ECS 20 — Lecture 4 — Fall 2013 —8 Oct 2013

Phil Rogaway

Today:

- Quiz 1
- More logic
    - Finish propositional calculus: Formal proofs, and some without-proof theorems
    - First-order logic (adding quantifiers) (didn't get to this)

Propositional Logic "Propositional Logic" = "Sentential Logic" = "Sentential Calculus"

Review: WFFs
truth tables
truth assignments
logical completeness
DNF
satisfiability
tautology $\models \phi$
is logically equivalent

A formula ϕ is **satisfiable** if *some* t.a. makes it true.
A set of formula Γ is **satisfiable** if *some* t.a. makes them all true.
A formula ϕ of propositional logic is **tautological** (or **valid**) if it is true for every t.a.
$\models \phi$ (It is satisfiable if it is true under *some* t.a.)

Formulas ϕ and ψ are **logically equivalent** , written $\phi \equiv \psi$, if $\phi \leftrightarrow \psi$ a tautology.

Prop: There is an algorithm (=a precisely-describable procedure, mechanism, recipe)
that, given a WFF of sentential logic, decides
- if it is a tautology.
- if it is a satisfiable.
- if it equivalent to some given, second formula. *f* |= =| *g*

Some simple tautologies Velleman, List from *How to Prove It*, p. 21, 23, 47, 49 .
You can check any of these with a truth table.

Associative: $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ //Mention the similarities to arithmetic
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$ //laws with $\vee$ corresponding to **addition**
//and $\wedge$ corresponding to **multiplication**

DeMorgan's: $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$
$\neg (P \vee Q) \equiv \neg P \wedge \neg Q$

Idempotent: P and P $\equiv$ P
$P \vee P \equiv P$

Contradiction $P \rightarrow Q \equiv \neg P \vee Q$
$P \rightarrow Q \equiv \neg (P \wedge \neg Q)$

Formal Proofs

Discuss conventional proofs vs. formal proofs.

I now discuss formal proofs, although what mathematicians – and you – will mostly be producing conventional (informal) ones.
Following from Wikipedia, *Propositional Calculus*. Following 14 rules

Axiom List W

Axioms		
Name	**Axiom Schema**	**Description**
THEN-1	$\phi \to (\chi \to \phi)$	Add hypothesis χ, implication introduction
THEN-2	$(\phi \to (\chi \to \psi)) \to ((\phi \to \chi) \to (\phi \to \psi))$	Distribute hypothesis ϕ over implication
AND-1	$\phi \land \chi \to \phi$	Eliminate conjunction
AND-2	$\phi \land \chi \to \chi$	
AND-3	$\phi \to (\chi \to (\phi \land \chi))$	Introduce conjunction
OR-1	$\phi \to \phi \lor \chi$	Introduce disjunction
OR-2	$\chi \to \phi \lor \chi$	
OR-3	$(\phi \to \psi) \to ((\chi \to \psi) \to (\phi \lor \chi \to \psi))$	Eliminate disjunction
NOT-1	$(\phi \to \chi) \to ((\phi \to \neg\chi) \to \neg\phi)$	Introduce negation
NOT-2	$\phi \to (\neg\phi \to \chi)$	Eliminate negation
NOT-3	$\phi \lor \neg\phi$	Excluded middle, classical logic
IFF-1	$(\phi \leftrightarrow \chi) \to (\phi \to \chi)$	Eliminate equivalence
IFF-2	$(\phi \leftrightarrow \chi) \to (\chi \to \phi)$	
IFF-3	$(\phi \to \chi) \to ((\chi \to \phi) \to (\phi \leftrightarrow \chi))$	Introduce equivalence

One of the reasons to have a list of axioms like the list just given is to develop a notion of “what is provable"” We will write $X \vdash Y$ if statement Y follows from X. Read: Y **is provable from** X. **Turnstyle** is the name of the symbol.

