HKN Review Sessions

CS 70 Midterm 1, Fall 2012

Govind Ramnarayan, Chris Turney and Lisa Yan

List of Topics

- Proofs
- Quantifiers
- Induction
- Stable Marriage
- Extended-gcd
- Modular Arithmetic
- Fermat's Little Theorem
- RSA
- Any others...?

Proofs: Direct Proofs

Direct Proof of $P \Longrightarrow Q$

Assume P

$\vdots$

Therefore Q

This is often easy when you have an easy-to-expand expression as P. For example:

Prove that, for m, n are odd integers, then mn is also an odd integer.

Proof:

We can write $m = 2k + 1, n = 2l + 1$ for some $k, l \in \mathbb{Z}$

$$\begin{aligned} & (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1 \\ &= 2a + 1 \text{ for some } a \in \mathbb{Z} \end{aligned}$$

So mn is, by definition, an odd number.

Proofs: Contraposition

Proof by Contraposition of $P \implies Q$

Assume $\neg Q$

$\vdots$

Therefore $\neg P$

So $\neg Q \implies \neg P \equiv P \implies Q$

Proofs by contrapositive are often easier to think about than direct proofs. When you are stuck on proving an implication, it is often really useful to think about proving the contrapositive.

Let's prove that if

$$x^2 \text{ is even, then } x \text{ is even, for } x \in \mathbb{Z}$$

Suppose x is not even. Let $x = 2k + 1$ for $k \in \mathbb{Z}$

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

We proved that x^2 is an odd number, so we have completed our proof by contrapositive.

Proofs: Contradiction

Proof by Contradiction of P

Assume $\neg P$

$\vdots$

R

$\vdots$

$\neg R$

Contradiction

Therefore P

Proofs by contradiction are also extremely useful.

Example:

Prove: There is no greatest integer.

Proof: Assume there is a greatest integer N. But we know that N+1 is also an integer (since integers are closed under addition, by definition), and N+1 > N so N is not the greatest integer. Contradiction.

Therefore there is no greatest integer.

Quantifiers

(Sinclair Spring 09 # 1)

In the following, P(n) and Q(n) denote propositions concerning the natural number n, and R(m, n) denotes a proposition concerning natural numbers m and n. Each part asserts a logical equivalence A ≡ B. For each part, say whether the equivalence is valid or invalid.

1. $$\forall n(\neg Q(n) \Rightarrow P(n)) \equiv \neg[\exists n(\neg P(n) \wedge \neg Q(n))]$$

2. $$\forall m \forall n\ [R(m,n) \Rightarrow \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \equiv$$
$$\forall m \forall n\ [\neg R(m,n) \vee \exists l\ (\neg R(m+l,n) \wedge \neg R(n,m+l))]$$

Quantifiers: Solution

1. $\forall n(\neg Q(n) \Rightarrow P(n)) \equiv \neg[\exists n(\neg P(n) \wedge \neg Q(n))]$

Valid: We can see this by rewriting the implication and applying De Morgan's laws.

$$\begin{aligned} \forall n(\neg Q(n) \Rightarrow P(n)) &\equiv \forall n(Q(n) \vee P(n)) \\ &\equiv \forall n \neg(\neg P(n) \wedge \neg Q(n) \\ &\equiv \neg[\exists n(\neg P(n) \wedge \neg Q(n))] \end{aligned}$$

2. $\forall m \forall n\ [R(m,n) \Rightarrow \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \equiv$
$\forall m \forall n\ [\neg R(m,n) \vee \exists l\ (\neg R(m+l,n) \wedge \neg R(n,m+l))]$

Valid: We can see this by rewriting the implication and applying De Morgan's laws.

$$\begin{aligned} & \forall m \forall n\ [R(m,n) \Rightarrow \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \\ \equiv\ & \forall m \forall n\ [\neg R(m,n) \vee \neg(\forall l[R(m+l,n) \vee R(n,m+l)])] \\ \equiv\ & \forall m \forall n\ [\neg R(m,n) \vee \exists l\ \neg(R(m+l,n) \vee R(n,m+l))] \\ \equiv\ & \forall m \forall n\ [\neg R(m,n) \vee \exists l\ (\neg R(m+l,n) \wedge \neg R(n,m+l))] \end{aligned}$$

