Class Notes for Lecture 3

The reading for Homework 2 is Rosen, sections 3.1-3.3.

Nearly all of the present and the next lectures, are devoted to one of the most important proof techniques for discrete structures: *mathematical induction*.
You've already seen this method in high school, but we want you to get really good at using it. It's really *practical*.

It's used for proving properties of natural numbers, and of objects defined with a recursive structure (trees, etc.).
It's also the basis of much of the work on *formal verification* of programs and algorithms.

Before starting, let's make some brief remarks about what we expect of your homeworks and about *mathematical definitions*.

5 What we Expect in your Proofs

In practice, people do not write out real proofs about interesting mathematical objects in a completely formal, step-by-step style. (Unless they are using a computer-aided theorem prover, which really does work step-by-step). Rather, they work more intuitively, skipping a lot of steps. Proof sketch.

But it is very important to work *correctly*, so that all the missing steps could really be filled in. It can be very hard to tell (impossible without some training) if a proof sketch is really valid. This course is designed to provide this training.

Basic objective: As in a scientific experiment, it has to be possible for someone else to "replicate" (ie, understand) your proof.

In the real world, anything that can be cited can be used without proof. But in homework, where everything we ask you to prove is already known, this defeats the purpose (namely, learning how to prove something that isn't already known).

We don't expect you to reprove arithmetic. Anything from high school math can be used without proof (unless stated otherwise).

Once something has been proved, you can use it again without proof, citing the theorem. Once it has been used so often as to become commonplace, you can even stop citing the theorem.

Do not introduce any new axioms!

When in doubt about whether something can be stated without proof, prove it!

Elements of a good proof:

- Correctness: first of all, a proof must be correct. Do not introduce more assumptions than the ones already stated in the hypothesis. Do not use unproved 'facts' and beware of fallacies, like the ones discussed in the previous lecture:
- Clarity: a good proof has nice structure, like a good program. It is broken up into separate "lemmas" that prove key intermediate properties. This makes it easy to understand the *reasons* why the whole thing works. It also makes it more likely that pieces can be reused.
- Brevity: a proof should be free of wordy arguments and repetitions.
- Elegance: a good proof has its pieces presented abstractly and generally. If you give an intermediate fact, state it as generally as you can. This avoids cluttering up a key piece of a proof with unnecessary hypotheses and arguments. It also makes it more likely you can reuse the piece.

  This is exactly analogous to what you do in designing subroutines for programs – make them general and abstract.

"The book proof" (Paul Erdos).

5.1 Some Actual Proofs...

If you make mistakes, you won't be alone!

Rigorous logical proof systems are nice, but no one really has the time or energy to be so careful. We prove things in a less formal way. The objective is to convince everyone that a truly rigorous proof could be built if someone took the time to do it. As a result, even great mathematicians can goof proofs.

- Andrew Wiles recently announced a proof of Fermat's Last Theorem. It was several hundred pages long. It took mathematicians months of hard work to discover it had a fatal flaw (so Wiles produced another proof of several hundred pages; this one seems to have convinced people for now).
- Kempe's invalid "proof" of the Four Color Theorem stood for 10 years (1879–1890)
- Gauss's 1799 Ph.D. thesis is usually referred to as being the first rigorous proof of the Fundamental Theorem of Algebra (every polynomial has a zero over the complex numbers). But it contains quotes like

> "If a branch of an algebraic curve enters a bounded region, it must necessarily leave it again. ... Nobody, to my knowledge, has ever doubted [this fact]. But if anybody desires it, then on another occasion I intend to give a demonstration which will leave no doubt."

Fields Medalist Steve Smale writes about this, calling it an "immense gap" in the proof that was not filled in until 1920, more than a hundred years later.

- In 1900 Poincare carelessly claimed a certain very simple topological characterization of the 3-dimensional sphere. Later realizing it was not so obvious, he demoted the claim to the status of a "conjecture" in 1904. The Poincare Conjecture is now one of the biggest open questions in mathematics (two Fields Medals have been given out for partial progress on it).

- In the 1940's Paul Erdos conjectured a certain combinatorial fact about arithmetic progressions (every set of natural numbers of positive density contains arbitrarily long arithmetic progressions), and offered $1000 for a proof or disproof. Endre Szemeredi proved the conjecture in 1972, but the proof was so long and badly written that Erdos was not sure whether to believe it. Finally, Andras Hajnal stepped in and wrote a much clearer version of the same proof, which was eventually published under Szemeredi's name. At some point during the write-up, Hajnal informed Erdos that he was now confident enough of the proof that he was willing to buy it from Szemeredi for $500.

