CSCI 2824 - CU Boulder, 2019 Summer

Lecture 7: Proof by cases, contradiction, and contrapositive

12 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications and Andrew Altomare's notes.

1 Converting base systems

When we talk about bases, I will denote the number y in base x as y_x.

To convert a_b to base p, we do the following after initially letting $x = a_b$:

- First, take x mod the new base p.
- Write that result.
- Now integer divide x by the new base p.
- That's our new new x. Repeat until x is 0.

When done, your answer is the reverse order of the results you've written down.

Exercise
What is 13_{10} in base 6?

Well let's calculate:

x	operation	digit
13	$13 \mod 6$	1
2	$2 \mod 6$	2
0	$0 \mod 6$	0

So, the answer is 21_6.

Exercise
What is $D1CE_{16}$ in base 10?

Another way: $D1CE_{16}$ can be expanded:

$$(D \times 16^3) + (1 \times 16^2) + (C \times 16^1) + (6 \times 16^0)$$

Since, A is 10, B is 11, C is 12, and D is 13 we can rewrite this:

$$(13 \times 16^3) + (1 \times 16^2) + (12 \times 16^1) + (6 \times 16^0)$$

Now, we just have a base 10 expansion which works out to 53710.

2 Review

We talked about rational numbers, divisibility, and induction. Let's go over the problems from the end of yesterday.

3 More Induction

Remember induction? We can prove cool things. Try the following:

Exercise
A *tromino* is three attached squares of any form. Since it's only three squares, you get either a straight segment or an L-shaped section. For any integer $n \geq 1$, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely coered with L-shaped trominoes.

The main idea is that $2^{k+1} = 2 \times 2^k$. So when we split a $2^{k+1} \times 2^{k+1}$ board in half vertically and horizontally, we get 4 quadrants that are $2^k \times 2^k$ checkerboards. Thus, we prove by induction.

Let S_n be the statement: *If any square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be completely covered by L-shaped trominoes*.

Consider the base case S_1. A $2^21 \times 2^1$ checkboard is four squares. If one square is removed, the remaining squares form an L which can be covered by a single L-shaped tromino.

Now suppose that for every integer $k \geq 1$, if S_k is true then S_{k+1} is also true.

Let k be any integer such that $k \geq 1$ and suppose S_k as the inductive hypothesis. Then, we must show S_{k+1}. Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Divide it into four equal quadrants, each consisting of a $2^k \times 2^k$ checkboard. In one quadrant, one square will be removed. The inductive hypothesis guarantees we can cover this quadrant with L-shaped trominoes.

For the remaining quadrants, no squares are missing and they meet at the center of the checkerboard. An L-shaped tromino can then cover the three remaining center squares meaning one square is blocked from each quadrant. By the inductive hypothesis, the remaining squares in each of the tree quadrants can be covered by L-shaped trominoes.

Thus, we have established the inductive step and the theorem is proven.

You might think, "who cares." It's an arbitrary problem. But, what if you're a shipping company and your semi-truck has humps in the storage area where the wheels rise up. That's just a more complicated version of this problem if you're trying to pack crates of a certain size and shape in the truck. You want to cover every bit to get the most money out of your shipment, so you want to solve a problem similar to this.

Exercise
Prove cool things about Ulam-Warburton Automatons.

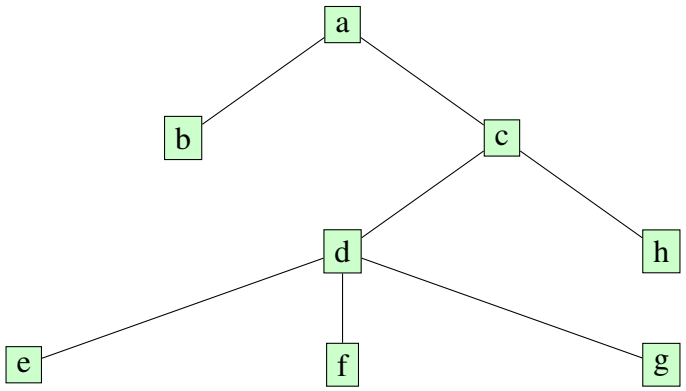
This is project 3!

4 Structural Induction

Enter my favorite thing, trees!

Definition: *Tree*
A **tree** is a non-empty collection of nodes and edges in which there exists only one path connecting two nodes.

We use trees for lots of things: sorting, data storage, regression, classification, you name it! They're beautifully elegant because of their recursive nature and ease of analysis in many settings.



