CISC-102
Winter 2016
Lecture 19

Methods of Proof

Axioms

Definition: An *axiom* is a statement or proposition that is regarded as being established, accepted, or self-evidently true.

Mathematics is a system created by humans, and can be developed in its entirety by a small collection of axioms that are assumed to be true.

Euclid of Alexandria (300 BC) developed an axiomatic approach for geometry starting with only 5 axioms.

In this course we have been making quite a few assumptions about what we accept as true. In practice it would be excruciating to prove everything from basic principles. There is an estimate that proving 2+2=4 from basic principles requires more than 20,000 steps.

Prove that 2 | a(a+1), for all a ∈ ℕ.

An informal proof of this result could be the observation that either a or (a+1) must be divisible by 2, and therefore the product a(a+1) must also be divisible by 2.

However, in our studies we saw a very similar example that provides a "template" for proving the result.

That is: Let a ∈ ℕ show that 3 | a(a+1)(a+2), that is the product of three consecutive integers is divisible by 3.

Familiar facts from high school math, as well as results that we have seen this term and used repeatedly can be assumed without further proof.

In practice for a course like this there is usually a very similar proof that you have seen that can be used as a template. And this will implicitly use assumptions that you may use.

Logical Deduction

We use logical deduction in a natural way to solve puzzles of many different forms, ranging from playing Sudoku to solving murder mystery's.

In mathematics logical deduction is used as we proceed from step to step in a proof.

The basic rule that we use, as described in formal logic, is:

$p, p \rightarrow q \vdash q$

We can verify that this is a valid argument. We can also reason this out informally as:

If p is true, and p implies that q is true, then we may conclude that q is true.

As an aside, this *inference rule* is named "*modus ponens*" by logicians, and is also known as the "law of detachment". You can look this up if you are interested but as far as this course goes, I think the informal explanation is sufficient.

Proof Templates

Proof by cases.

Proofs by cases can be used for the following results:

1. Prove that 2 | a(a+1), for all a $\in \mathbb{N}$.

2. Prove that 3 | a(a+1)(a+2), for all a $\in \mathbb{N}$.

The basic template is to partition all possible outcomes into individual cases that are easier to handle separately than together.

Consider the following problem:

Prove that 6 | a(a+1)(a+2), for all a ∈ $\mathbb{N}$.

Proof: We can use case analysis from the previous two results (result 1, result 2) as a template. We already know by result 2 that:

3 | a, or 3 | a+1 or 3 | a+2 so.

Case 1. 3 | a, then by result 1. 2 | (a+1)(a+2). Thus 6 | a(a +1)(a+2).

Case 2. 3 | a+2, then by result 1. 2 | a(a+1). Thus 6 | a(a +1)(a+2).

Case 3. 3 | a+1.

Case 3.1 a and a+2 are both even, then 2 | a and 3 | a +1, so 6 | a(a+1)(a+2).

Case 3.2 a and a+2 are both odd, therefore a+1 is even, so 2 | a+1, so a+1 is divisible by 2 and 3 and we are back to square 1. OOPS!

Prove that 6 | a(a+1)(a+2), for all a ∈ $\mathbb{N}$.

Here is a very slick proof:

Proof: Observe that a(a+1)(a+2) = (a+2)!/(a-1)! which is equal to:

$$6\binom{a+2}{3} = 6\frac{(a+2)!}{3!(a-1)!}$$

We know that $\binom{a+2}{3}$ is an integer so we conclude that: 6 | a(a+1)(a+2). □

Prove that a(a+1)(a+2)(a+3) is divisible by 24.

Let's try the previous solution as a template.

Proof: Observe that a(a+1)(a+2)(a+3) = (a+3)!/(a-1)! which is equal to:

$$24\binom{a+3}{4} = \frac{24(a+3)!}{4!(a-1)!}$$

We know that $\binom{a+3}{4}$ is an integer so we conclude that: 24 | a(a+1)(a+2)(a+3). □

Theorem: Every collection of 6 people includes 3 people who have all met each other, or 3 people who have never met.

Proof:
Let x denote one of the 6 people. Now consider the number of people from the other 5 who have met or have not met x.

There are two cases to consider.

- case 1: There are 3 or more people who have met x.
    - case 1.1 Among those who have met x, none have met each other, so this satisfies the requirements of the theorem.
    - case 1.2 Among those who have met x, at least one pair have met each other. Since they have also met x, this satisfies the requirements of the theorem

- case 2: There are 3 or more people who have not met x.
    - case 2.1 Those who have not met x, have all met each other, and this satisfies the requirements of the theorem.
    - case 2.2 Amongst those who have not met x, there are 2 (or more) who have not met each other. That pair together with x satisfy the requirements of the theorem.

Thus we have proved that every collection of 6 people includes 3 people who all have met each other, or 3 people who have never met by using an exhaustive case analysis. □

Note: This collection of 6 people can be thought of as a set of 6 elements. People either have met or have never met, there is no other possibility. In general the “met” property could be any arbitrary (Boolean) function of two elements of the set that returns true or false.

Direct Proof:

Let a be a natural number. If a is even then a+1 is odd and a+2 is even.

Proof: If a is an even natural number we have

$a = 2m$ for some natural number m.

then

$a + 1 = 2m + 1$ implying that a is odd,

and

$a+2 = 2m + 2 = 2(m+1)$ implying that a is even. □

Indirect Proof

If a is an integer and a^2 is odd then a is also odd.

Proof: If a^2 is odd we have:

$$a^2 = 2m + 1$$

Now a can be written as:

$$a = \sqrt{2m + 1}$$

and I don't know how to continue this proof.

Sometimes the contrapositive leads to a simpler proof.