Formal proofs are quite different from **conventional proofs**, but a **thesis** in mathematics is that conventional proofs can be recast as formal ones. What are formal proof? They are syntactic objects in some formalized system. There are many choices one has in how to do the formulation,

but here is what we would typically have: that a formal proof is a sequence of formula: $\phi_1, ..., \phi_n$
where each ϕ_i is either

1. an **assumption** or
2. an **axiom** (it appear on a list like Axiom List W) or
3. it follows from a previous set of lines in the proof by one of a number of enumerated rules – indeed we can make do with one rule, modes ponens,

   i) $(A \rightarrow B)$
   ...
   j) A
   ...
   k) B *modes ponens*

if $\phi_1, ..., \phi_n$ are the assumptions used in a proof and ϕ is a statement in the proof then we write
$\phi_1, ..., \phi_n \vdash \phi$ to indicate that ϕ can be proven from $\phi_1, ..., \phi_n$

Definition: if $\{ \phi_1, ..., \phi_n \} \vdash \phi$ then $(\phi_1, ..., \phi_n) \vdash \phi$

Example:
$\vdash (PQ)(P \vee R \rightarrow S)(SQ \rightarrow T) \rightarrow T$

1. PQ assumption
2. $P \vee R \rightarrow S$ assumption
3. $SQ \rightarrow T$ assumption
4. P "conjunction elimination" ($P \wedge Q \Rightarrow P$) applied to (1)
5. Q "conjunction elimination" ($P \wedge Q \Rightarrow Q$) applied to (1)
6. $P \vee R$ "disjunction introduction" ($P \vee R \rightarrow S$) applied to (5)
7. S modus ponens ($A \rightarrow B$ A gives B) applied to (2) and (6)
8. SQ "conjunction introduction" ($S, Q \Rightarrow SQ$) applied to (7) and (5)
9. T modus ponens applied to (3) and (8)

therefore

$\{ PQ, \; P \vee R \rightarrow S, \; SQ \rightarrow T \} \vdash T$ //The given statement is provable

$\vdash \phi$ can derive (prove) ϕ (from the $\varnothing$ — no assumptions)
$\Gamma \vdash \phi$ can derive ϕ from Γ

Some theorem and terms: Completeness, Soundness, and Compactness of Predicate Calculus

SOUNDNESS: $\Gamma \vdash \phi$ ➔ $\Gamma \models \phi$

COMPLETENESS: $\Gamma \models \phi$ ➔ $\Gamma \vdash \phi$

COMPACTNESS: Let Γ be a set of WFFs.
Suppose that *every finite subset* of Γ is satisfiable.

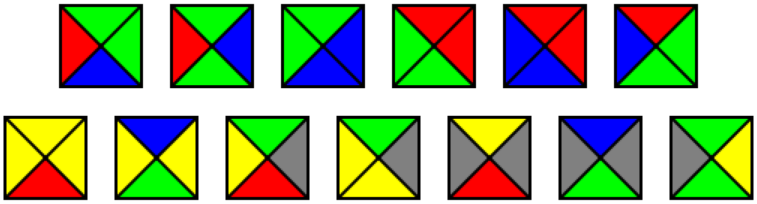
Then Γ is satisfiable.

(contrapositive:
Let Γ be a set of WFFs.
If Γ is unsatisfiable then some finite subset of Γ is too)

Don't prove -- want to use this in a computer-science example.

Application: **TILING** (Dominos)
Can you tile the with tiles of specified types
(adjacent edges of the same color)

Eg:



Make an example where the plane is and is not tileable. Indicate that, in ecs120, common to prove that the TILING decision question is **undecidable**. But not our interest here. We are interested in whether the tileability of the plane for a given set of tile types is FALSIFIABLE -- is there a proof of untileability? There will be if the following is true:

If the plane is untellable, it is already untileable on some finite subset of the plane.

Not an obvious claim -- a priori possible that plane is untileable even though every finite rectangle of it is tileable.

To prove from compactness:

Introduce a variable
$P[i,j,k]$: there is a tile of type k at position (i, j)

Write a boolean formula to capture
- One and only one tile per cell: $P[i,j,k] \rightarrow$ not $P[i,j,k']$ for all i,j and all $k \neq k'$.
- Adjoining tiles are of compatible types. $P[i,j,k] \rightarrow (\vee_{k'} P[i+1,j,k'])$, for all i, j, if a tile of type k' can be put atop a tile of type k; and so on (three more sets of rules)

Now: connect it to compactness theorem. The set Γ is all the formulas above. If it is unsatisfiable, then some finite subset of Γ_0 is unsatisfiable. Let n be the largest index used by a variable in Γ_0. Then the $[-n..n] \times [-n..n]$ subset of the plane is already untileable.

Gamma is satisfiable iff every the plane can be tiled with tiles
of the given types.

In the language you will learn in ecs120, **TILING is co-RE**