We have lots of conventions about trees. Each node has children, nodes that descend from them, as well as parents, nodes that directly precede them. We use family terminology like sibling, grandparent, ancestor, and descendent to talk about node relations. a is called the root of the tree since it has no parent. But notice that if we start at c and ignore a and b we get a whole other subtree. Thus, trees are recursive, i.e. a's children are trees themselves!

We call something a full binary tree if each node has zero or two children, never just one.

Definition: *Height of a full binary tree*
The height $h(T)$ of a full binary tree T can be defined recursively:

- **Basis step**: The height of a full binary tree T containing of only a root r is $h(T) = 0$.
- **Recursive step**: If T_1 and T_2 are full binary trees, then the height of the binary tree T formed by a node having T_1 as its left child and T_2 as its right child is $h(T) = 1 + \max(h(T_1), h(T_2))$.

Exercise
Let $n(T)$ be the number of nodes in a full binary tree T. Prove that if T is a full binary tree, then $n(T) \leq 2^{h(T)+1} - 1$.

We prove this with structural induction.

First, the base case. For the full binary tree T of height 0, it consists of just one node, the root node. Thus, $n(T) = 1$ which holds since $1 \leq 2^{h(T)+1} - 1 = 1$.

Now we assume by the inductive hypothesis that $n(T_1) \leq 2^{h(T_1)+1} - 1$ and $n(T_2) \leq 2^{h(T_2)+1} - 1$ whenever T_1 and T_2 are full binary trees that are children for a binary tree T. By the recursive formulae for $n(T)$ we have $n(T) = 1 + n(T_1) + n(T_2)$ and $h(T) = 1 + \max(h(T_1), h(T_2))$. Then,

$$
\begin{aligned}
n(T) &= 1 + n(T_1) + n(T_2) && \text{by the recursive formula for } n(T) \\
&\leq 1 + \left(2^{h(T_1)+1} - 1\right) + \left(2^{h(T_2)+1} - 1\right) && \text{inductive hypothesis} \\
&\leq 2 \max\left(2^{h(T_1)+1}, 2^{h(T_2)+1}\right) - 1 && \text{sum is at most double largest} \\
&= 2 \times 2^{\max(h(T_1),h(T_2))+1} - 1 && \max\left(2^x, 2^y\right) = 2^{\max(x,y)} \\
&= 2 \times 2^{h(T)} - 1 && \text{by def} \\
&= 2^{h(T)+1} - 1
\end{aligned}
$$

This completes the recursive step so the proof is done.

5 Proof by Cases

Another very natural direct way of proving something is to consider general cases to think about. We kind of saw this with the proof that "any integer $n > 1$ is divisible by a prime number" since we considered each number to be prime or not.

You know that if 3 is odd then 3+1=4 is even and so forth. This is called alternating parity.

Exercise
Prove: Any two consecutive integers have opposite parity.

Suppose that two consecutive integers are given m and $m + 1$. By the parity property, m is either even or odd.

Case 1: m **is even**. In this case $m = 2k$ for some integer k so $m + 1 = 2k + 1$ which is odd by definition. They have opposite parity.

Case 2: m **is odd**. In this case $m = 2k + 1$ for some integer k and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer and $m + 1$ is even. They have opposite parity.

It follows that regardless of which case, for a particular m and $m + 1$ then m and $m + 1$ have opposite parity.

In general, we call this the Method of Proof by Division into Cases.

Definition: *Method of Proof by Division into Cases*
To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C prove all the following:

If A_1, then C
If A_2, then C
...
If A_n, then C.

This process shows that C is true regardless of which $A_1, A_2, \ldots A_n$ happens to be the case.

Exercise
Prove: The square of any odd integer has the form $8m + 1$ for some integer m.

Suppose n is an odd integer. By the quotient-remainder theorem, n can be written in one of the forms: $4q$ or $4q+1$ or $4q+2$ or $4q+3$ for some integer q. In fact, since n is odd and $4q$ and $4q+2$ are even, n must have one of two forms: $4q + 1$ and $4q + 3$.

Case 1, $n = 4q + 1$. Since $n = 4q + 1$

$$\begin{aligned} n^2 &= (4q+1)^2 \\ &= (4q+1)(4q+1) \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 \end{aligned}$$

Let $m = 2q^2+q$. Then, m is an integer since 2 and q are integers and sums and products of integers are integers. Thus substitution yields $n^2 = 8m + 1$.

Case 2, $n = 4q + 3$

$$\begin{aligned} n^2 &= (4q+3)^2 \\ &= (4q+3)(4q+3) \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8+1) \\ &= 8(2q^2 + 3q + 1) + 1 \end{aligned}$$

Let $m = 2q^2+3q+1$. Then, m is an integer since $1, 2, 3$, and q are integers and sums and products of integers are integers. Thus, by substitution $n^2 = 8m + 1$.

