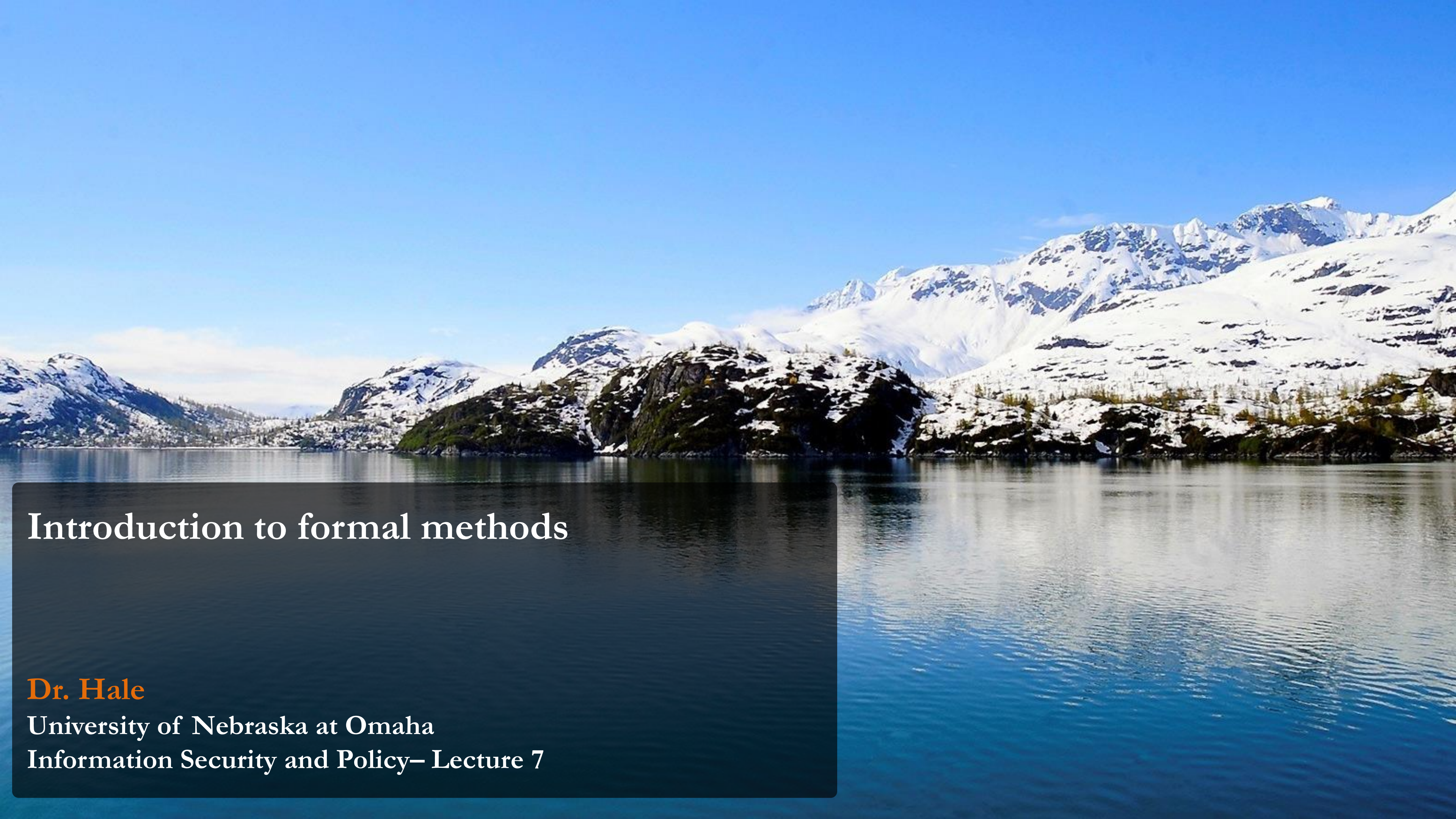


Introduction to formal methods

Dr. Hale

University of Nebraska at Omaha

Information Security and Policy– Lecture 7

Today's topics:

Introduction to formal methods

- What are formal methods?
- Why uses formal methods?

