ECS 20 — Lecture 3 — Fall 2013 —3 Oct 2013

Phil Rogaway

Today:

- Review of propositional logic: Boolean values, circuits and their efficiency, design problems, satisfiable and tautological formulas.

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

Universe of two points: 0 (F) and 1 (T).
Give some basic examples.
Truth tables.
Definitions of conditional and biconditionals.

Def: A well-formed formula (WFF) of the propositional logic over a set of **variables** $\mathcal{P}$ (finite or countably infinite) (the variables may not contain any of: $\neg$ $\vee$ $\wedge$ ( ) **F** **T** // we may alternatively use 0 and 1 for **F** and **T**

- **F** and **T** are WFF
- If $P \in \mathcal{P}$ then P is a WFF
- If x and y are WFFs then so are: $(\neg x)$, $(x \vee y)$, $(x \wedge y)$,
  // stop here: let's treat $(x \rightarrow y)$, $(x \leftrightarrow y)$ as "syntactic sugar"

Nothing else is a WFF.

This is an example of a **recursive definition**.
Formulas are just **strings**: sequences of symbols from an alphabet.
A **truth assignment** t on $\boldsymbol{P}$ is a map t: $\boldsymbol{P} \rightarrow \{\mathbf{F}, \mathbf{T}\}$.
A t.a. is also called a **model**.

A t.a. gives a formula ϕ a truth value (**T** or **F**) in the natural way; formally, we extend t to a t.a. on WFFs by asserting that

$t(\mathbf{T})=\mathbf{T}$
$t(\mathbf{F})=\mathbf{F}$
$t((x \vee y)) = t(x) \vee t(y)$
$\mathrm{t}((x \wedge y)) = t(x) \wedge t(y)$
$\mathrm{t}((\neg x)) = \neg\, t(x)$

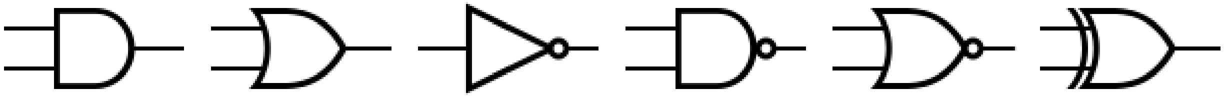
A **recursive definition.**

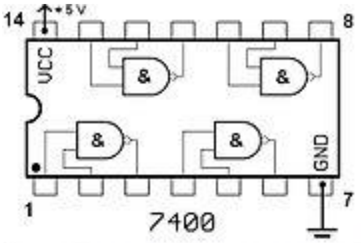
Don't confuse strings of **symbols** with their semantics (eg, the wedge in the third formula has a very different meaning in the third formula); there is a big difference between a **formal symbol** and a **logical operation.**

In common usage we use a **precedence order** and omit many "unnecessary" parenthesis, adopting a convention:

$\neg$
$\wedge$
$\vee$
$\rightarrow$
$\leftrightarrow$ (or some would put at same level as $\rightarrow$)

and right-to-left within a level (or some would say left-to-right; or some would say ill-defined).





Design something, say a **majority circuit** – returns 1 if a majority of its inputs are on. Do for 3 gates.
How would you do it for 100 gates?

Describe the class **NC.**

Describe **Disjunctive Normal Form** (DNF).
Proposition: Each WFF is equivalent to one in DNF.
Give a proof, and give an upper bound on the number of two-input gates to realize any n-input functionality.

Define: a set of operators being **logically complete**.
Show that the following sets of operators are logically complete:
$\{\wedge, \vee, \neg\}$
$\{\wedge, \neg\}$

$\{\overline{\wedge}\}$ (write NAND as a wedge with a bar over it).

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.

Proof: "Truth-table algorithm"
Example:
Contrapositive: $\models (P \to Q) \leftrightarrow (\neg Q \to \neg P)$
DeMorgan's law:
Discuss the **inefficiency** of the truth-table algorithm.
Remarkable claim**:** no efficient means are known for any of these problems.