- There's also the story of Newton waiting 20 years to publish the Principia because he didn't see how to prove that one could assume all the mass of a sphere to be concentrated at its center when calculating gravitational attraction. The proof ultimately required the invention of calculus ...

6 Definitions

When working in a logical proof system, we start with some basic concepts
E.g., start with natural numbers, define addition in term of increments.
We can continue, defining multiplication in terms of addition, then subtraction and division as inverses of addition and multiplication respectively, etc.

Definitions are not strictly necessary. One could always write out the defined object in terms of basic notions, but this would soon get messy. Thus, definitions are used to establish convenient shorthand.

6.1 What Definitions to Make?

Definitions call attention to something interesting that we expect to encounter frequently. Some typical examples from number theory:

- A *factor* of a natural number n is a positive integer that divides n without remainder.
- A *prime number* is a number ≥ 2 whose only factors are 1 and itself.

These are very useful definitions. They save us lots of typing:

Ex: Expanding the second: "A number ≥ 2 for which no number other than itself and 1 divides into it without remainder."

Prime numbers arise in many situations,
e.g., cryptography (RSA), so it's nice to have a short name for them.

There are many interesting theorems about prime numbers,
e.g., the Fundamental Theorem of Arithmetic states that all positive integers can be factored into primes, in a unique way.

In contrast, the following would not be a useful definition:

- A *K-number* is one that is divisible by 5 and by 7, but not by 13 or 43.

This definition also provides a shorthand, but it's not very useful. One would most probably not use it very often and there aren't many interesting results that depend on it.

6.2 Well-Definedness

It is important that a definition define a concept, unambiguously. We often express this by saying that the concept be *well-defined* by the definition.

Some examples of bad definitions – in which concepts aren't well-defined:

- $f(n)$ is the largest rational number (strictly) less than n

  Sometimes there is no such number.
  How to prove this?
  Construct a larger one by $\frac{n+f(n)}{2}$.

- $\sqrt{x}$ is the complex number y such that $y^2 = x$.

  $\sqrt{x}$ is not well defined by this definition, because it can take on two possible values. Pretending that it is well-defined and proceeding with usual manipulations leads to fallacies like:

$$\begin{aligned} 1 &= \sqrt{1} \\ &= \sqrt{(-1)(-1)} \\ &= \sqrt{(-1)}\sqrt{(-1)} \\ &= -1 \end{aligned}$$

6.3 Peano's Axioms

Peano's axioms are actually an attempt to *define* the natural numbers. Basically, gives a set of axioms that we want to be true for the naturals. These axioms turn out to be sufficient to capture everything that makes the natural numbers special—in other words, these axioms define a set that is basically unique.

We present Peano's axioms:

- As an example of axioms, rules of inferences.
- As a way of defining the natural numbers. Alternative: Just assume as understood, with all the usual basic notions: arithmetic operators, properties of those operators, etc.
- As an introduction to an important proof technique: Induction. This method is one of the most important methods for reasoning about computational objects. It's introduced here very formally, as an explicit axiom. We will do lots of very formal examples to make sure you understand it very well.

We will start here by doing some examples very formally, with all the steps. Then pretty soon, we start doing proof sketches. Our goal is to give you enough experience so you can write correct proof sketches, knowing that they can be completed.

Peano's Axioms define the natural numbers $\mathbb{N}$. We use two primitive symbols: 0 and $'$ (successor).

1. $0 \in \mathbb{N}$
2. $(\forall x \in \mathbb{N}),\ x' \in \mathbb{N}$
3. $\forall x, y \in \mathbb{N},\ x' = y' \implies x = y$ (no two numbers have same successor)

4. $\neg\exists x \in \mathbb{N}$ such that $0 = x'$ (equivalently, $\forall x \in \mathbb{N}, x' \neq 0$)

5. (Induction) $\forall S \subseteq \mathbb{N}$, if $0 \in S$ and $\forall x \in \mathbb{N}, (x \in S \implies x' \in S)$, then $S = \mathbb{N}$.

Notation: $1 = 0'$, $2 = 1'$, etc.

