ECS 20 — Lecture 5 — Fall 2013 —10 Oct 2013
Phil Rogaway

Today: o First Order Logic
o Sets

Adding quantifiers – First order logic $\forall$ $\exists$

All apples are bad
$(\forall x)\ (A(x) \rightarrow B(x))$ // universe of discourse?

Some apples are bad
$(\exists x)\ (A(x) \wedge B(x))$ // universe of discourse?

"BILLY has beat up every boy at the elementary school"

$(\forall x)\ ((\text{Student}(x) \wedge \text{Boy}(x) \wedge (x \neq \text{BILLY}) \rightarrow \text{HasBeatUp}\ (\text{BILLY}, x))$

// universe of discourse?

Universe of discourse = what quantifiers range over. Always important to know the universe of discourse; it's implicit, or explicit, in any discussion of logical formulas involving quantifiers.

All lions are fierce $(\forall x)\ (L(x) \rightarrow F(x))$
Some lions do not drink coffee $(\exists\ x)\ (L(x) \wedge \neg\ C(x))$
Some fierce creatures do not drink coffee $(\exists x)\ (F(x) \wedge \neg\ C(x))$

"Nobody likes a sore loser"

universe of discourse = human beings (is this really unambiguous?)
L(x,y) - predicate - true iff person x likes y (is this really unambiguous?)
S(x) - person x is a sore loser

$(\forall x)\ (S(x) \rightarrow (\forall y)\ \ \neg\ L(y, x))$

(Apparently, a sore loser doesn't like even himself)

If anyone in the dorm has a friend who has the measles,
then EVERYONE in the dorm will have to be quarantined.

Universe of discourse - people
D(x) - person x lives in some (unspecified but understood) dorm
Q(x) - person x must be quarantined
F(x,y) - person x is friends with person y
M(x) - person x has the measles (oh no!)

$(\exists x)(D(x) \wedge (\exists y)(F(x,y) \wedge M(y))) \ \rightarrow\ \ (\forall x)(D(x) \rightarrow Q(x))$

3. T/F: universe of discourse: *Natural numbers {1,2,3, …}*

$(\forall x)(\exists y)(x<y)$	TRUE	*There are always bigger numbers*
$(\exists y)(\forall x)(x<y)$	FALSE	*There is a number that's bigger than everything*
$(\exists x)(\forall y)(x<y)$	FALSE	*There is a number smaller than everything*
$(\forall y)(\exists x)(x<y)$	FALSE	*There's always a smaller number*

Discuss the mismatch / absurdity of trying to translate English into logical formulas

People like to speak of the variables as corresponding to declarative claims in English, either true or false, and they like to speak of our WFFs as modelling English-language sentences built around if, or, and, not. If it disingenuous. We don't use language in similar ways in math and in every-day language.

- If the US captures nearly everything you do on the internet, then democracy is over.

The first sentence is not to be answered yes, unless you are trying to be cute. The second sentence is expressing a causal or foundational matter; it cannot be replaced by

- If sqrt (2) is irrational then democracy is over.
- True

and preserve its meaning.
Don't take seriously any claim of a meaningful relationship between logic and natural language communications!

Formalizing First-Order Logic

Below, **not** a formal treatment, but a formal treatment can be found in any standard logic book, eg., in Enderton.

The **vocabulary** consists of:

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)

Number Theory

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

"Any number other than 0 is the successor of some number"

$(\forall x)(\neg(x=0) \rightarrow (\exists y)(S(y)=x))$

"2+2=4"

SS 0 = SSSS 0

"There is no largest prime number" -- "There are infinitely man prime numbers"

PRIME(p) = $(\forall a)(\forall b)(a*b=p \rightarrow a=1 \vee b=1)$

$(\forall x)(\exists y)(x<y \wedge \text{PRIME}(y))$

$(\forall x)(\exists y)((x<y \wedge (\forall a)(\forall b)(a*b=p \rightarrow a=1 \vee b=1))$

Completeness Theorem (Godel's 1929): If a 1^{st} order formula is **valid** (true in every "structure") (generalizes a t.a.) then there is a finite deduction (a formal proof) of the formula.

