

18739A: Foundations of Security and Privacy

Introduction to Logic

Anupam Datta

CMU

Fall 2011

Logics in Security and Privacy

- Useful for **specifying** properties
 - Authentication, confidentiality, anonymity, coercion-resistance, notice, consent,...
- Useful for **proving** properties
 - Unbounded number of principals, sessions etc. (in contrast with finite state model checking)

What is a proof?

Intuitively, a proof is a sequence of “**statements**”, each of which follows “**logically**” from some of the previous steps.

What are “statements”? What does it mean for one to follow “logically” from another?

Propositions

A proposition is a statement that is either true or false.

snow is white

$$2+2 = 5$$

Socrates had six digits on his left hand

the summer solstice occurs on June 21st

Propositions

A proposition is a statement that is either true or false.

snow

$2+2$

is xadk keosign sziabile?

these are not propositions

Complex Statements

If snow is white then the sun rises in the west

Socrates was bald and Cicero ate a pie

$2 + 2 = 5$ if and only if $4 + 4 = 9$

Snow is not white

Complex Statements

snow is white \Rightarrow the sun rises in the west

Socrates was bald \wedge Cicero ate a pie

$2 + 2 = 5 \Leftrightarrow 4 + 4 = 9$

\neg (Snow is white)

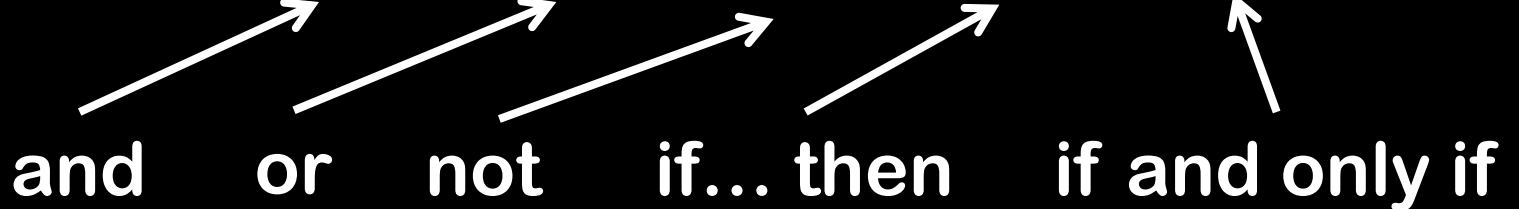
Syntax of Well-Formed Statements

Every “simple” proposition is a well-formed propositional statement

If A and B are well-formed

so are $(A \wedge B)$, $(A \vee B)$, $\neg A$, $(A \Rightarrow B)$, $(A \Leftrightarrow B)$

and or not if... then if and only if



Semantics: The “meaning” of these connectives

$(A \wedge B)$ “A and B”

true if both A and B
are true

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

$(A \vee B)$ “A or B”

true if at least one of
A and B is true

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

$\neg A$ “not A”

true if A is false

A	$\neg A$
T	F
F	T

The “meaning” of these connectives

$(A \Rightarrow B)$ “if A then B”
 “A implies B”

what are the rules for this?

The “meaning” of these connectives

$(A \Rightarrow B)$ “if A then B”
“A implies B”

what are the rules for this?

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

Equivalent to $(\neg A \vee B)$

$(A \Leftrightarrow B)$ “A if and only if B”

same as $(A \Rightarrow B)$ and $(B \Rightarrow A)$

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

**Let's abstract out the
underlying mathematical
structure...**

Well-Formed Propositional Formulas

The truth values T and F are well-formed

All variables p, q, p_1, p_2, \dots are well-formed

If A and B are well-formed

so are $(A \wedge B), (A \vee B), \neg A, (A \Rightarrow B), (A \Leftrightarrow B)$

Is $\neg(p \vee \neg q)$ well formed?

$p?$ $(p \vee \neg(\neg q))?$ $(p \Rightarrow q) \Rightarrow (\neg p \Rightarrow q)?$ $(\vee p \neg q)?$

(Well-Formed) Propositional Formulas

Each propositional formula **B** on n variables defines a function f_B from $\{T,F\}^n$ to $\{T,F\}$.

this is the “evaluation” function

“what is the value of the formula when the variables are set to T/F as given”

Defined by induction over the structure of the formula.