Let's discuss these axioms a bit. E.g., the first four are satisfied by the nonnegative reals. It is the fifth, the important Induction Axiom, that ensures that we generate all of $\mathbb{N}$ by starting with 0 and taking successors.

Have we hit bottom? Not really. We have used *naive set theory*. Set theory axioms are harder than you might think.

Peano states axiomatically that $\mathbb{N}$ has these 5 properties. From set theory, you can prove $\mathbb{N}$ *exists*. Then these properties become definitions instead of axioms.

Real numbers can be defined by about 10 axioms.

Later, we will see how to build other definitions, e.g. addition and multiplication, atop the successor operator of the Peano axioms.

6.4 Using Peano's Axioms

Peano's induction axiom is extremely powerful. It lets us prove just about everything known about the natural numbers.

Theorem 6.1 $(\forall x) x \neq x'$.

Proof. Let $S = \{x \mid x \neq x'\}$. $0 \in S$, since $0 \neq x'$ for any x including 0. Furthermore,

$$\begin{aligned} x \in S &\implies x \neq x' \\ &\implies x' \neq x'' \\ &\implies x' \in S \end{aligned}$$

(In the second implication we apply the contrapositive of axiom 3, taking $y = x'$).

Thus (by the syllogism inference rule and universal generalization) $x \in S \implies x' \in S$. Thus, by the induction axiom, $S = \mathbb{N}$. ■

7 Real World Proofs By Induction

7.1 What They Are

We have just seen an induction axiom given as part of the definition of $\mathbb{N}$, and used it in a very formal way to prove something about $\mathbb{N}$.

Induction is a method used to prove that some property holds for all natural numbers, or more generally, for all elements of some set defined by base elements plus generation rules. (E.g., well formed formulas, binary trees.)

For starters, we'll consider natural numbers.
Simple induction is expressed by Peano's Induction Axiom:

- (Induction) $\forall S \subseteq N$, if $0 \in S$ and $\forall x \in \mathbb{N}, (x \in S \implies x' \in S)$, then $S = \mathbb{N}$.

Or, restating in terms of predicates instead of sets,
(and writing $n+1$ instead of n'):

> Let $P(n)$ be a predicate, and suppose
>
> - $P(0)$
> - $(\forall n \in \mathbb{N})\ (P(n) \implies P(n+1))$.
>
> Then $P(n)$ is true for all natural numbers n.

This is equivalent to the previous induction rule (Peano axiom 5): simply define S to be the set of numbers $n \in \mathbb{N}$ for which $P(n)$ is true. If we prove $S = \mathbb{N}$, then we have proved $(\forall n \in \mathbb{N}) P(n)$.

That is, to prove a property P for all natural numbers, it's enough to prove it for 0, then to show that truth for any n implies truth for $n+1$. Why does this say it's true for all of $\mathbb{N}$? Well, it's true for 0 by some proof of $P(0)$, then for 1 because it's true for 0, then for 2 because it's true for 1, etc.

Note, we don't *prove* that induction is a valid rule – we *assume* it as an axiom. There's no way to prove it from the other axioms (to demonstrate, consider the positive reals with $x' = x + 1$. They obey the first 4 axioms but not the fifth).

Think of dominoes:
Want to say that all the dominoes in a row fall down. Assume we push the first one (domino 0) down. Then suppose that any domino that falls causes the next to fall. Then all fall.

A proof by induction is *not* a circular proof (which is a fallacy). We do *not* prove that $P(n) \implies P(n)$.

Simple variant:
In order to prove $P(n)$ for all $n \geq 1$, just prove

- $P(1)$
- $(\forall n \geq 1)\ (P(n) \implies P(n+1))$.

Same for any starting value.

In most of the rest of the class, we give examples of inductive proofs.

Although we've expressed induction as an axiom, we are not going to be so formal here in our reasoning about $\mathbb{N}$.
Besides the simple concepts and facts mentioned in the Peano axioms, we are going to use other operations like $+$, $\times$, etc., relations like $<$, and lots of basic properties from elementary school arithmetic.

We will get formal again (briefly) in the next lecture, in order to consider the relationship between the Peano induction axiom and some alternative induction axioms.

Vital: When doing an induction proof, write down exactly what P is!

7.2 Simple Number Properties

Simple induction. Just numbers.

Example 1 Prove for all $n \in \mathbb{N}$, $n^3 - n$ is divisible by 3.