Logic and Set theory Primer

- Propositional logic
- First order Logic
- Set theory

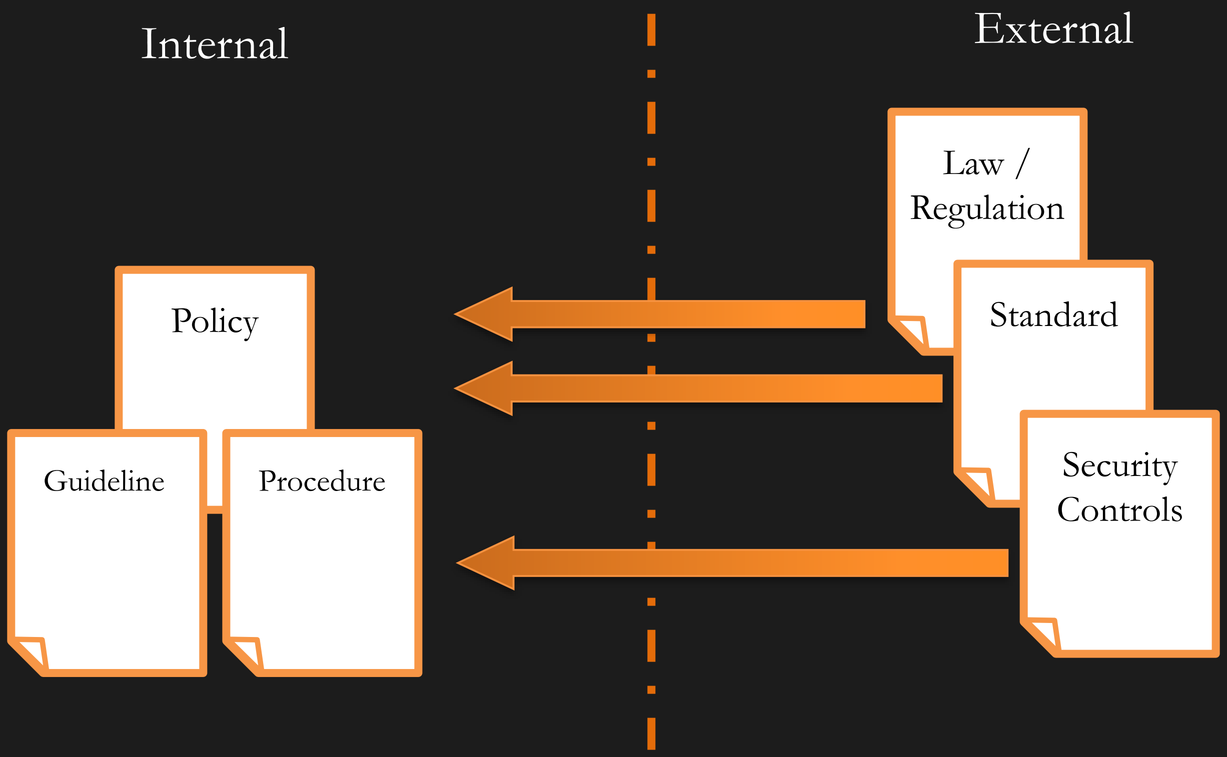
Formally Modelling Policy as Constraints

- Protection States
- Policy mechanisms as logic constraints

Up until now…

Policy has meant *high level* natural language.

Intro



Internal

External

Law / Regulation

Standard

Security Controls

Policy

Guideline

Procedure

Policy Natural Language Verbosity

I. UNO STUDENT PARKING POLICY

A. STUDENT: The term ‘student’ refers to anyone who is currently enrolled (registered) for classes held on or off the UNO Campus, either part or full-time, whether or not it leads to an academic degree.