The proposition is:

If a is an integer and a^2 odd **then** a is also odd.

or for a an integer: a^2 odd → a odd

The contrapositive would be

not a odd → not a^2 odd or

a even → a^2 even.

If a is an integer and a^2 is odd then a is also odd.

Proof: We will prove that the contrapositive is true. That is, let a be an integer, if a is even then a^2 is even.

We know in general that if $b \mid c$ then $b \mid mc$ for any integer m. Therefore as a special case we have $2 \mid a$ so $2 \mid a^2$. Therefore we can conclude that if a^2 is odd then a must also be odd. □

An *indirect proof* proves the contrapositive of the proposition.

Proof by Contradiction.
Let a be an integer, if a^2 is even then a is even.

How would we prove this proposition?

Proof: Suppose a^2 is even and a is odd. If a is odd then we have the equation: $a = 2m + 1$, where m is an integer. Now square both sides to get the equation:

$$a^2 = 4\,m^2 + 4m + 1. \qquad (1)$$

Let $n = m^2 + m$, and notice that n is an integer. Thus equation (1) simplifies to:

$$a^2 = 4\,n + 1$$

and is odd. Assuming a^2 is even and a odd leads to a contradiction, so we conclude that if a^2 is even then a is even. □

Proof by the Pigeon Hole principle:

Prove that at least 5 days of the month of March fall on the same week day.

Proof: Imagine that there are 7 pigeon holes with 4 chairs inside each. There are 31 days in March so at most 28 days can be seated on the chairs. Therefore there are at least 5 days that fall on the same day of the week. □

The pigeon hole principle is a particular case of a larger method of proof called proof by contradiction.

Proof by Contradiction

We know that $p, p \rightarrow q \vdash q$ that is if p is true and $p \rightarrow q$ is true then the logical consequence is that q must be true.

Suppose we know that a proposition is false, and we want to prove that p is true. Consider this round about method of proving that p is true.

$\neg p, \neg p \rightarrow F \vdash p$

We can verify this with a truth table.

p	$\neg p$	$\neg p \rightarrow F$	$\neg p \wedge \neg p \rightarrow F \rightarrow p$
T	F	T	T
F	T	F	T

Prove that at least 5 days of the month of March fall on the same week day.

Let p be the proposition that 5 or more days of the month of March fall on the same day of the week. Now ¬p is the proposition that at most 4 days of the month of March fall on the same day of the week. The false proposition is $7 \times 4 \geq 31$. ($7 \times 4 \geq 31$ is the same as saying that every day in March gets to sit in a chair in the pigeon holes.) The assumption that at most 4 days of March fall on the same day of the week leads to a contradiction. □

We can further dissect the concept of proof by contradiction by taking a closer look at a previous problem.

Let a be an integer, if a^2 is even then a is even.

Let p(a) denote the proposition a^2 even $\rightarrow$ a even

The assertion can be re-written as:

$$\forall a,\ a \in \mathbb{Z},\ p(a)$$

and its negation:

$$\neg(\forall a,\ a \in \mathbb{Z},\ p(a)) \equiv \exists a,\ a \in Z, \neg p(a)$$

In our proof by contradiction we showed that:

$$\neg(\forall a,\ a \in \mathbb{Z},\ p(a)) \equiv \exists a,\ a \in Z, \neg p(a) \equiv \text{False}$$

and this implies

$$\forall a,\ a \in \mathbb{Z},\ p(a) \equiv \text{True}$$

Prove that $\sqrt{2}$ is irrational.

Proof: We show that the assumption that $\sqrt{2}$ is rational leads to a contradiction.

If $\sqrt{2}$ is rational then we can write it as the quotient a/b where a,b are both integers. Furthermore, we assume that a/b have no common factors, that is we reduced the quotient to lowest terms. Thus:

$$\sqrt{2} = a/b$$

square both sides of equation:

$$2 = a^2/b^2$$

now multiply both sides by b^2:

$$2\,b^2 = a^2.$$

Therefore a^2 is even implying a is even.
If a is even we can write it as $a = 2m$ for some integer m.
Now we get

$$2b^2 = 4m^2.$$

Divide both sides by 2:

$$b^2 = 2m^2.$$

So b^2 is even implying b is even.

We have established that both a and b are even, but when we started we said that a and b have no common factors. Thus we have established a contradiction to the assertion that $\sqrt{2}$ is rational, so we conclude that $\sqrt{2}$ is irrational. □

Recall we saw a proof by contradiction when we studied prime factorization. (Lecture 10, Feb. 4)

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof:

(1) Suppose there is an integer $k > 1$ that is the largest integer that is the product of primes. This then implies that the integer k+1 is not prime or a product of primes.

(2) If k+1 is not prime it must be composite and:
$k+1 = ab,\ a,b \in \mathbb{Z},\ a,b \notin \{1,-1, k+1, -(k+1)\}$.

(3) Therefore, $|a| < k+1$ and $|b| < k+1$.
So |a| and |b| are prime or a product of primes.

(4) Since k+1 is a product of a and b it follows that it too is a product of primes.

(5) Thus we have contradicted the assumption that there is a largest integer that is the product of primes, and we can therefore conclude that every integer n > 1 is either prime or written as a product of primes.

In proving that “every integer $n > 1$ is either prime or can be written as a product of primes” we used the well ordering principle to justify the fact that if there is an integer that is the product of primes then there is a least integer that is the product of primes. Well ordering is also implied when we argue that we can express a rational number in lowest terms.

Some additional problems.

1. Prove $|xy| = |x|\,|y|$ for all integers x and y.
2. Prove that the sum of two rational numbers is rational.
3. Prove that if $3n+2$ is odd, then n is odd.