Let $P(n)$ be the predicate $n^3 - n$ is divisible by 3.

$P(0)$: 0 is divisible by 3.
Yes. 0 is divisible by everything, by convention.

Assume $P(n)$, prove $P(n+1)$:
$P(n)$ says $n^3 - n$ is divisible by 3.
$P(n+1)$ says $(n+1)^3 - (n+1)$ is divisible by 3.
Now, $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1)$
$= (n^3 - n) + 3(n^2 + n)$.

The first term divisible by 3, by inductive hypothesis.

The second term is obviously divisible by 3.
Therefore, the sum is divisible by 3.

Note: We assume $P(n)$, but we make no assumptions about the value of n. The proof $P(n) \implies P(n+1)$ has to work regardless of what n is.

Example 2 Show $2^n \geq n^2$ if $n \geq 4$.

$P(n) : 2^n \geq n^2$ if $n \geq 4$
Here we do an induction with base case $n = 4$, thus proving $2^n \geq n^2$ for all $n \geq 4$.

BASE: $2^4 = 4^2$.
INDUCTIVE STEP: Assume $2^n \geq n^2$ and $n \geq 4$.
How?
We can prove it as a lemma by doing another induction:
Let $Q(n) : n^2 \geq 2n + 1$
$Q(4)$ is true.
We have $Q(n) = \{n^2 \geq 2n + 1\}$.
$Q(n+1)$ says $(n+1)^2 \geq 2(n+1) + 1 = 2n + 3$.
$(n+1)^2 = n^2 + 2n + 1$
$\geq 2n + 1 + 2n + 1$ (by inductive hypothesis)
$= 4n + 2$.
This is $\geq 2n + 3$ because $n \geq 4$, as needed.

7.3 Die Hard

Here's an example of induction, where we will have **to strengthen the hypothesis** in order to prove the statement. This is an important technique in induction.

In Die Hard III (Die Hard with a Vengeance), Bruce Willis and Samuel Jackson had to disarm a bomb using the old boy scout trick of measuring four gallons of water using a three-gallon jug and a five-gallon jug. (You can figure out how this goes.)
The jugs are initially empty.
They have access to a reservoir of water.
They need to pour out four gallons into a special container.
The only operations they are permitted are those of pouring water using the three-gallon jug and the five-gallon jug.
Whenever they pour water from a jug, they either have to pour out all the water in the jug, or pour until the receptacle into which the water is being poured becomes full.
They can also fill either jug from the reservoir.

In Die Hard IV, they again have to pour out four gallons, this time using a 3 gallon and a 6 gallon jug. The movie is not likely to have a happy ending, because:

Theorem 7.1 Using a 3 gallon jug and a 6 gallon jug and the operations above, it is not possible to measure 4 gallons.

We want to prove this by induction, but there is no obvious inductive hypothesis here.
We could try:
$Q(n)$: After n operations, it's impossible for either jug to contain exactly 4 gallons.
Then $Q(0)$ is fine – both are empty at first.
Inductive step: Assume $Q(n)$, prove $Q(n+1)$. ???
But just knowing $Q(n)$ isn't enough to prove $Q(n+1)$:
Maybe it's possible for the 6 gallon jug to contain 1 gallon after n operations. (The inductive hypothesis doesn't rule this out – only rules 4 out.)
If this can happen, then one more operation could yield 4 gallons.

However, it *is* possible to prove this theorem by induction. The trick, though, is to *strengthen* the property to be proved so that it:

1. Implies the property that we really want, and
2. Can be proved by induction.

Very important method.
Here, the strengthened property that works is:
$P(n)$: After n operations, the number of gallons in each jar is divisible by 3.

Proof. Prove P by induction on n, the number of operations.
BASE CASE:
$P(0)$ is clearly true since the containers are initially empty.
INDUCTIVE STEP:
Assume $P(n)$ is true.
Consider $(n+1)$ operations.
At the end of the first n operations, by the inductive hypothesis, all containers contain a number of gallons divisible by 3.
There are several possibilities for the $(n+1)$st operation:
A jug could be filled from the reservoir, or emptied into the reservoir, or one jug could be poured into the other.
In any of these cases, the resulting number of gallons in both containers continues to be divisible by 3.
This completes the proof by induction (go through the cases to convince yourself).

Since 4 is not divisible by 3 it is not possible to measure 4 gallons. ∎