose $2p - 1$ numbers from our original sequence, find p of them with sum divisible by p, put them away in a group G_2, and recycle the $p - 1$ numbers not chosen. How many groups can we form if we keep doing this? $2pq - 1 = (2q - 2)p + (2p - 1)$, so after finding $2q - 2$ groups, we have $2p - 1$ numbers left. We form a final group of size p, and throw away the $p - 1$ numbers.

Now have groups $G_1, G_2, \ldots, G_{2q-1}$ each with sum $k_1p, k_2p, \ldots, k_{2q-1}p$. Now what we do is find q numbers from $k_1, k_2, \ldots, k_{2q-1}$ with sum divisible by q, say the chosen numbers are $k'_1, k'_2, \ldots, k'_q$. Now think about choosing the numbers from these corresponding groups... We have q groups of p numbers each, so we have chosen pq numbers. And their sum is $(k'_1 + k'_2 + \cdots + k'_q)p = (kq)p$, so the sum is divisible by pq, thus we found our contradiction.

[7] Here n is not necessarily the greatest element, the elements aren't in order

Let's now deal with the case when n is prime. Firstly, let's reduce all numbers and our calculations *mod* n, because we only care about the remainders when divided by n. Can $\geq n$ numbers from the $2n-1$ be equal? In that case we're already done, n numbers from those obviously have a sum divisible by n. So let's assume each number appears less than n times.

We divide the numbers into n groups:

$$\begin{gathered}(a_1,b_1)\\(a_2,b_2)\\\vdots\\(a_{n-1},b_{n-1})\\(c)\end{gathered}$$

We also add the restiction that no 2 numbers of each group are equal *mod* n. Can we always do this? Just sort the numbers in ascending order, and put them in the groups in the order $a_1, a_2, \ldots, a_{n-1}, c, b_1, b_2, \ldots, b_{n-1}$. The only way you can have a repetition is if when you add many copies of a number, it somehow occupies every spot from a_i to b_i. But this would mean the number is present in our sequence at least $n+1$ times, which we already concluded is not the case.

We claim that there's a way to pick 1 number from each group such that the sum is divisible by n. How we show this, is by showing that there are at least n different sums we can make by choosing different numbers from each group. Assume we are working just with the first group. We have 2 different sums, a_1 and b_1. If we include the second group, we have 4 sums: $a_1+a_2, a_1+b_2, b_1+a_2, b_1+b_2$. But these sums may not be distinct *mod* n. So how do we proceed? We induct on the number of groups we are working with; we claim with i groups there are at least $i+1$ sums we can form. (Here i ranges from 1 to $n-1$, the n^{th} group has no choice.)

When $i=1$ it's obvious we have 2 distinct sums, a_1 and b_1 as $a_1 \neq b_1$ *mod* n. Now assume the statement is true for i, we have to show it's true for $i+1$. Let the $i+1$ sums we got from the first set of i groups be $\{s_1, s_2, \ldots, s_{i+1}\}$. Now by taking the $(i+1)^{th}$ group we get the sums:
$\{s_1 + a_{i+1}, s_2 + a_{i+1}, \ldots, s_{i+1} + a_{i+1}\}$
$\{s_1 + b_{i+1}, s_2 + b_{i+1}, \ldots, s_{i+1} + b_{i+1}\}$
It's clear that all elements inside one of these sets are distinct as all the s's are distinct. But how do we know 2 elements from different sets are distinct? Note that if there's just a single difference between both the sets, we will get $i+2$ new sums, and our induction is done. So how do we show each set isn't identical to each other *mod* n?

The trick is to show that the sum of numbers in each set aren't equal. If so, the difference of the sums would be 0 *mod* n. Note that the difference is just $(i+1)(b_{i+1} - a_{i+1})$ as all the s terms cancel. If this was 0 *mod* n, as n is prime, either $i+1$ or $b_{i+1} - a_{i+1}$ is divisible by n. But this isn't possible as $i+1$ is smaller than n [8] and by our construction of the groups, $a_{i+1} \neq b_{i+1}$ *mod* n. So it's impossible for both sets to be same, our induction step is true.

Now that our induction is complete, by choosing different elements we can get n different sums *mod* n, so basically we can get any sum *mod* n, including 0 *mod* n which is what we want. This completes the proof for the whole theorem.

[8] Strictly speaking i ranges from 1 to $n-1$, so why can't $i+1=n$? But our final induction is from $i=n-2$ to $i+1=n-1$ so we don't have to deal with this case