Math 55 - Spring 04 - Lecture notes # 2 - Jan 22 (Thursday)

Today's goals: variables and quantifiers ("for all integers x, x+1 > x")
Proof techniques

First goal: dealing with variables in propositions
So far, our propositions cannot include variables, like 'x'.
So, we can't say "x<1 -> x+1<2"; we'd like to.
We introduce them by having propositional functions p(x). It
becomes true or false once we assign the variable x a value
ASK&WAIT EG: p(x) = 'x > 3', p(2) = ?? , p(4) = ??
ASK&WAIT EG: q(x,y) = ' x = y-1', q(1,2) = ?
ASK&WAIT EG: p(x) = ' x is prime ', p(111201) = ?
EG: p(x) = ' x is student at Berkeley '
ASK&WAIT EG: If (x>0) then y=x+1; is this a propositional function?
Note: x must "type check" for these to make sense, i.e.
DEF: The Universe of Discourse is the set of values x is
allowed to take in p(x)
ASK&WAIT What are Universes of Discourse for above examples?

DEF: "for all x p(x)" is a proposition which is true if and only if
p(x) is true for all x in the universe of discourse;
also called "for each x, p(x)",
"universal quantification of p(x)"
some times write "for all x in U. of D., p(x)"

ASK&WAIT EG: for all integers n, 2*n is even
ASK&WAIT EG: for all real numbers z, z^2 > 0
ASK&WAIT EG: for all real numbers z, 0<z<1 -> z^2 < .5
ASK&WAIT EG: for all integers z, 0<z<1 -> z^2 < .5
ASK&WAIT EG: for all Berkeley L&S CS students S, S must take
discrete math
ASK&WAIT EG: For all positive integers n, x, y, z, n>2 -> x^n != y^n + z^n
(Fermat's Last Theorem)