Recursive Evaluation for B

```
eval(formula B, input M from {T,F}n)
{
    If (B == "T") return T;
    if (B == "F") return F;
    if (B == "B1 ∧ B2")
        return eval(B1,M) ∧ eval(B2,M);
    ...
    ...
}
```

Tautologies (a.k.a. Truths)

A propositional formula **B** is a **tautology** if it is true for every setting of the variables

T F p p ∧ q

p ∨ ¬p p ∧ ¬p

(¬p ∨ q) ⇔ (p ⇒ q) (p ∨ q) ⇔ (q ∨ p)

(p ⇔ q) ⇔ ((p ⇒ q) ∧ (q ⇒ p))

Checking for Tautologies

Evaluate the propositional formula **B** on every input in $\{T, F\}^n$

How?

E.g., $B = (p \wedge (p \Rightarrow q)) \Rightarrow q$

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
T	T			
T	F			
F	T			
F	F			

$$\text{E.g., } B = (p \wedge (p \Rightarrow q)) \Rightarrow q$$

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

- A model maps propositions to T or F
- A tautology is T in all models

Truth Table for formula B

Create a table with 2^n rows

$p_1=T, p_2=T, p_3=T\dots, p_n=T$ **$B(T,T,T,\dots,T)$**

$p_1=F, p_2=T, p_3=T\dots, p_n=T$ **$B(F,T,T,\dots,T)$**

$p_1=T, p_2=F, p_3=T\dots, p_n=T$ **$B(T,F,T,\dots,T)$**

⋮

⋮

$p_1=F, p_2=F, p_3=F\dots, p_n=F$ **$B(F,F,F,\dots,F)$**

Evaluate the function for each setting

Takes at least 2^n time

OK, quick recap

propositional formulas

a formula maps each possible “world” in $\{T,F\}^n$
into either T or F

some formulas are “truths” (tautologies):
they are true in all possible 2^n worlds

can check if a formula is a tautology in $\approx 2^n$ time

What is a proof?

The truth table gives us a “proof” that a propositional formula is a tautology

What are the pros of this proof technique?

What are the cons?

Some cons

Does not give much “intuition”

Even simple things have very long proofs

$$\begin{aligned} & ((p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \dots \wedge (p_{n-1} \Rightarrow p_n)) \\ \Rightarrow & (p_1 \Rightarrow p_n) \end{aligned}$$

has truth-table of size 2^n

Does not scale to non-Boolean proofs.

We will want to prove things about
all the naturals, then we're in trouble with brute-force.

A “more natural” way to prove things...

Let us start with a simple tautology

$$(\neg A \vee A) \quad \text{we'll call this an "axiom"}$$

And use one of these rules at each step:

$$\frac{A \vee (B \vee C)}{(A \vee B) \vee C}$$

associativity

$$\frac{A \vee A}{A} \quad \text{contraction}$$

$$\frac{A}{B \vee A} \quad \text{expansion}$$

$$\frac{(A \vee B), (\neg A \vee C)}{(B \vee C)} \quad \text{cut rule}$$

we'll call these
“inference rules”

Whatever we can prove, we'll call “theorems”

Proof of commutativity rule $\frac{A \vee B}{B \vee A}$

$A \vee B$ (hypothesis) (1)

$\neg A \vee A$ (axiom) (2)

$B \vee A$ (cut rule to 1,2)

Proof of new expansion rule $\frac{A}{A \vee B}$

A (hypothesis)

B \vee A (expansion rule)

A \vee B (commutativity)

Proof of “modus ponens” $\frac{A, A \Rightarrow B}{B}$

Since the logical system does not have “ \Rightarrow ”
we define it to be $\neg A \vee B$

A (hypothesis) (1)

A \Rightarrow B (hypothesis)

$\neg A \vee B$ (def. of \Rightarrow) (2)

A \vee B (apply expansion to 1) (3)

B \vee B (cut rule to 2,3)

B (contraction)

What is a proof?

A sequence of statements,
each of which

is an axiom,

or a hypothesis,

or follows from previous statements
using an inference rule

Another recap

(well-formed) propositional formulas

some formulas are
tautologies (“truths”)

$$p \vee \neg p$$

$$(p \wedge (p \Rightarrow q)) \Rightarrow q$$

can check by
truth-table

some formulas are
“theorems”

$$p \vee \neg p$$

$$(p \wedge (p \Rightarrow q)) \Rightarrow q$$

these are formulas
for which we
can give proofs

For this logical system and Boolean formulas

Are all theorems “true” (i.e., tautologies)?

Yes.

Our logical system is “sound”.
We only prove truths.

Are all tautologies theorems?

Yes.

Our logical system is “complete”.
We can prove all the truths via inference rules.