Induction

Prove the following using induction:

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Induction: Solution

Base case:

$$\text{Let } n = 1. \text{ Then } n^3 = 1^3 = \left(\frac{1(1+1)}{2}\right)^2.$$

Inductive hypothesis:

$$\text{Assume } \sum_{k=1}^{m} k^3 = \left(\frac{m(m+1)}{2}\right)^2 \text{ for some } m.$$

Inductive Step

$$\sum_{k=1}^{m+1} k^3 = \sum_{k=1}^{m} k^3 + (m+1)^3$$

$$= \left(\frac{m(m+1)}{2}\right)^2 + (m+1)^2(m+1) \text{ (By inductive step)}$$

$$= \left(\frac{m^2}{4} + (m+1)\right)(m+1)^2 = \frac{m^2+4m+4}{4}(m+1)^2$$

$$= \frac{(m+2)^2}{2^2}(m+1)^2 = \left(\frac{(m+2)(m+1)}{2}\right)^2$$

Therefore by induction,

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Induction #2

(Sahai Fall 08 #2)
Prove the following using induction:

$$\forall n \geq 1, \sum_{k=1}^{n} k \cdot k! = (n+1)! - 1.$$

Induction #2: Solution

Solution: For $n = 1$,

$$\begin{aligned}\sum_{k=1}^{1} k \cdot k! &= 1 \times 1! \\ &= 1 \\ &= (1+1)! - 1.\end{aligned}$$

Induction hypothesis:
Solution: Assume that for some $n = l \geq 1$, $\sum_{k=1}^{l} k \cdot k! = (l+1)! - 1$.

Induction step:
Solution: For $n = l + 1$,

$$\begin{aligned}\sum_{k=1}^{l+1} k \cdot k! &= (l+1) \times (l+1)! + \sum_{k=1}^{l} k \cdot k! \text{ by spliting the sum} \\ &= (l+1) \times (l+1)! + [(l+1)! - 1] \text{ by induction hypothesis} \\ &= (l+1+1) \times (l+1)! - 1 \text{ by collecting the first two terms} \\ &= (l+2) \times (l+1)! - 1 \\ &= (l+2)! - 1.\end{aligned}$$

Therefore, by induction, $\forall n \geq 1$, $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Stable Marriage (Tse & Rao Fall 2009 #4)

A - Perform the traditional stable marriage algorithm to find the male-optimal pairing for this situation:

Men (1-4)					Women (A-D)				
1:	A	B	D	C	A:	2	3	4	1
2:	C	B	A	D	B:	1	4	2	3
3:	D	C	B	A	C:	1	4	2	3
4:	D	C	A	B	D:	1	3	2	4

B - For a stable marriage problem with n men and n women, what is the minimum number of different stable pairings that must exist for any set of preferences?

C - It is possible for man M and woman W to be paired in a stable pairing even if each is at the bottom of the other's preference list. How many couples can have this property in a stable pairing?

Stable Marriage Solution:

A - (A,1), (B,2), (C,4), (D,3).

B - 1. Suppose man 1 and woman A are each at the top of each other's preference lists, man 2 and woman B are at the top of each other's lists, and so on. The only stable pairing is (1,A), (2,B), etc.

C - Just 1. If there were 2 such pairs, (1, A) and (2, B), then (1, B) and (2, A) would be rogue couples - everyone involved will happily ditch their partner for anyone else.

Extended-gcd

Evaluate:

extended-gcd(37,10)

Show all recursive steps and return values. Use this information to provide a solution, if any, to

$$10x = 1 \bmod 37$$

Extended-gcd: Solution

e-gcd(37,10)
e-gcd(10,7)
e-gcd(7,3)
e-gcd(3,1)
e-gcd(1,0)

Extended-gcd: Solution

e-gcd(1,0)	returns (1,1,0)
e-gcd(3,1)	returns (1,0,1)
e-gcd(7,3)	returns (1,1,-2)
e-gcd(10,7)	returns (1,-2,3)
e-gcd(37,10)	returns (1,3,-11)

So a solution for $10x = 1 \bmod 37$ is $x=-11$, or equivalently, $x = 26 \bmod 37$.