(We only got to about here; teaching slowly today, I guess)

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 $P \to Q \equiv \neg P \vee Q$
$P \to Q \equiv \neg (P \wedge \neg Q)$

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

$A \to (B \to A)$	implication introduction
$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$	distribute hypothesis over implication
$A \wedge B \to A$, $A \wedge B \to B$	conjunction elimination
$A \to (B \to (A \wedge B))$	conjunction introduction
$A \to (A \vee B)$, $B \to (A \vee B)$	disjunction introduction
$(A \to B) \to ((C \to B) \to (A \vee C \to B))$	disjunction elimination
$(A \to B) \to ((A \to \neg B) \to \neg C)$	introduce negation
$A \to (\neg A \to B)$	eliminate negation
$A \vee \neg A$	law of excluded middle
$(A \leftrightarrow B) \to (A \to B)$, $(A \leftrightarrow B) \to (B \to A)$	eliminate equivalence
$(A \to B) \to ((B \to A) \to (A \leftrightarrow B))$	introduce equivalence

One of the reasons to have 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: $\phi_1, \ldots, \phi_n$ where each ϕ_i is either
- an **assumption** or
- an **axiom** (it appear on a list like Axiom List W) or
- 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) $(A \to B)$
  ...
j)   A
  ...

k) B *modes ponens*

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

1. PQ assumption
2. $P \vee R \to S$ assumption
3. $SQ \to T$ 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" ($P \vee R \to P$) applied to (5)
7. S modus ponens ($A \to B$ 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

$\vdash (PQ)(P \vee R \to S)(SQ \to T) \to T$ //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: $\Gamma \vdash \phi$ ➔ $\Gamma \vDash \phi$

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

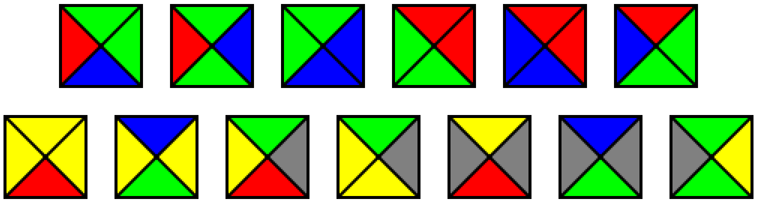
COMPACTNESS: Let Γ be a set of WFFs.
Suppose that *every finite subset* of Γ is satisfiable.
Then Γ is satisfiable.

(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] $\to$ P[i,j,k'] for all i,j and all k $\neq$ k'.
- Adjoining tiles are of compatible types. P[i,j,k] $\to$ ($\vee_{k'}$ 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*] × [-*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**

Adding quantifiers -- First order logic

"All apples are bad"
$(\forall x)\ (A(x) \to B(x))$ // 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 Caesar-Chavez elementary school"

$(\forall x)\ ((\mathrm{Student}(x) \wedge \mathrm{Boy}(x) \wedge (x \neq \mathrm{BILLY}) \to \mathrm{HasBeatenUp}(\mathrm{BILLY}, x))$

// 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	$(\forall x)\ (L(x) \to F(x))$
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 quarantines
F(x,y) - person x is friends with person y
M(x) - person x has the measles (oh no!)

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

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.

- For lunch, do you want Indian or Thai?
- If the US is storing and analyzing virtually everything you say on the phone or 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 π is irrational then democracy is over.

or

- π is irrational

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

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:

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

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

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

$(\forall x)\ (\exists y)\ (y>x \land \neg\exists\ z\ (z^2 + 5z = y))$m
$(\forall x)\ (\exists y)\ (y>x \land \quad \forall z \neg\ (z^2 + 5z = y))$
$(\forall x)\ (\exists y)\ (y>x \land \quad \forall z (z^2 + 5z \neq y))$

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

"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!

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

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

Formalizing First-Order Logic

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

In general:

vocabulary consists of:

LOGICAL SYMBOLS

1. Parenthesis (,)
2. Sentential connectives $\neg\ \land\ \lor \rightarrow$
3. Variables v_1, v_2, ... (name points in the universe)
4. Equality symbol: = (usually)

PARAMETERS:

1. $\forall$, $\exists$
2. predicate symbols // functions from the universe U to {**T**, **F**}
3. constant symbols // each names a point in the universe U
4. function symbols // maps a tuple of points in the universe U to a point in U

Important Examples

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

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)

$a \not\in A = \neg (a \in A)$
$A \subseteq B = (x \in A \rightarrow x \in B)$
$A \supseteq B = (x \in B \rightarrow x \in A)$