The high-level picture

A Logical System

A “logic” consists of:

- 1) A collection S of well-formed sentences
 - 2) Some sentences in S called “axioms”
 - 3) A set of “rules of inference”
-

A “truth concept” consists of:

- 1) A collection S of well-formed sentences
- 2) Some sentences in S called “truths”

A Logical System for Propositions

Axiom:

$$(\neg A \vee A)$$

Inference Rules:

$$\frac{A \vee (B \vee C)}{(A \vee B) \vee C}$$

associativity

$$\frac{A \vee A}{A} \text{ contraction}$$

$$\frac{A}{B \vee A} \text{ expansion}$$

$$\frac{(A \vee B), (\neg A \vee C)}{(B \vee C)} \text{ cut rule}$$

This logical system is

sound

“all theorems are true”

and

complete

“all truths are theorems”

for propositional truths (tautologies)

Onwards and Upwards!

Propositional logic is fine in its place

but it does not capture too much...

E.g., consider this sequence of statements

Socrates is a human.

All humans are crazy.

Hence Socrates is crazy.

$H(s)$ $\forall x H(x) \Rightarrow C(x)$ $\therefore C(s)$

Or

$\forall x, y ((x < y) \Rightarrow (x+1 < y+1))$

First Order Logics

Have variables, and usual logical operators

But variables can range over
more general structures

Can have functions and predicates

and quantifiers

One concrete example

Let's say we want a language for protocol properties
that captures statements like:

Only A & B have secret

“ $\forall X. \text{Has}(X, \text{secret}) \supset (X = A \vee X = B)$ ”

Some session of A sent a signature on message m

“ $\exists s. \text{Sent}(A, s, \text{sig}(A, m))$ ”

Properties refer to possibly unbounded number of
principals
(contrast with model checking)

Syntax of First-Order Logic (1)

Language consists of:

- A set of function and predicate symbols, each with an associated arity
 - sig [function symbol of arity 2]
 - Has [predicate symbol of arity 2]
- A countable set X of individual variables
 - x, y, \dots
- The propositional connectives \wedge and \neg
- The universal quantifier symbol \forall
- Parentheses

Syntax of First-Order Logic (2)

Terms: Variables, function symbols of the appropriate arity applied to terms

X [a variable]

secret [a constant symbol, i.e. 0-ary function symbol]

sig(A,m) [a binary function symbol]

Syntax of First-Order Logic (3)

Well formed formulas, wffs:

- Atomic formulas are predicate symbols of the appropriate arity applied to terms

Has(X, secret), Sent(A, s, sig(A,m))

- If A, B are wffs then $(A \wedge B)$, $\neg A$ are wffs

\neg Sent(A, s, sig(A,m))

