CS 70 Spring 2006 — Discrete Mathematics for CS, Vazirani — Lecture 2

Guest Lecturer: Sara Robinson (aras@cs.berkeley.edu)

About the game from last time

You, as a class, made three key insights:

- If a player gets an even number, s/he can always give the other player an odd number.
- If a player gets an odd number, s/he *must* give back an even number.
- ”Eventually,” someone gets 1 and loses.

To prove a rigorous theorem about the game requires induction, next week’s topic, but you’ll be asked to prove something informally on the first homework. Part of the task will be to figure out what theorem to prove.

Back to Quantifiers and Negations

Some Definitions:

$\{0,1,2,\ldots\} = \mathbf{N}$: the natural numbers.

$\{\ldots,-2,-1,0,1,2,\ldots\} = \mathbf{Z}$: the integers.

$\{1,2,\ldots\} = \mathbf{Z}^+$: the positive integers.

Let’s do a quick warm-up. Tell me whether each of the following statements is true or false:

- $(\exists n \in \mathbf{Z}^+)(n$ is prime $\implies n$ is divisible by 9.). TRUE, in a stupid way. Take $n = 4$. This is why you never see theorems of the form $(\exists x)(P(x) \implies Q(x)$.
- $(\forall n \in \mathbf{N})(n^2+n+41$ is prime.) FALSE, because the negation is true: $(\exists n \in \mathbf{N})(n^2+n+41$ is not prime.), namely $x = 41$.
- $(\forall x in \mathbf{R})(\exists y \in \mathbf{R})(xy = 1)$ FALSE, because $(\exists x in \mathbf{R})(\forall y \in \mathbf{R})(xy \neq 1)$, namely $x = 0$
- $(\forall x in \mathbf{R}^+)(\exists y \in \mathbf{R}^+)(xy = 1)$ TRUE. For any given x, take $y = \frac{1}{x}$, which is well-defined and in $\mathbf{R}^+$. Then $xy = x\frac{1}{x} = 1$

Proofs

Many of the unenlightened believe proofs to be pointless formal exercises. Far from it. We all like to assert things, and few of us like to say things that turn out to be false. Proof means never having to say you’re sorry—it provides a means for *guaranteeing* your claims once and for all. [1]

What we would like to do now is to make these concepts more precise.

Proofs in mathematics and computer science (as opposed to law and politics) require a precisely stated proposition to be proved. That was why we discussed propositions in Tuesday's lecture.

What is a proof? Recall that an axiom is a statement we accept without proof. (We have to start somewhere). A formal proof is a sequence of statements, ending with the proposition being proved, with the property that each statement is either an axiom or its truth follows easily follows from the fact that the previous statements are true. Indeed, the fact that each statement follows from the previous statements, can be checked by a (simple and efficient) computer program.

A formal proof for all but the simplest propositions is too cumbersome to be useful. In practice, mathematicians routinely skip steps to give proofs of reasonable length. How do they decide which steps to include in the proof? The answer is sufficiently many steps to convince themselves that they could fill in all the details if challenged, and sufficiently many steps to convey to the reader how to fill in all the details (this of course depends upon the knowledge and skill of the audience. So in practice proofs are socially negotiated).

There is a crucial aspect about proofs that the previous formal description left out. Proofs provide insights into why a proposition is true. Usually the proof of a proposition contains one or more major ideas. These are the aspects of proof that we will emphasize in this course. During the first couple of weeks of the semester, the proofs we will write will be relatively more formal. As you get more comfortable with the notion of a proof (and more adept at filling in missing details), we will relax a bit. Our proofs will then begin to emphasize the insights and creativity embodied in the main idea that makes a proof work, and leave out the relatively trivial side points. A proof, for the purposes of this class, is eventually a convincing argument. Convincing to whom? First, to you, the author, second, to your classmates, third, to your professor and your TA.