B. Individuals who work for the University as student workers and are registered for classes are considered students.

C. Students desiring to park at the UNO Dodge, Pacific or Center locations must purchase and display a valid parking permit.

D. Student parking areas are designated by parking lot signs red in color. Specific student lots are as follows: Lots A, D, F, G, H, K, N, T, V, X, St. Margaret Mary’s Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area) at the Dodge campus; Lots 2, 5, 8, 9 (South portion) and 14 at the Pacific campus and Lot 20 at the Center campus. Permits can also be purchased for the East and West Garage, check on availability.

E. Students are restricted to student lots from 7 a.m. to 2:30 p.m., Monday through Friday. After 2:30 p.m., vehicles bearing valid parking permits may park in Student Lots and designated Faculty/Staff Lots as follows: G, H, M, S , X at the Dodge campus, and Lot 6 at the Pacific campus.

F. After 7 p.m., vehicles bearing valid parking permits may park in designated Faculty/Staff Lots R and W at the Dodge campus, and Lot 4 at the Pacific campus.

G. Students with “Night Only” parking permits may park on campus after 2:30 p.m. in the lots specified above. If you need to park on campus before 2:30 p.m., you may park in the Crossroads Mall Parking Garage and take the free shuttle bus which runs from 7 a.m. until 6 p.m., or stop by Parking Services and obtain a Temporary Parking Permit for one or two consecutive days to allow your vehicle on campus prior to 2:30 p.m. Only four free temporary permits issued per academic year.

H. Graduate Teaching Assistants may apply for G.T.A. parking privileges. G.T.A. permits are restricted to Faculty/Staff lots only.

I. Parking is also available in the Crossroads Mall Parking Garage from 7 a.m. - 7 p.m. when classes are in session during fall and spring semesters. No parking permit is required to park at the Crossroads Mall Parking Garage. (See Crossroads Mall Parking Garage for more details).

Controls and mitigations have also been natural language.

What do security controls look like?

NIST: AU-12.c: Audit Generation

The information system generates audit records for the events defined in AU-2.d with the content defined in AU-3.

AU-2.d: Audit Events

The organization determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

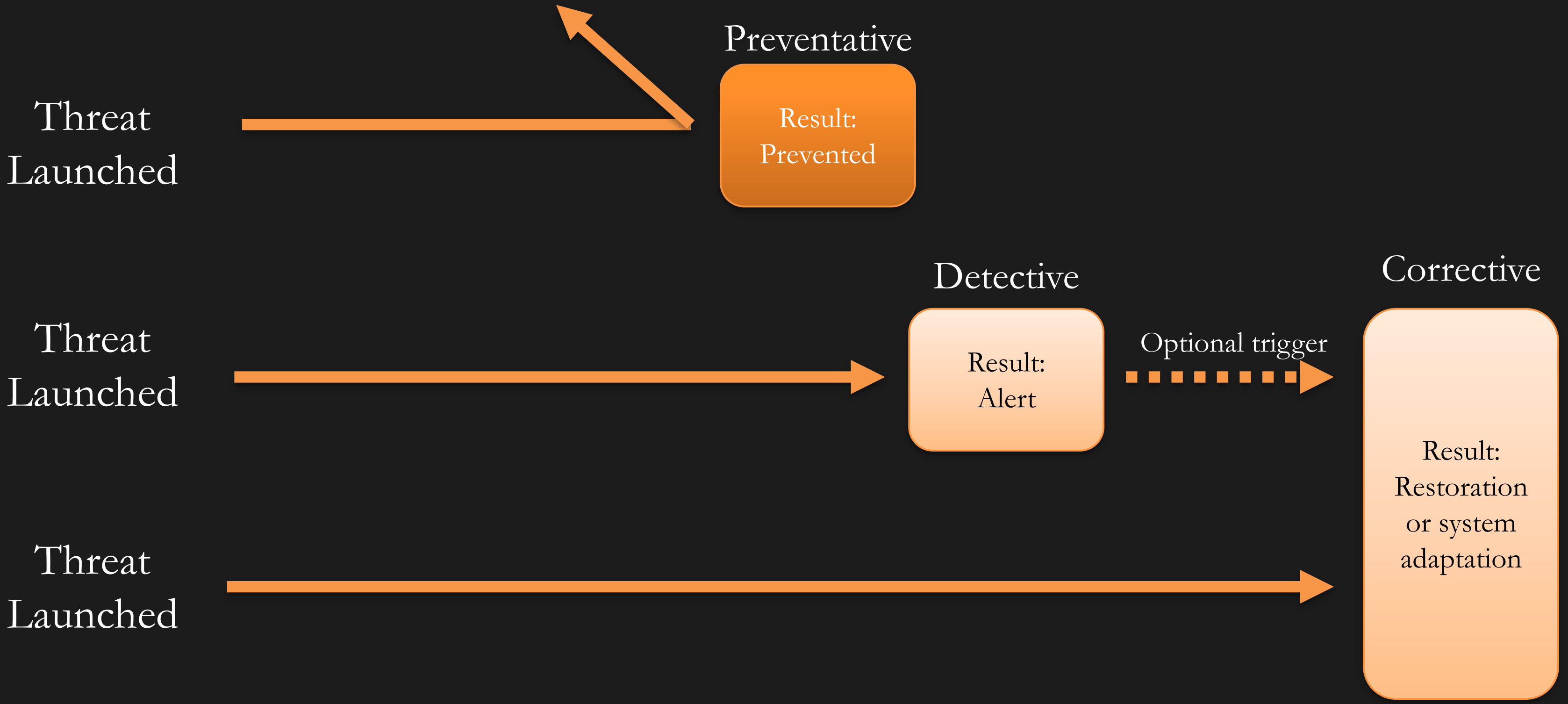
AU-3: Content of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