DEF: "there exists an x such that p(x)" is a proposition which is
true if and only if p(x) is true for at least one x in the
universe of discourse, "existential quantification"
ASK&WAIT EG: there exists an integer n, 2*n is even
ASK&WAIT EG: there exists a Berkeley Student S, S works hard
ASK&WAIT EG: there exists a real number z, z^2 < 0
ASK&WAIT EG: there exists a real number z, z^2 <= 0

```
ASK&WAIT   EG: there exists a real number z, z^2 <= 1

           EG: (Lewis Carroll, author of 'Alice in Wonderland')
               Universe of Discourse = 'creatures'
               "All bears are fierce"
               "Some bears do not drink Peet's coffee"
               "Some fierce creatures do not drink Peet's coffee"
                Let B(x) = "x is a bear"
                Let F(x) = "x is fierce"
                Let P(x) = "x drinks Peet's coffee"
               Express above using forall, thereexists:
ASK&WAIT       "All bears are fierce"
ASK&WAIT       "Some bears do not drink Peet's coffee"
ASK&WAIT       why not "there exists x (B(x) -> not P(x))" ?
ASK&WAIT       "Some fierce creatures do not drink Peet's coffee"

ASK&WAIT   EG: forall real x, thereexists real y, x=y+1
ASK&WAIT   EG: thereexists real y, for all real x, x=y+1

           EG: From calculus: lim(x -> a) f(x) = b really means
               forall eps>0 therexists delta>0 forall x
                      0<abs(x-a)<delta -> abs(f(x)-b)<eps

ASK&WAIT   EG: restate not( forall x p(x) ) using thereexists:
ASK&WAIT   EG: restate not( thereexists x p(x) ) using forall:

           DEF: A variable is bound, if it is either fixed, or
                in a "for all" or "there exists". Only if all variables
                in a propositional function are bound is it a proposition.
                An unbound variable called free
           EG: P(x,y,z) = x=y and y<z
               there exists y for all z P(0,y,z)
           CS: analogy: to evaluate a function, need to know all the
               arguments

    Proof techniques (aka rule of inferences)

    [ p and (p -> q)] -> q
    Names: modus ponens, law of detachment, "common sense"
    EX: p = "3|n", q = "9|n^2", then "p -> q" is clearly true.
          So for example, if n=6, so that p is true, you can conclude 9|6^2
```

```
Other common sense stuff:
[(p -> q) and (q -> r)] -> (p -> r)
EX: p = '3|n', q = '9|n^2', r = '18|2*n^2', so p->q and q->r
    Thus p->r, i.e. 3|n -> 18|2*n^2

(p and q) -> p
EX: p = "3|n" , q = "2|n", (p and q) = '6|n', so 6|n -> 3|n

p -> (p or q)
EX: p = '3|n', q = '2|n', so 3|n -> (3|n or 2|n)

[ not q and (p -> q) ] -> not p
Name: modus tollens
Works because (p -> q) <-> (not q -> not p)
EX: Show "if 3n+2 is odd then n is odd",
    use p="n is even", q="3n+2 is even"; then p -> q is clearly true,
    so 3n+2 odd and (p -> q) is the same as not q and (p -> q) whence
    not p i.e. n is odd

[ not p -> F) ] -> p
Name: proof by contradiction
EX: cuberoot(5) is irrational, i.e. cannot be written as a/b where
    a and b are nonzero integers without common divisor
    let p = "cuberoot(5) is irrational"
    so not p = "cuberoot(5) is rational"
             -> cuberoot(5) = a/b, where a and b have no common divisor
             -> 5 = a^3/b^3, or 5 b^3 = a^3 (use b != 0)
             -> 5 | a^3 -> 5 | a -> a=5*c -> 5 b^3 = 125 c^3
             -> b^3 = 25 c^3 -> 5 | b^3 -> 5 | b
             -> 5|a and 5|b
             -> a and b have a common factor and do not have a
                common factor
             -> false
    so p is true

 case analysis
 EX: show that min(x,y) + max(x,y) = x+y
     Three possible cases: x<y, x=y and x > y
        Case 1: min(x,y) = x, max(x,y)=y, so min+max=x+y
        Case 2: min(x,y) = x = y, max(x,y) = y = x, so min+max=x+y=2*x
        Case 3: min(x,y) = y, max(x,y)= x , so min+max=y+x=x+y
```

```
      EX: Are this statement and its proof correct?
          Let a(0), a(1), and a(2) be three different points in the plane,
          and let T be the triangle they form. Let
             theta(1) be the clockwise angle between the line segments
                  (a(0),a(1)) and (a(1),a(2))
             theta(2) be the clockwise angle between the line segments
                  (a(1),a(2)) and (a(2),a(0))
             theta(0) be the clockwise angle between the line segments
                  (a(2),a(0)) and (a(0),a(1))
          Then theta(1)+theta(2)+theta(3) = 180 degrees.
          Proof: Draw the figure
                       a(1)-----a(0)
                         \       /
                          \     /
                           \   /
                            a(2)
                 and use the fact that the sums of the angles in a triangle
                 is 180 degrees.

ASK&WAIT: Are this statement and its proof correct?

      EX: Are this statement and its proof correct?
          The number of primes is infinite:
          Proof: Suppose that the number of primes is finite; we will
                 get a contradiction.  Denote these primes by
                 p1,p2, ... , pn. Let N = p1*p2*...*pn+1. N is not
                 divisible by any of p1, p2, ..., pn, because it has
                 a remainder of 1 when you divide by any of them.
                 Therefore N is another prime.

ASK&WAIT: Are this statement and its proof correct?

      Def: "p if and only if q" means "p <-> q is a tautology"
           To prove this you have to show that p and q are both true at
           at the same time, and both false at the same time

      EX: Are this statement and its proof correct?
          a*b is rational if and only a and b are rational
          Proof: Suppose a=p/q and b=r/s are rational, i.e. quotients
                 of integers. Then a*b = (p*r)/(q*s) is rational.

ASK&WAIT: Are this statement and its proof correct?
```

```
Proving "NOT EXIST x such that P(x)" is same as
    "FORALL x NOT P(x)"
EX: Are following statement and proof correct?
    There is no polynomial p(n) with integer coefficients
    such that p(n) is prime for all integers n >= 0.
    In other words, there is no simple (polynomial) formula for
    generating primes.
    Proof: instead show "FORALL polynomials p(n),
           there is an n >= 0 such that p(n) is not prime":
          Write p(n) = p_(d)*n^d + p_(d-1)*n^(d-1) + ... + p_(1)*n + p_(0)
                     = r(n) + p_(0)
           If p_(0) = 0, then p(0)=0 is not prime
           If p_(0) = 1 or -1, then p(0)=1 or -1, so not prime
           If p_(0) is composite, so is p(0) = p_(0)
           If p_(0)=q is prime, then q|r(q), so q|p(q)=r(q)+q

ASK&WAIT: Are this statement and its proof correct?
```