Some definitions:

THEOREM

A **theorem**, informally speaking, is a true proposition that is guaranteed by a proof. If you haven't a clue whether a particular statement is true or false, call it a proposition. If you think it's true but can't prove it, call it a **conjecture**, essentially an educated guess.

CONJECTURE

LEMMA

AXIOM

A concept useful for writing up complicated proofs is that of a **lemma**, which is a little theorem that you use in the proof of a bigger theorem. An **axiom** is a statement we accept without proof. (We have to start somewhere).

Now let's look at some examples:

Direct Proof

Let n be a postive integer less than 1000.

Theorem 2.1: *If the sum of the digits of n is divisible by 9, then n is divisible by 9.*

Note: The theorem is true for arbitary n. We're just doing the three digit case to keep the notation from getting distracting.

This is just a straightforward statement of the form $(\forall n)(P(n) \implies Q(n))$. To prove that it holds for every n, we just show that whenever $P(n)$ is true for some n, $Q(n)$ must be true as well.

Proof:

[1] "What about incorrect proofs?" you may ask. An incorrect proof is not a proof, any more than artificial grass is grass.

Suppose we have n such that the sum of the digits of n is divisible by 9. Let a be the hundred's digit of n, b the ten's digit, and c the one's digit. Then $n = 100a + 10b + c$. Now suppose that the sum of the digits of n is divisible by 9. Then,

$$a+b+c = 9k, k \in \mathbf{Z}$$

. Adding $99a+9b$ to both sides of the equation, we get

$$100a+9b+c = n = 9k+99a+9b = 9(k+11a+b)$$

So n is divisible by 9.

□

Notice the □ marking the end of a proof.[2]

In this case the converse of the theorem is also true: If n is divisible by 9, the sum of its digits is divisible by 9, too. In other words, the sum of the digits of n is divisible by 9 if and only if n is divisible by 9. In general, to prove $P \iff Q$, you have to do two proofs: You must show that $P \implies Q$ and then, separately, you must also show that $Q \implies P$. In this particular case, however, one proof just reverses the steps of the other so it's possible to prove both directions at once:

Theorem 2.2: *n is divisible by 9 iff the sum of the digits of n is divisible by 9.*

Proof:

n is divisible by 9
$\iff n = 9l, l \in \mathbf{Z}$
$\iff 100a + 10b + c = 9l, l \in \mathbf{Z}$
$\iff 99a + 9b + (a+b+c) = 9l, l \in \mathbf{Z}$
$\iff a+b+c = 9l - 99a - 9b, l \in \mathbf{Z}$
$\iff a+b+c = 9(l - 11a - b), l \in \mathbf{Z}$
$\iff a+b+c = 9k, k \in \mathbf{Z}$ $(k = l - 99a - b)$
$\iff a+b+c$ is divisible by 9 □

Be *very careful* when proving a biconditional statement in this manner. For the proof to be legitimate, the steps have to make just as much sense backwards as forwards. Go back and read the proof backwards, starting with the last line and ending with the first, and check for yourself that it works.

Proof by Contrapostion

In the last lecture, we learned that a statement of the form $P \implies Q$ is logically equivalent to its contrapositive: $\neg Q \implies \neg P$. This means that for all possible combinations of truth values of inputs P and Q, the two statements have the same truth values. Sometimes proving the contrapositive of a statement is easier than proving the statement directly. Here is an example that will come in handy on your homework. We'll call it a theorem for now, but you can use it later as a lemma.

Let n be an integer and let d be a divisor of n. (From now on, we'll use the notation $d|n$, read as "d divides n," to say that d is a divisor of n.)

Theorem 2.3: *If n is odd then d is odd.*

[2] In better days, people wrote QED instead, standing for for *quod erat demonstrandum*—Latin for *which was the thing to be demonstrated.*

Proving this directly would be difficult. We would assume n is odd but what then? Proving the contrapositive of the statement, however, is straightforward. The contrapositive is: If d is even then n is even: $\neg Q \implies \neg P$.