Modular System of Equations

(Sinclair Spring 09 # 1)

Solve for x and y:

$$3x + 5y = 2 \bmod 19$$

$$7x + 3y = 8 \bmod 19$$

Modular System of Equations

Solve for x and y:

3x + 5y = 2 mod 19

7x + 3y = 8 mod 19

$$3x + 5y \equiv 2 \mod 19 \rightarrow$$
$$7x + 3y \equiv 8 \mod 19 \rightarrow$$
$$26x \equiv 34 \mod 19 \rightarrow$$
$$7^{-1} \equiv -8 \mod 19 \rightarrow$$
$$x \equiv -6 \mod 19 \rightarrow$$
$$-18 + 5y \equiv 2 \mod 19$$
$$5y \equiv 20 \mod 19 \rightarrow$$
$$y \equiv 5^{-1} \mod 19 \rightarrow$$

$$-9x - 15y \equiv -6 \mod 19$$
$$35x + 15y \equiv 40 \mod 19$$
$$7x \equiv 15 \mod 19$$
$$x \equiv -8 \cdot 15 \mod 19$$
$$\mathbf{x \equiv 13 \mod 19}$$

$$5y \equiv 1 \mod 19$$
$$\mathbf{y \equiv 4 \mod 19}$$

Fermat's Little Theorem

$a^{p-1} = 1 \bmod p$

for prime p

and $a \in \{1, \ldots, p-1\}$

Fermat's Little Theorem Practice Question

Calculate $2^{125} \bmod 127$. Hint: 127 is prime.

Fermat's Little Theorem Practice Question Solution

Calculate 2^{125} mod 127. Hint: 127 is prime.

$= 2^{-1} * 2^{126}$ mod 127

$= 2^{-1} * 1$ mod 127 (using FLT)

$= 2^{-1}$ mod 127

= 64 mod 127 (you can do this using ext-gcd):

ext-gcd(127, 2) (1,1,-63)

ext-gcd(2,1) (1,0,1)

ext-gcd(1,0) --> (1,1,0)

$2^{-1} = -63 = 64$ (mod 127)

RSA Problem - Sahai Fall 2008 #5

We have chosen p = 5 and q = 7.

1- How many choices for e are there?

2 - If e = 17, find d.

3 - Encode the message x = 2 (using e = 17 again).

4 - What is 100^{100} mod 35?

RSA Problem Solutions

1: e must be coprime with (p-1)*(q-1), which = 4 * 6 = 24. 24 = 2^3 * 3, so the options for e are values that are not divisible by 2 or 3 (note that if e = 1 messages will not be encoded, so that value of e cannot be chosen): 5, 7, 11, 13, 17, 19, and 23, of which there are 7.

2: d = e^{-1} mod (p-1)*(q-1). Running ext-gcd(24, 17) gives d = 17.

3: Encoding x involves computing x^e mod N. N = pq = 35, so:

x^e mod N =

= 2^{17} mod 35

= 2 * $(2^8)^2$ mod 35

= 2 * $(256)^2$ mod 35

= 2 * $(11)^2$ mod 35

= 2 * 121 mod 35

= 2 * 16 mod 35

= 32

RSA Problem Solutions Continued

4: $100^{100} \bmod 35$

$= 100^{96} * 100^4 \bmod 35$

$= (100^{24})^4 * 100^4 \bmod 35$

$= 1^4 * 100^4 \bmod 35$ using the extension to FLT

$= 1 * 30^4 \bmod 35$

$= (30^2)^2 \bmod 35$

$= (900)^2 \bmod 35$

$= (25)^2 \bmod 35$

$= 625 \bmod 35$

$= 30$