Cases 1 and 2 show that for any odd integer, $n^2 = 8m + 1$ for some integer m.

6 Proof by Contradiction

There are indirect forms of proof too. Suppose you were accused of robbing a bank. You might prove that you didn't by saying, "Suppose I did commit the crime. Then at the time of the crime, I

would have had to be at the scene of the crime. In fact, at the time of the crime I was in a meeting with 20 people far from the crime scene, as they will testify. This contradicts the assumption that I committed the crime since it is impossible to be in two places at one time. Hence that assumption is false." Assuming your claims can be verified, any reasonable jury will accept this alibi. This is proof by contradiction since you supposed that the statement was not true and showed the result was absurd.

Definition: *Method of proof by contradiction*

1. Suppose the statement to be proved is false.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved must actually be true.

We can use this idea to prove that there is no biggest integer.

Exercise
Prove: There is no greatest integer.

Suppose that N is the greatest integer. Then, $N \geq n$ for every integer n. Let $M = N + 1$. Now M is an integer because it is a sum of integers. Also, $M > N$. Thus, M is an integer greater than N, a contradiction. Therefore, there is no greatest integer.

Exercise
Prove: There is not integer that is both even and odd.

Suppose p is an integer that is both even and odd. Then, $\exists a \in \mathbb{Z}$ such that $p = 2a$ and $\exists b \in \mathbb{Z}$ such that $p = 2b+1$. Further, $2a = 2b+1$. Then, $a-b = 1/2$. But no two integers must have a distance of at least 1 apart, thus a contradiction. Therefore, there is no integer that is both even and odd.

Exercise
Prove: The sum of any rational number and any irrational number is irrational.

Let $p \in \mathbb{Q}$ and $q \in \mathbb{R} \setminus \mathbb{Q}$. Suppose that their sum $r = p + q$ is rational. Since rationals are closed under subtraction then $q = r - p$ is also rational, a contradiction. Therefore, the sum of any rational and irrational number is irrational.

7 Proof by Contrapositive

A more complicated form of proof relies on the idea of contraposition. Remember that a conditional statement is logically equivalent to its contrapositive. We exploit that here:

Definition: *Method of proof by contraposition*

1. Express the statement to be proved in the from $\forall x \in D, P(x) \to Q(x)$.
2. Rewrite this in the contrapositive form $\forall x \in D, \not{Q}(x) \to \not{P}(x)$
3. Prove the contrapositive by direct proof, i.e. suppose $x \in D$ such that $Q(x)$ is false and show that $P(x)$ is false.

It may seem weird and silly to prove things like this. But, there are times that it is easier.

Theorem 7.1. *For all integers n, if n^2 is even then n is even.*

Proof. **[By contraposition]**. Suppose n is any odd integer. By definition of odd $n = 2k + 1$ for some integer k. Then,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

. But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2q + 1$ where $q = 2k^2 + 2k$ and thus by definition is odd. □

We could have also proved this with contradiction.

Proof. **[By contradiction]** Suppose not, i.e. suppose there is an integer n such that n^2 is even but n is not event. By the quotient remainder theorem with $d = 2$, any integer is even or odd. Hence, since n is not even it is odd and thus $n = 2k + 1$ for some integer k. By algebra:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So, $n^2 = 2q + 1$ where $q = 2k^2 + 2k$ and thus by definition, it is odd. Therefore, n^2 is both odd and event. This contradicts our previous theorem that no integer can be both even and odd. □

8 What's to come

8.1 Sequences

Definition: *Sequence*
A sequence is a function whose domain is either all the inters between two given integers or all the integers greater than or equal to an integer.

We can then define sequences like $1, 2, 4, 9, 16, \ldots$ rigorously. We will also learn to define sequences recursively. For example, the Fibonacci sequence:

$$F(n) = \begin{cases} 1 & n = 1 \text{ or } n = 2 \\ F(n-1) + F(n-2) & \text{otherwise} \end{cases} \tag{1}$$

This creates a famous sequence $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. We'll learn how to find and prove close-form expressions for the k-th term in a sequence. For example, the k-th term of the Fibonacci sequence is: $\frac{\varphi^k - \psi^k}{\sqrt{5}}$ where $\varphi = \frac{1+\sqrt{5}}{2}$ and ψ is the golden ratio: $1 - \varphi$.