Proof: We will prove the contrapositive: if d is even then n is even.

Suppose d is even, then (by definition) $d = 2k$ for some $k \in \mathbf{Z}$.
Because $d|n$, $n = dl$, for some $l \in \mathbf{Z}$.
Combining these two statements, we have $n = dl = (2k)l = 2(kl)$.
So n is even.
□

Proof by Contradiction

Proof by contradiction is also called *reductio ad absurdum* (reduction to an absurd thing). The idea is to assume the opposite of what one is trying to prove and then show that this leads to something that is clearly nonsensical: a contradiction.

Proof by contradiction is closely related to proof by contraposition, but it is a far more powerful technique. Contraposition can only be used for propositions of the form $(\forall x)(P(x) \implies Q(x))$ (in which case, we prove $(\forall x)(\neg Q(x) \implies \neg P(x)$.) Contradiction, on the other hand, can be used to prove a proposition of any form. Note that any proof by contraposition of $(\forall x)(P(x) \implies Q(x))$ can be turned into a proof by contradiction (but not vice-versa.) A proof by contraposition shows that $\neg Q(a) \implies \neg P(x)$. For a proof by contradiction, you would assume that the statement is false, i.e. that it's negation is true: There exists a such that $P(a)$ and $\neg Q(a)$. Because $\neg Q(x) \implies \neg P(x)$, you must have $\neg P(a)$. Thus, you have $P(a)$ and $\neg P(a)$, a contradiction. Note that we got to assume more to prove the statement by contradiction

Our first example of a proof by contradiction dates back more than 2000 years – to Euclid. (Note that it is not of the form $P \implies Q$ so contraposition is not an option.)

Theorem 2.4: *There are infinitely many prime numbers.*

Proving this directly would be difficult. How do we construct infinitely many prime numbers? But, as we will see, bad things happen when we assume that this statement is fale: that there are only finitely many primes. Before we prove the theorem, we will state a lemma that we'll need without proof. We will prove it next week when we learn induction:

Lemma 2.1: *Every natural number greater than one is either prime or it has a prime divisor.*

Proof:

Suppose toward a contradiction that there are only finitely many primes. Then, we can enumerate them: $p_1, p_2, p_3, \cdots, p_k$.

Consider the number $q = p_1 p_2 p_3 \dots p_k + 1$, the product of all the primes plus one. Note that q cannot be prime because it is strictly larger than all the primes. Thus, by the lemma, it has a prime divisor, p. Because $p_1, p_2, p_3, \dots, p_k$ are all the primes, p must be equal to one of them, so p is a divisor of their product.

So we have that p divides $p_1 p_2 p_3 \dots p_k$, and p divides q, but that means p divides their difference, which is 1. This is nonsense, because p must be greater than one.

□

In class, many of you wanted to immediately conclude that q is prime, and get the contradiction that way, but this is an unwarranted conclusion. It's certainly not the case that a product of primes plus one must always be prime (think of $7 \cdot 2 + 1$). When writing a proof, try to get in the habit of carefully thinking through each step, ensuring that it's logically justified. The most important part of learning mathematics is learning a habit of thinking clearly and precisely. This habit will serve you well in life, regardless of what you decide to do.

RATIONAL NUMBER

IRRATIONAL

Okay, back to the lecture. Let's look at another classic proof by contraction. A **rational number** is a number that can be expressed as the ratio of two integers. For example, $2/3$, $3/5$, and $9/16$ are all rational numbers. In fact, any number with a finite or recurring decimal representation is a rational. (Perhaps you'll prove this on one of your homeworks.) Numbers that cannot be expressed as fractions are called **irrational**.

