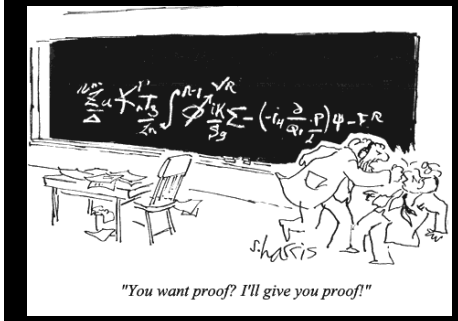

"You want proof? I'll give you proof!"

CS151 Fall 2014
Lecture 7 – 9/16
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

Universal Generalization

valid rule $\dfrac{A \rightarrow R(c)}{A \rightarrow \forall x.R(x)}$

providing c is independent of A

e.g. given any number c, 2c is an even number

=> for all x, 2x is an even number.

Vacuous quantification

$$\forall x \in \emptyset \quad P(x)$$

All even prime numbers greater than 5 have 3 as the last digit

Vacuously true

Not Valid

$\forall z\,[Q(z) \vee P(z)] \rightarrow [\forall x.Q(x) \vee \forall y.P(y)]$

Proof: Give ***counterexample***, where
$\forall z\,[Q(z) \vee P(z)]$ is true,
but $\forall x.Q(x) \vee \forall y.P(y)$ is false.

Find a domain, and a predicate.

In this example, let domain be integers,
$Q(z)$ be true if z is an even number, i.e. Q(z)=even(z)
$P(z)$ be true if z is an odd number, i.e. P(z)=odd(z)

Then $\forall z\,[Q(z) \vee P(z)]$ is true, because every number is either even or odd.
But $\forall x.Q(x)$ is not true, since not every number is an even number.
Similarly $\forall y.P(y)$ is not true, and so $\forall x.Q(x) \vee \forall y.P(y)$ is not true.

Mathematical Proof

We prove mathematical statement by using logic.

$$\frac{P \to Q,\ Q \to R,\ R \to P}{P \wedge Q \wedge R}$$

not valid

To prove something is true, we need to assume some **axioms**!

This is invented by Euclid in 300 BC,
who begins with 5 assumptions about geometry,
and derive many theorems as logical consequences.

http://en.wikipedia.org/wiki/Euclidean_geometry

(see http://en.wikipedia.org/wiki/Zermelo–Fraenkel_set_theory for the ZFC axioms for set theory)

Basic Definitions

An integer n is an even number
if there exists an integer k such that n = 2k.

An integer n is an odd number
if there exists an integer k such that n = 2k+1.

Proving an Implication

Goal: If P, then Q. (P implies Q)

Method 1: Write assume P, then show that Q logically follows.

Claim: If $0 \le x \le 2$, then $-x^3 + 4x + 1 > 0$

Reasoning: When x=0, it is true.
When x grows, 4x grows faster than x^3 in that range.

Proof: $-x^3 + 4x + 1 = x(2-x)(2+x) + 1$
When $0 \le x \le 2$, $x(2-x)(2+x) \ge 0$ □

Direct Proofs

The sum of two even numbers is even.

Proof x = 2m, y = 2n
x+y = 2m+2n
= 2(m+n)

The product of two odd numbers is odd.

Proof x = 2m+1, y = 2n+1
xy = (2m+1)(2n+1)
= 4mn + 2m + 2n + 1
= 2(2mn+m+n) + 1.

Divisibility

a "divides" b (a|b):
b = ak for some integer k

5|15 because 15 = 3⊠5
n|0 because 0 = n⊠0
1|n because n = 1⊠n
n|n because n = n⊠1

A number p > 1 with no positive integer divisors other than 1 and itself is called a **prime**. Every other number greater than 1 is called **composite**.

2, 3, 5, 7, 11, and 13 are prime,
4, 6, 8, and 9 are composite.

Simple Divisibility Facts

1. If a | b, then a | bc for all c.
2. If a | b and b | c, then a | c.
3. If a | b and a | c, then a | sb + tc for all s and t.
4. For all c ≠ 0, a | b if and only if ca | cb.

Proof of (1)
a | b
⇒ b = ak
⇒ bc = ack
⇒ bc = a(ck)
⇒ a|bc

a "divides" b (a|b):
b = ak for some integer k

Simple Divisibility Facts

1. If a | b, then a | bc for all c.
2. If a | b and b | c, then a | c.
3. If a | b and a | c, then a | sb + tc for all s and t.
4. For all c ≠ 0, a | b if and only if ca | cb.

Proof of (2)
a | b => $b = ak_1$
b | c => $c = bk_2$
=> $c = ak_1k_2$
=> a|c

a "divides" b (a|b):
b = ak for some integer k

Simple Divisibility Facts

1. If a | b, then a | bc for all c.
2. If a | b and b | c, then a | c.
3. If a | b and a | c, then a | sb + tc for all s and t.
4. For all c ≠ 0, a | b if and only if ca | cb.

Proof of (3)
a | b => $b = ak_1$
a | c => $c = ak_2$
sb + tc
= $sak_1 + tak_2$
= $a(sk_1 + tk_2)$
=> a|(sb+tc)

a "divides" b (a|b):
b = ak for some integer k

Proving an "if and only if"

Goal: Prove that two statements P and Q are "**logically equivalent**", that is, one holds if and only if the other holds.

Example:
An integer is even if and only if the its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Method 1': Prove P implies Q **and** not P implies not Q.

Method 2: Construct a chain of if and only if statement.

Proof the Contrapositive

An integer is even if and only if the its square is even.

Method 1: Prove P implies Q **and** Q implies P.

Statement: If m is even, then m^2 is even

Proof: $m = 2k$

$m^2 = 4k^2$

Statement: If m^2 is even, then m is even

Proof: $m^2 = 2k$

$m = \sqrt{(2k)}$

??

Proof the Contrapositive

An integer is even if and only if the its square is even.

Method 1': Prove P implies Q **and** not P implies not Q.

Statement: If m^2 is even, then m is even

Contrapositive: If m is odd, then m^2 is odd.

Proof (the contrapositive):

Since m is an odd number, $m = 2k+1$ for some integer k.

So $m^2 = (2k+1)^2$

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

So m^2 is an odd number.