What do security controls look like?

CC: FAU_GEN.1.1(c) Audit Data Generation

The TSF shall be able to generate an audit record of the following auditable events [assignment: other specifically defined auditable events]


Threat Launched
Preventative
Result: Prevented
Threat Launched
Detective
Result: Alert
Optional trigger
Corrective
Result: Restoration or system adaptation
Threat Launched

These are ideas and words that may be ambiguous or open to interpretation.

How to make policy unambiguous?

Solution:

+

-

Policy Expression

- Natural Language
  - Imprecise but easy to express
  - Interpretation may vary due to ambiguity
  - e.g. All cars on campus should be in their designated lots
- Mathematically / Logically
  - Precise but difficult to express
  - Interpretation, once formalized, is stable and unambiguous
  - Secure (allowed) states
    - For all cars with a UNO sticker, car is parked in lot listed on sticker
    - For all cars without a UNO sticker, car is parked in visitor space in correct lots or contains temporary permit
  - Non-secure (disallowed) states
    - There exists a car parked in grass or on street
    - There exists a car with a UNO sticker that is in lot not listed on sticker
    - There exists a car without a sticker that is not in visitor space
  - What if I'm going to UNL with a UNO campus sticker, where do I park?
    - Policy: All cars with UNO sticker can park in corresponding UNL spots. Permits will be honored.

Before jumping into formal policy expression…

Lets cover some notational basics.

Some material from notes by
Andreas Geyer-Schulz, Chuck Dyer, and
UMBC CS671

Logic Primer

Propositional Logic

- A simple language useful for showing key ideas and definitions
- **Logical constants:** true, false
- **Propositional symbols:** P, Q, S, ... (**atomic sentences**)
- Wrapping **parentheses**: (…)
- Sentences are combined by **connectives**:

∧ ...and	[conjunction]
∨ ...or	[disjunction]
⇒...implies	[implication / conditional]
⇔..is equivalent	[biconditional]
¬ ...not	[negation]

