ECS 20 — Lecture 6 — Fall 2013 —16 Oct 2013

Phil Rogaway

Today: o Number theory: an important axiom (the "principle of induction")
o Set theory -- Sets, relations, and functions

Recall ... We "customize" first-order logic

LOGICAL SYMBOLS

1. Logical connectives $\neg \wedge \vee \rightarrow$
2. Parenthesis (,)
3. The quantifier symbols: $\forall$, $\exists$
4. Variables $v_1, v_2, \ldots$ (name points in the universe) (infinite set)
5. Equality symbol: = (usually)

NON-LOGICAL SYMBOLS

1. predicate symbols // functions from tuples of points in the universe U to {T, F} (eg, <)
   Each has an **arity** (binary, ternary, ...)
2. function symbols // maps a tuple of points in the universe U to a point in U (eg, +)
3. constant symbols // each names a point in the universe U (like 0)

as with:

Number Theory

1. constant symbol: 0
2. predicate symbol: <
3. function symbol: S (1-ary) (successor function)
   + (2-ary)
   * (2-ary)
   E (2-ary)

Always add: = is reflexive, symmetric, transitive

Axioms of arithmeitic ("Peano arithmetic") – see list on Wikipedia or Wolfram

1. $\neg(\exists x)\,(Sx = 0)$
2. $(\forall x)(\forall y)(Sx=Sy \rightarrow x=y)$
3. $(\forall x)\,(x + 0 = x)$
4. $(\forall x)(\forall y)(x + S(y) = S(x+y))$
5. $(\forall x)\,(x * 0 = 0)$
6. $(\forall x)(\forall y)(x * S(y) = x*S(y) + x)$
7. $(\forall x)(\forall y)\,)(\forall c)\,(x < y \rightarrow x+c \leq y+c)$
8. $(\forall x)(\forall y)\,)(\forall c)\,(x < y \rightarrow x*c \leq y*c)$

9. If a **set** contains zero and the successor of every **number** is in the set, then the set contains the natural numbers. Or: for all predicates P

   $(P(0) \;\wedge\; (\forall n)(P(n) \rightarrow P(n+1)) \;\rightarrow\; \wedge\; (\forall n)(P(n))$ **Not a 1st order property**

Principle of mathematical induction

To prove a proposition $P(n)$ for all integers $n \geq n_0$:

1) Prove P(n_0) **(Basis)**
2) Prove that P(n)→ P(n+1) for all $n > n_0$ **(Inductive step)**
   (Inductive hypothesis)

The above sounds slightly more general (because I let you start at n_0), but easily seen to be equivalent. Also equivalent: "strong" form of induction:

> To prove a proposition $P(n)$ for all integers $n \geq n_0$:
> 1) Prove P(n_0) **(Basis)**
> 2) Prove that (P(1) ∧ … ∧ P(n)) → P(n+1) for all $n > n_0$ (inductive step)
> *(stronger inductive hypothesis, may make it easier to get the conclusion)*

EXAMPLE 1: Prove that the sum of the odd integers 2 .. 2n-1 is n^2

$1 + 3 + \ldots + (2n-1) = n^2$.

Basis: n=1, check

Inductive step:

$$\begin{aligned} 1 + 3 + \ldots (2n-3) &= (n-1)^2 \\ + 2n-1 &= \qquad + 2n-1 \\ &= n^2 - 2n + 1 \quad + 2n - \ 1 = 1 \\ &= n^2 \end{aligned}$$

EXAMPLE 2. Sam's Dept. Store sells enveloped in packages of 5 and 12.
Prove that, for any $n \geq 44$, the store can sell you exactly n envelopes.
[GP, p.147]

Try it: 44 = 2(12) + 4(5)
45 = 9(5)
46 = 3(12) + 2(5)
?...?

SUPPOSE: it is possible to buy n envelopes for some $n \geq 44$.
SHOW: it is possible to buy n+1 envelopes

```
    x    x xx x x  x x xx x  x x  xx   x x xxxxxxxxxxxxxxxxx
123456789012345678901234567890123456789012345678901234567890
0        1         2         3         4         5         6
```

- If purchasing **at least seven** packets of 5, **trade in seven packets of five** for **three packets of 12**:
  7(5) -> 3(12)
  35 36

- **If <7 packets of 5**, ie ≤ 6 fewer packets of 5, so **at most 30** of the envelopes are in packets of 5; so there are ≥ **44-30 = 14 envelopes** being bought in packets of 12, so ≥2 two packets of twelve. So take **two of the packets of 12** (ie 24 envelopes) and **trade them for 5 packets of 5:**
  2(12) -> 5(5)
  24 25

EXAMPLE 3: Show that you can tile any "punctured" $2^n \times 2^n$ grid of *trominos*

```
#
##     (may be rotated)
```

Illustrate and prove, dividing board in into four $2^n \times 2^n$ to prove.
Puncture the $2^{n+1} \times 2^{n+1}$ grid; tile that one of the four subgrids (by inductive assumption); puncturing three the three near-center center points (for the three $2^n \times 2^n$ pieces that lacking the puncture); recurse on those three pieces; add one more tormino.

EXAMPLE 4: Cake cutting

See http://www.cs.berkeley.edu/~daw/teaching/cs70-s08/notes/n8.pdf for a nice writeup

n people want to divide a piece of cake equally.
n=2: known case.
$n \geq 3$:

1. Persons 1 .. $n-1$ people divide the cake into $n-1$ pieces (using a recursive call to this procedure).
2. Persons 1 .. $n-1$ divide their piece into n equal shares.
3. Person n takes the largest piece among the pieces held by each person 1 .. n-1.
4. Persons 1 .. $n-1$keep their remaining $n-1$pieces for themselves

Number of cuts
$T_n = T_{n-1} + (n-1)^2$

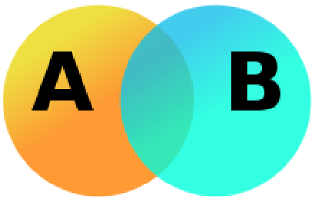
Prove exponential growth rate …
Yuck!

Set Theory

predicate symbols: 2-ary $\in$
function symbol: $\varnothing$

Introduced union, complement, symmetric difference, a first Venn diagram.

Venn Diagrams



Set Difference

$A \setminus B$ or $A - B$

Algebra of sets

$A \cup A = A$	$A \cap A = A$
$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
$A \cup B = B \cup A$	$A \cap B = B \cap A$
$A \cup (B \cap C) = (A \cup C) \cap (B \cup C)$	$A \cap (B \cup C) = A \cap B \cup A \cap C$
$A \cup \varnothing = A$	$A \cap \varnothing = \varnothing$
$A \cup U = U$	$A \cap U = A$
$(A^c)^c = A$	
$A \cup A^c = U$	$A \cap A^c = \varnothing$
$U^c = \varnothing$	$\varnothing^c = U$
$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$ <-- **DeMorgan's laws**