- If A is a wff and x is an individual variable, then $\forall x. A$ is a wff

$\forall X. \text{Has}(X, \text{secret}) \supset (X = A \vee X = B)$

First-Order Languages

Functions and predicates vary from application to application

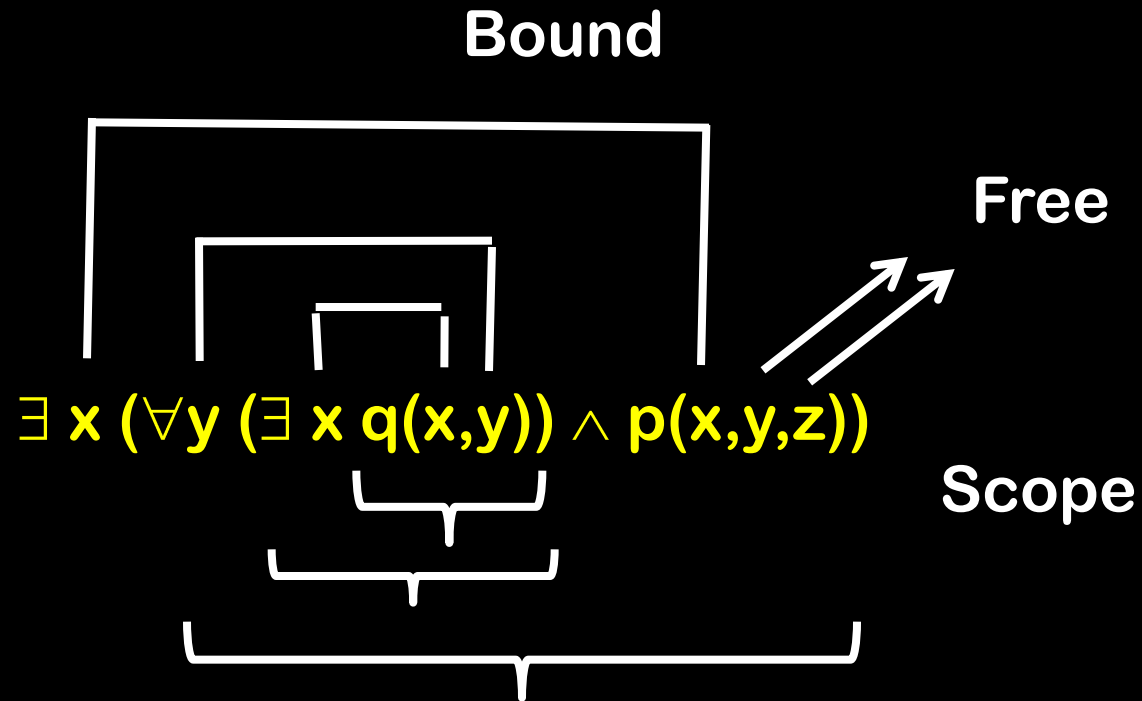
Language of protocols

- Function symbols: $\text{enc}(\dots)$, $\text{sig}(\dots)$, $\text{pair}(\dots)$
- Predicates: $\text{Has}(\dots)$, $\text{Send}(\dots)$,...

Language of number theory

- Function symbols: $+$, $*$, 0 , 1
- Predicates: $=$

Scope, Bound and Free Variables



$f(w)$ is free for z in the formula, i.e., no variables are captured if $f(w)$ is substituted for z
...but $f(x)$ is not free for z in the formula

Proof System of First-Order Logic

Axiom Schemata:

$$(1) (A \vee A) \Rightarrow A$$

$$(2) A \Rightarrow (B \vee A)$$

$$(3) (A \Rightarrow B) \Rightarrow ((C \vee A) \Rightarrow (B \vee C))$$

$$(4) \forall x. A \Rightarrow [t/x] A \quad (t \text{ is free for } x \text{ in } A)$$

$$(5) \forall x. (A \vee B) \Rightarrow A \vee \forall x. B \quad (x \text{ is not free in } A)$$

Inference Rules

$$\frac{A \quad A \Rightarrow B}{B}$$

Modus ponens (MP)

$$\frac{A}{\forall x. A}$$

Generalization (Gen)

Semantics of First-Order Logic (1)

Structure $M = \langle \text{Domain } D, \text{ Interpretation function } I \rangle$

The domain is what we interpret the language to be about
Set of components of messages = $\{A, \text{secret}, \text{sig}(A, m), \dots\}$

The interpretation function gives meaning to terms and predicates

$I(A) = A, I(\text{sig}(A, m)) = I(\text{sig})(I(A), I(m)) = \text{sig}(A, m)$

$I(\text{Has}(A, \text{secret})) = \text{Has}(A, \text{secret})$

Semantics of First-Order Logic (2)

Denotation

If c is a constant, then denotation $D_{M,s}(c)$ is $I(c)$, and if v is a variable, then $D_{M,s}(v)$ is $s(v)$ where s is an assignment from variables to domain \mathcal{D}

$$s(X) = A$$

Semantics of First-Order Logic (3)

Satisfaction

$M, s \models \varphi$ M satisfies φ under the assignment s

- If t_1 and t_2 are terms, then $M, s \models t_1 = t_2$ if and only if $D_{M,s}(t_1)$ is the same as $D_{M,s}(t_2)$
- If P is a zero-place predicate letter, then $M, s \models P$ if and only if $I(P)$ is T

Semantics of First-Order Logic (4)

- If S^n is an n -place predicate letter and t_1, \dots, t_n are terms, then $M, s \models S t_1 \dots t_n$ if and only if the n -tuple $\langle D_{M,s}(t_1), \dots, D_{M,s}(t_n) \rangle$ is in $I(S)$
- $M, s \models \neg \theta$ if and only if it is not the case that $M, s \models \theta$
- $M, s \models (\theta \wedge \psi)$ if and only if both $M, s \models \theta$ and $M, s \models \psi$.
- $M, s \models \forall x. \theta$ if and only if $M, s' \models \theta$, for every assignment s' that agrees with s except possibly at the variable x .

Soundness and Completeness

The proof system is

sound

“all theorems are true”

and

complete

“all truths are theorems”

Acknowledgement

- Slides 3-37 are from CMU 15-251:
Great Theoretical Ideas in Computer
Science with minor edits