- **Literal**: atomic sentence or negated atomic sentence

Propositional Logic

- User defines a set of propositional symbols, like P and Q.
- User defines the **semantics** of each propositional symbol:
  - P means “It is cold”
  - Q means “It is raining”
  - R means “It is snowing”
- A sentence (well formed formula) is defined as follows:
  - A symbol is a sentence
  - If S is a sentence, then $\neg S$ is a sentence
  - If S is a sentence, then (S) is a sentence
  - If S and T are sentences, then $(S \lor T)$, $(S \land T)$, $(S \rightarrow T)$, and $(S \leftrightarrow T)$ are sentences
  - Any sentence results from a finite number of applications of the above rules

Propositional Logic sentence examples

If it is cold and raining, then its snowing

$P \land Q \Rightarrow R$

If it is snowing, then it is cold

$R \Rightarrow P$

If it is snowing, then it is raining.

$R \Rightarrow Q$

it is cold and raining if and only if (iff) it is snowing

$P \land Q \Leftrightarrow R$

A BNF grammar of sentences in propositional logic

```
S := <Sentence> ;
<Sentence> := <AtomicSentence> | <ComplexSentence> ;
<AtomicSentence> := "TRUE" | "FALSE" | <Atom>
<ComplexSentence> :=  ( <Sentence> ) |
                      <Sentence> <Connective> <Sentence> |
                      "NOT" <Sentence> ;
<Connective> := "AND" | "OR" | "IMPLIES" | "EQUIVALENT" ;
<Atom> := “A” | “B” |…
```

Propositional Logic terms

- A sentence can be evaluated to determine its truth value
- A tautology is a sentence that is always true $(P \lor \neg P)$
- A contradiction is a sentence that is always false $(P \land \neg P)$
- A sentence can entail another sentence
  - written $P \models Q$.
  - Entailment means that if P is True, then so is Q.
- A truth table is a list of possible truth values for a statement

Propositional Logic truth tables

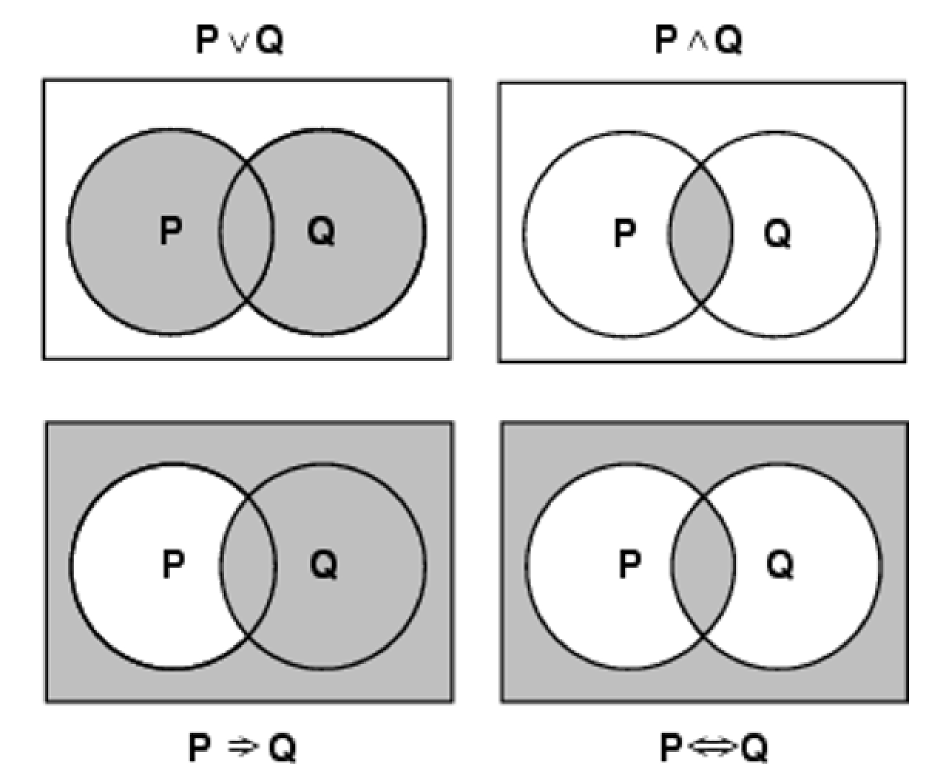
The five logical connectives:

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
False	False	True	False	False	True	True
False	True	True	False	True	True	False
True	False	False	False	True	False	False
True	True	False	True	True	True	True

Example complex sentence:

P	H	$P \vee H$	$(P \vee H) \wedge \neg H$	$((P \vee H) \wedge \neg H) \Rightarrow P$
False	False	False	False	True
False	True	True	False	True
True	False	True	True	True
True	True	True	False	True

Propositional Logic Venn diagrams of truth



Propositional Logic Inference Rules

- Logical inference is used to create new sentences that logically follow from a given set of predicate calculus sentences (KB).
- An inference rule is sound if every sentence X produced by an inference rule operating on a KB logically follows from the KB. (That is, the inference rule does not create any contradictions)
- An inference rule is complete if it is able to produce every expression that logically follows from (is entailed by) the KB. (Note the analogy to complete search algorithms.)

Propositional Logic Inference Rules: Soundness

- Here are some examples of sound rules of inference
  - *A rule is sound if its conclusion is true whenever the premise is true*
- Each can be shown to be sound using a truth table

RULE	PREMISE	CONCLUSION
Modus Ponens	$A, A \rightarrow B$	B
And Introduction	A, B	$A \wedge B$
And Elimination	$A \wedge B$	A
Double Negation	$\neg\neg A$	A
Unit Resolution	$A \vee B, \neg B$	A
Resolution	$A \vee B, \neg B \vee C$	$A \vee C$

Propositional Logic Proving things

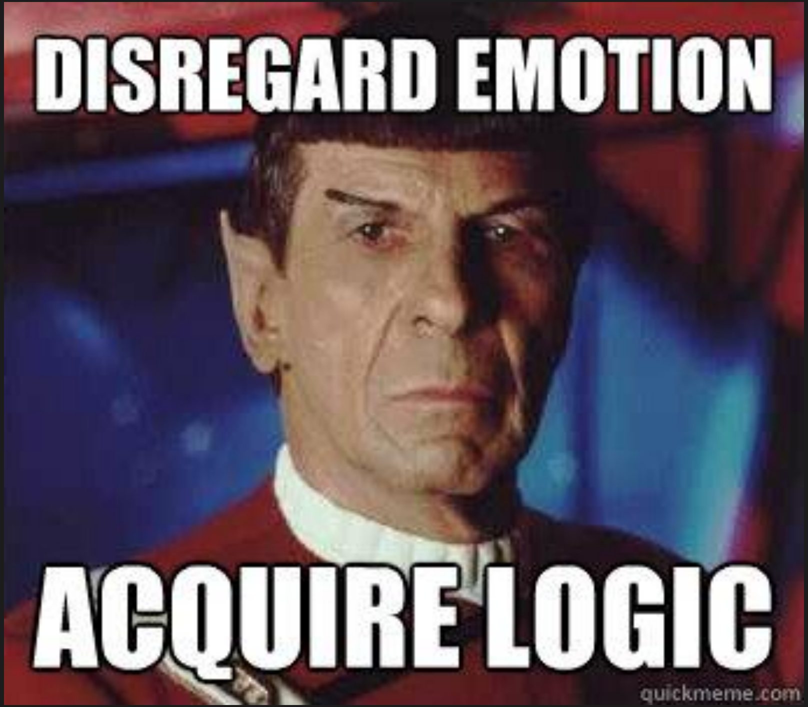
- A proof is a sequence of sentences, where each sentence is either a premise or a sentence derived from earlier sentences in the proof by one of the rules of inference.
- The last sentence is the theorem (also called goal or query) that we want to prove.
- Example “morning problem”

1 P	Premise	“It is early”
2 $P \rightarrow Q$	Premise	“If it is early, I’m tired”
3 Q	Modus Ponens (1, 2)	“I’m tired”
4 $(P \wedge Q) \rightarrow R$	Premise	“If it’s early and I’m tired, I want to nap”
5 $P \wedge Q$	And Introduction(1, 3)	“It is early and I’m tired”
6 R	Modus Ponens(4, 5)	“I want to nap”

Propositional logic is … weak.

