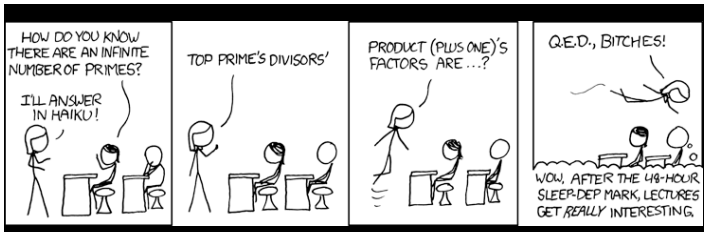


Randall Munroe http://xkcd.com/622/

CS151 Fall 2014
Lecture 8 – 9/18
Proofs

Prof. Tanya Berger-Wolf
http://www.cs.uic.edu/CS151

Adapted from Lap Chi Lau – The Chinese University of Hong Kong
and David Liben-Nowell – Carleton College

Proof by Contradiction

$$\frac{\overline{P} \rightarrow \mathrm{F}}{P}$$

To prove P, you prove that not P would lead to ridiculous result, and so P must be true.

You are working as a clerk.
If you have won lottery, then you would not work as a clerk.
$\therefore$ You have not won lottery.

Infinitude of the Primes

Theorem. There are infinitely many prime numbers.

Proof (by contradiction):

Let $p_1, p_2, \ldots, p_N$ be all the primes.

Consider $p_1 p_2 \ldots p_N + 1$.

Claim: if p divides a, then p does not divide a+1.

Proof (by contradiction):

a = cp for some integer c
a+1 = dp for some integer d
=> 1 = (d-c)p, contradiction because p>=2.

So none of $p_1, p_2, \ldots, p_N$ can divide $p_1 p_2 \ldots p_N + 1$, a contradiction.

Divisibility by a Prime

Theorem. Any integer n > 1 is divisible by a prime number.

- Let n be an integer.
- If n is a prime number, then we are done.
- Otherwise, n = ab, both are smaller than n.
- If a or b is a prime number, then we are done.
- Otherwise, a = cd, both are smaller than a.
- If c or d is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we have found a prime factor of n.

Idea of induction.

Proof by Cases

$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\therefore r$$

e.g. want to prove a nonzero number always has a positive square.

x is positive or x is negative

if x is positive, then $x^2 > 0$.

if x is negative, then $x^2 > 0$.

$\therefore x^2 > 0$.

The Square of an Odd Integer

$$\forall \text{ odd } n, \exists m, n^2 = 8m + 1?$$

Idea 0: find counterexample.

$3^2 = 9 = 8+1$, $5^2 = 25 = 3x8+1$ ..... $131^2 = 17161 = 2145x8 + 1$, ...

Idea 1: prove that $n^2 - 1$ is divisible by 8.

$n^2 - 1 = (n-1)(n+1) = ??...$

Idea 2: consider $(2k+1)^2$

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

If k is even, then both k^2 and k are even, and so we are done.

If k is odd, then both k^2 and k are odd, and so k^2+k even, also done.

http://www.themathlab.com/geometry/funnyproofs.htm

Odd Powers Are Odd

Fact: If m is odd and n is odd, then nm is odd.

Proposition: for an odd number m, m^k is odd for all non-negative integer k.

$$\forall k \in N \ odd(m^k)$$

Let P(i) be the proposition that m^i is odd.

$$\forall k \in N \ P(k)$$

Idea of induction.

- P(1) is true by definition.
- P(2) is true by P(1) and the fact.
- P(3) is true by P(2) and the fact.
- P(i+1) is true by P(i) and the fact.
- So P(i) is true for all i.

Divisibility by a Prime

Theorem. Any integer n > 1 is divisible by a prime number.

- Let n be an integer.
- If n is a prime number, then we are done.
- Otherwise, n = ab, both are smaller than n.
- If a or b is a prime number, then we are done.
- Otherwise, a = cd, both are smaller than a.
- If c or d is a prime number, then we are done.
- Otherwise, repeat this argument, since the numbers are getting smaller and smaller, this will eventually stop and we have found a prime factor of n.

Idea of induction.

Idea of Induction

Objective: Prove $\forall n \geq 0 \;\; P(n)$

This is to prove

$$P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(n) \ldots$$

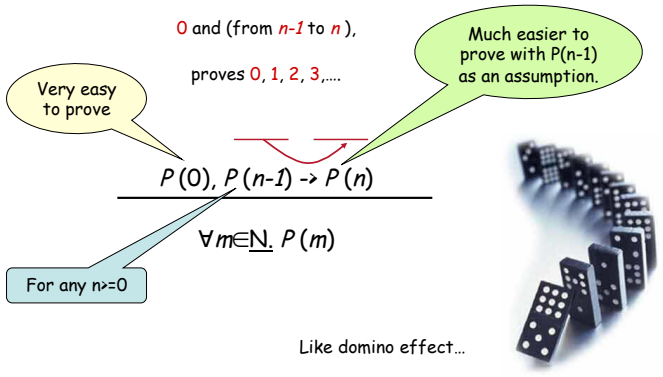
The idea of induction is to first prove P(0) unconditionally,

then use P(0) to prove P(1)

then use P(1) to prove P(2)

and repeat this to infinity…

The Induction Rule



Proof by Induction

Let's prove:

$$\forall r \neq 1. \; 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$$

Statements in green form a template for inductive proofs.

Proof: (by induction on *n*)

Base case P(0), is:

$$\forall r \neq 1. \;\; 1 + r + r^2 + \ldots + r^0 = \frac{r^{0+1} - 1}{r - 1}$$

$$1 = \frac{r - 1}{r - 1}$$

Proof by Induction

Let's prove:

$$\forall r \neq 1.\ 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$$

Statements in green form a template for inductive proofs.

Proof: (by induction on *n*)

The induction hypothesis, *P(n-1)*, is:

$$\forall r \neq 1.\ 1 + r + r^2 + \ldots + r^{n-1} = \frac{r^n - 1}{r - 1}$$

Proof by Induction

Induction Step: Assume *P(n-1)* for some $n \geq 0$ and prove *P(n)*:

$$\forall r \neq 1 \quad 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Have *P (n-1)* by assumption:

So let *r* be any number ~= 1, then from *P (n-1)* we have

$$1 + r + r^2 + \cdots + r^{n-1} = \frac{r^n - 1}{r - 1}$$

How do we proceed?

Proof by Induction

adding r^n to both sides,

$$1 + r + r^2 + \cdots + r^{n-1} + r^n = \frac{r^n - 1}{r - 1} + r^n$$

$$= \frac{r^n - 1 + r^n(r-1)}{r - 1}$$

$$= \frac{\cancel{r^n} - 1 + r^{n+1} - \cancel{r^n}}{r - 1}$$

$$= \frac{r^{n+1} - 1}{r - 1}$$

But since *r* ~= 1 was arbitrary, we conclude (by Universal Generalization), that

$$\forall n \geq 0 \quad \forall r \neq 1 \quad 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

which is *P (n)*. This completes the induction proof.