Soundness Theorem (Godel's 1929): If a 1^{st} order formula has a finite deduction (a formal proof) then it is valid.

A formula is logically valid if and only if it is the conclusion of a formal deduction.

Incompleteness theorem: no consistent system of axioms whose theorems can be listed by an "effective procedure" is capable of proving all truths about the relations of the natural numbers.

Negating Quantified Boolean Expressions

PUSHING QUANTIFIERS

$\neg(\forall x\, \phi) \equiv (\exists x)(\neg\phi)$

$\neg(\exists x\, \phi) \equiv (\forall x)(\neg\phi)$

Negate this:

$(\exists x)(\forall y)(y>x \rightarrow \exists z\,(z^2 + 5z = y))$

$\neg(\exists x)(\forall y)(y>x \rightarrow \exists z\,(z^2 + 5z = y))$

$(\forall x)\neg(\forall y)(y>x \rightarrow \exists z\,(z^2 + 5z = y))$

$(\forall x)(\exists y)\neg(y>x \rightarrow \exists z\,(z^2 + 5z = y))$

$\neg(A \rightarrow B) \equiv \neg(\neg A \vee B) \equiv (A \wedge \neg B)$

$(\forall x)(\exists y)(y>x \wedge \neg\exists z\,(z^2 + 5z = y))$m

$(\forall x)(\exists y)(y>x \wedge \forall z \neg(z^2 + 5z = y))$

$(\forall x)(\exists y)(y>x \wedge \forall z(z^2 + 5z \neq y))$

Example: **negligible functions**

A function f: $\mathbf{N} \rightarrow \mathbf{R}$ is negligible if it vanishes faster than the inverse of any polynomial:

$(\forall c>0)(\exists N)(\forall n \geq N)\, f(n) \leq n^{-c}$ shorthand for

$(\forall c)\ (\exists N)\ (\forall n)\ (\ c>0 \wedge n \geq N \rightarrow\ f(n) \leq n^{-c})$

"eventually, you're less than n^{-c} for ANY c. Negate it:

"there is a c s.t., infinitely often, you're bigger than n^{-c}"

Even grad students and researchers get confused about this!

$\neg\,(\forall c)\ (\exists N)\ (\forall n)\ (\ c>0 \wedge n \geq N \rightarrow\ f(n) \leq n^{-c})$
= $(\exists c) \neg\,(\exists N)\ (\forall n)\ (\ c>0 \wedge n \geq N \rightarrow\ f(n) \leq n^{-c})$
= $(\exists c)\ (\forall N) \neg\,(\forall n)\ (\ c>0 \wedge n \geq N \rightarrow\ f(n) \leq n^{-c})$
= $(\exists c)\ (\forall N)\ (\exists n) \neg\,(\ c>0 \wedge n \geq N \rightarrow\ f(n) \leq n^{-c})$
= $(\exists c)\ (\forall N)\ (\exists n)\ (\ c>0 \wedge n \geq N\ \wedge\ f(n) > n^{-c})$

Infinitely often, you are bigger than n^{-c}

Set Theory

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

Note "syntactic sugar" -- write $a \in A$ instead of $\in(a,A)$.
But that doesn't change that $\in$ is a 2-ary predicate.

"For any pair of sets, x and y, there a set $x \cup y$ that contains all of the elements of x and y"

$(\forall x)(\ \forall y)(\ \exists z)\ (\forall u)\ \ (u \in z\ \leftrightarrow (u \in x) \vee (u\ \in\ y))$

Seems very spare, just \in.
What are other operators on sets, and how would we define them?

$A \subseteq B$: (another 2-ary predicate)

$a \notin A\ \ =\ \ \neg\,(a \in A)$
$A \subseteq B\ \ =\ \ (x \in A \rightarrow x \in B)$
$A \supseteq B\ \ =\ \ (x \in B \rightarrow x \in A)$