Propositional Logic Problems

- Hard to make statements about the properties of individual instances
  - “Class is on Tuesday and Thursday”
  - “Today is Thursday”
  - “Class is today”
  - how to represent this in PL?
- Generalizations, patterns, regularities can’t easily be represented
  - “all triangles have 3 sides”
  - “There is an exception to every rule”
  - How to represent this in PL?



Introducing: First Order Logic

First order predicate Logic

- Operate on sets in different domains
- Involve Quantifiers
- Can operate on all propositional logic symbols and any truthy functions (aka predicates)

$x > y$

$x = y$

$x < y$

First order Logic: Predicates

Definition:

Predicates are truthy propositions that evaluate to truth values given some functional input.

Example:

$P(x, y) := x + y = 0$

$x = 1, y = -1$: $P(x, y)$ is true

$x = 1, y = 1$: $P(x, y)$ is false

Sets

Definition:

A *set* is a mathematical construct that collects distinct objects.

Common sets include:

Z: the set of all integers {…, -2, -1, 0, 1, 2, …}

N: the set of all natural numbers {0, 1, 2, …}

R: the set of real numbers { -∞,…,0,…0.4132425236…∞}

Sets can be nearly anything

classDays : {Tues, Thurs}

Each item in a set is unique

Set notation and operators you may use in this class

- brackets: {…}
  - contain items of a set
- Element of: ∈
  - denotes that an item is in a set e.g. $a \in \{a,b\}$
- Not element of: ∉
  - means the opposite e.g. $t \notin \{a,b\}$
- Empty set: ∅
  - denotes a set with nothing in it e.g. $\{\} = \emptyset$
- Set subtraction: $A - B$
  - operator that removes items in B from A
  - e.g. $A = \{a, t\}$, $B = \{t\}$ $A - B = \{a\}$

Set notation and operators you may use in this class

- Set intersection: $A \cap B$
  - an operator that collects only the items that are in both sets
  - e.g. $A \cap B = \{t\}$, where $A = \{a, t\}$ and $B = \{b, t\}$
- Set Union: $A \cup B$
  - opposite operator of intersection, combines all unique items from two sets
  - e.g. $A \cup B = \{a, b, t\}$, where $A = \{a, t\}$ and $B = \{b, t\}$
- Subset: $A \subseteq B$
  - indicates that one set is entirely present in another
  - e.g. $A \subseteq B$ where $A = \{b, t\}$ and $B = \{b, t\}$
- Proper subset: $A \subset B$
  - subset plus one element (or more) of B is not in A
  - e.g. $A \subset B$ where $A = \{t\}$ and $B = \{b, t\}$
- Not a (proper) subset: $A \not\subset B$
  - something in a is not in b

Quantifiers

Definition:

Quantifiers are a type of notation that denote a set of elements from a domain (i.e. a set).

They come in two forms: Universal and Existential

Universal Quantifier

Definition:

The universal quantifier, given by the symbol ∀ (read as "For All") indicates all items in a set.

Logical statements:

∀<vars> ∈ <Domain>, <statement> or ∀<vars> ∈ <Domain> : <statement>

e.g. $\forall\ x \in Z, x \leq x^2$ or $\forall\ x \in Z : x \leq x^2$

read as "for all x in Z, x is less than or equal to x squared"

evaluates to true if the statement evaluates to true for all items.

You may see me or others write using Set builder notation

{∀ <vars> : <statement on vars> } or {<vars> : <statement on vars> }

e.g. $\{\forall\ x : x \leq x^2 \}$ or $\{ x : x \leq x^2 \}$ creates a set of all x where $x \leq x^2$ is true.