8.2 Sets

We are starting to use some more rigorous ideas of sets. Naively, we can think of a set as just a collection of distinct mathematical objects. However, that leads to Russell's paradox:

$$\text{Let } R = \{x | x \notin x\}, \text{ then } R \in R \leftrightarrow R \notin R$$

.

Informally, consider the set of everything that is not a flamingo. Well this set itself is not a flamingo so it's inside itself. That's kind of weird, right? We'll call sets that don't contain themself "normal" and weird sets that contain themself "abnormal." Think about the set of all normal sets. Is it normal or abnormal? If it's normal, then it should be a member of itself. But then, it's by definition abnormal. That's a contradiction. But, if it's abnormal, then it's by definition a member of itself but it contained only normal sets to begin with... oh no! We have a paradox!

To resolve this, a long line of fundamental math research has been conducted to define things from first principles rigorously. There are many attempts. We will talk about one of the most popular called Zermelo-Fraenkel set theory. It is based on a set of axioms:

- **Axiom of extensionality**. Two sets are equal and are the same set if they have the same elements. $\forall x \forall y \left[\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y\right]$
- **Axiom of regularity or Axiom of foundation**. Every non-empty set x contains a member y such that x and y are disjoint sets. $\forall x \left(x \neq \emptyset \rightarrow \exists y \in x (y \cap x = \emptyset)\right)$
- **Axiom schema of specification**. For any formula ϕ in ZFC with all free variables $x, z, w_1, \ldots, w_n$. Then, $\forall z \forall w_1 \forall w_2 \ldots \forall w_n \exists y \forall x \left[x \in y \leftrightarrow (x \in z \wedge \phi)\right]$. It lets you construct sets. This helps avoid Russell's paradox. This also tells us that empy sets exist. Let ϕ be a property no set has such as $(u \in u) \wedge \neg(u \in u)$. Then, $\emptyset = \{u \in w | \phi(u)\}$
- **Axiom of pairing**. For sets x and y there's a set that contains x and y as elements. $\forall x \forall y \exists z (x \in z \wedge y \in z)$.
- **Axiom of union**: The union of any sets exists. For sets $\mathcal{F}$ there is a set A that contains every element that is a member of some member of $\mathcal{F}$: $\forall \mathcal{F} \exists A \forall Y \forall x \left[(x \in Y \wedge Y \in \mathcal{F}) \rightarrow x \in A\right]$.
- **Axiom schema of replacement**: The image of a set under any function is also inside a set. We can let ϕ be a formula with free variables $x, y, Aw_1, \ldots, W_n$. Then,

$$\forall A \forall w_1 \forall w_2 \ldots \forall w_n \left[\forall x (x \in A \rightarrow \exists! y \phi) \rightarrow \exists B \forall x (x \in A \rightarrow \exists y (y \in B \wedge \phi))\right]$$

- **Axiom of infinity**. There exists a set having infinitely many members. More formally, let $S(w)$ abbreviate $w \cup \{w\}$ where w is some set. Then, there exists a set X such that the empty set $\emptyset$ is a member of X, and, whenever a set y is a member of X, then $S(y)$ is also a member of X.
$$\exists X \left[\emptyset \in X \wedge \forall y(y \in X \rightarrow S(y) \in X)\right]$$
- **Axiom of power set**. For a set X, there is a set Y that contains every subset of X. $\forall x \exists y \forall z \left[z \subset x \rightarrow z \in y\right]$.
- **Well-ordering theorem**: For any set X there is a binary relation R which well-orders X. Thus, R is a linear order on X such that every nonempty subset of X has a member which is minimal under R. $\forall X \exists R(R \text{ well orders } X)$. A well ordering is a binary relation R on some set X that holds the following:
  - It's antisymmetric. If $a \leq b$ and $b \leq a$ then $a = b$.
  - It's transitive. If $a \leq b$ and $b \leq c$ then $a \leq c$.
  - It's connex. $a \leq b$ or $b \leq a$.
  - Every non-empty subset of S has a least element in the ordering.

Once we establish this, we can talk about interesction ($\cap$) and union of sets ($\cup$) as well as a host of other fun things that arise.

8.3 Functions

Given that we know what sets are, we can map from one set to another using functions. We will talk about injections, surjections, and bijections. We can then talk about the limiting behavior of functions using the ideas of asymptotic notation, that big-oh stuff you've heard aobut. This lets us analyze programs and a host of other fun behaviors.

8.4 The world of usage

From there, we can talk more recursion. We can use combinatorics to help us count things and analyze. We introduce discrete probability. We can talk about structures we encounter in problems through graphs. We will git some applications along the way of AI, graphics/fractals, cryptography, and networks.