Theorem 2.5: *$\sqrt{2}$ is irrational.*

In our proof of this theorem, we will make use of a classic result, also due to Euclid: the Fundamental Theorem of Arithmetic:

Theorem 2.6: *Every natural number greater than one can be expressed uniquely (except for rearrangements) as a product of one or more primes.*

Proof: Suppose toward a contradiction that the $\sqrt{2}$ is rational.
By the definition of rational numbers, there are integers a and b, $b \neq 0$, such that $\sqrt{2} = \frac{a}{b}$.
Squaring both sides of the equation, we get $2 = a^2/b^2$.
Multiplying both sides by b^2, we have $a^2 = 2b^2$. We'll call this number c.
Note that a prime factorization of $c = a^2$ can be obtained by writing out the prime factorization of a and doubling the number of times each term appears, i.e., if $a = 2^{p_1}3^{p_2}5^{p_3}\dots$ then $a^2 = 2^{2p_1}3^{2p_2}5^{2p_3}\dots$. Thus, the number of 2s in the prime factorization of a^2 must be even (or zero.)
Similarly, b^2, too, must have an even number of 2s in its prime factorization.
But that means $2b^2 = c$ must have an odd number of 2s in its factorization.
Thus, we've provided two different prime factorizations of c, one with an even number of 2s and one with an odd number of 2s.
This contradicts uniqueness of prime factorizations.
Hence, our assumption that $\sqrt{2}$ is rational must have been in error, and it must be the case that $\sqrt{2}$ is irrational.
□

Proof by Cases

Sometimes we don't know which of a set of possible cases is true, but we know that at least one of the cases is true. If we can prove our result in each of the cases, then we have a proof. The English phrase "damned if you do and damned if you don't" sums up this proof method. Here's a nice example:

Theorem 2.7: *For some irrational numbers x and y, x^y is rational.*

Proof: Since the theorem is existentially quantified, we need only prove the existence of at least one example. Consider the case $x = \sqrt{2}$ and $y = \sqrt{2}$. It must be true that

(a) $\sqrt{2}^{\sqrt{2}}$ is rational

or (b) $\sqrt{2}^{\sqrt{2}}$ is irrational.

In case (a), we have shown irrational numbers x and y such that x^y is rational.

In case (b), consider the values $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have

$$\begin{aligned} x^y &= (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \\ &= \sqrt{2}^{\sqrt{2}\sqrt{2}} \text{ by the axiom } (x^y)^z = x^{yz} \\ &= \sqrt{2}^2 = 2 \end{aligned}$$

Hence we have shown irrational numbers x and y such that x^y is rational.
Since one of cases (a) and (b) must be true, it follows that for some irrational numbers x and y, x^y is rational. $\square$

NONCONSTRUCTIVE

Notice that even after the proof, we still don't know which of the two cases is true, so we can't actually exhibit any irrational numbers satisfying the theorem. This is an example of a **nonconstructive** proof, one in which an existential theorem is proved without constructing an example.

Non-proof

Failure to note the justification for each step can lead easily to non-proofs. Consider the following example.

Theorem 2.8: *(not!)* $1 = -1$

Proof: $1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \sqrt{-1}^2 = -1$ $\square$

Since we have concluded a falshood, at least one of these steps is false. Indeed, it is simply untrue that $\sqrt{xy} = \sqrt{x}\sqrt{y}$. If you think carefully through each step of your proofs, you can avoid such missteps.

Other classic errors:

- Dividing both sides of an equation by a variable. For example:

  $$ax = bx \text{ hence } a = b$$

  The "axiom" to which this step implicitly appeals is false, because if $x = 0$, the claim $a = b$ does not follow. Some extra work may be needed to prove $x \neq 0$.

- Dividing both sides of an inequality by a variable. This is even worse! For example:

  $$ax < bx \text{ hence } a < b$$

  Here the claim $a < b$ is false if $x < 0$, and unproven if $x = 0$.

Again, get in the habit of thinking carefully before you write down the next sentence of your proof. If you cannot explain clearly why the step is justified, you are making a leap and you need to go back and think some more.