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?

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

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.

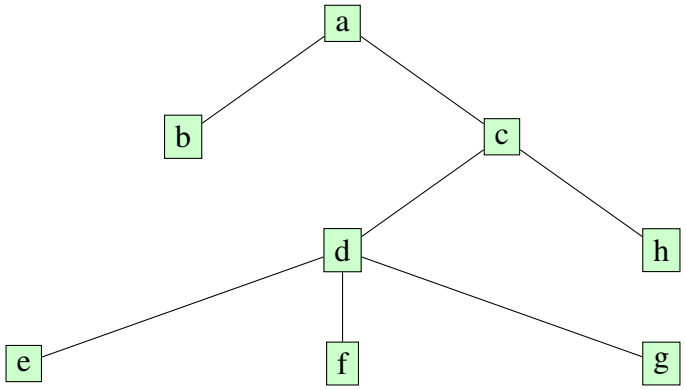
You might think, "who cares." It's an arbitrary problem. But, what if you're a shipping company and your semi-truck has humps in the storage area where the wheels rise up. That's just a more complicated version of this problem if you're trying to pack crates of a certain size and shape in the truck.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

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 $n(T) \leq 2^{h(T)+1} - 1$.

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.

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 $\ldots$ or A_n, then C prove all the following:

If A_1, then C
If A_2, then C
$\ldots$
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.

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.

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

Exercise
Prove: The sum of any rational number and any 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. □