Existential Quantifier

Definition:

The existential quantifier, given by the symbol ∃ (read "There Exists") indicates a single item in a set.

Logical statements:

∃ <vars> ∈ <Domain>, <statement> or ∃ <vars> ∈ <Domain> : <statement>

e.g. $\exists\ x \in Z, x \leq x^2$ or $\exists\ x \in Z : x \leq x^2$

"there exists x in Z such that x is less than or equal to x squared"

evaluates to true if the statement evaluates to true for *at least one item*.

Quantifier Examples

- Quantifiers can be part of logic statements
- “Everyone loves snow”
  - $\forall x \in P : \text{lovesSnow}(x)$
- “Noone loves snow”
  - $\forall x \in P : \neg\, \text{lovesSnow}(x)$
- “Someone loves snow”
  - $\exists x \in P : \text{lovesSnow}(x)$
- “At least someone doesn’t love snow”
  - $\exists x \in P : \neg\, \text{lovesSnow}(x)$

Quantifier Negation

- What happens when you negate a quantifier?
  - e.g. $\neg \forall x\, P(x)$
- Apply *DeDorgan's Law*
  - *19th* century British mathematician
- Law states:
  - $\neg \forall x\, P(x) \equiv \exists x \neg P(x)$
  - or
  - $\neg \exists\, x\, P(x) \equiv \forall\, x \neg P(x)$

Quantifier Negation Examples

- "Not Everyone loves snow"

  $\neg\ \forall x \in P : \text{lovesSnow}(x)$

  $\equiv \exists x \in P \neg\ \text{lovesSnow}(x)$

  (There exists at least one person that doesn't love snow)

- "Noone loves snow"

  - $\neg\ \exists x \in P : \text{lovesSnow}(x)$

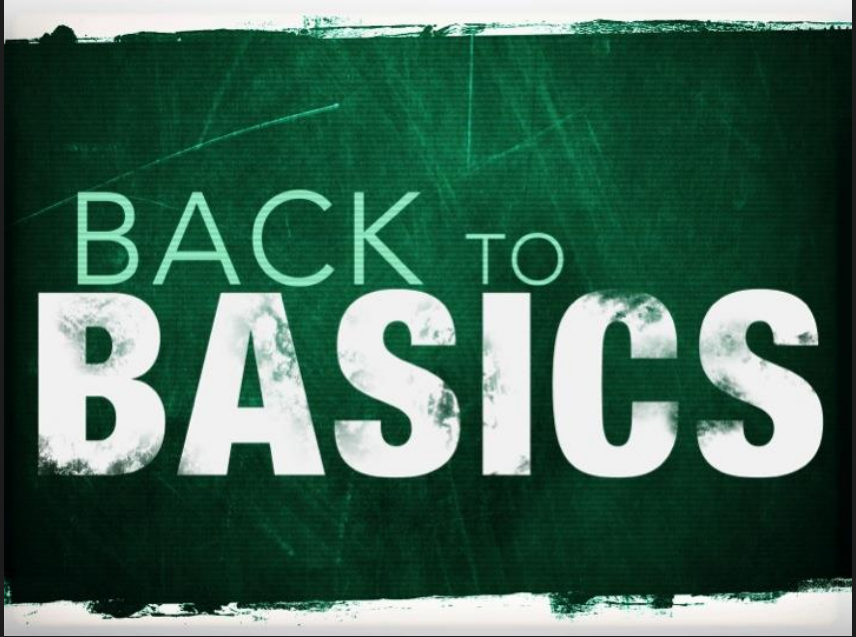
  $\equiv \forall x \in P : \neg\ \text{lovesSnow}(x)$

  (There exists no person that loves snow)

Wrap-up: Some misc. rules

- Quantifiers can be chained on the same statement or can be nested
  - "There is cure that cures every disease"
  - e.g. $\exists\ c \in \text{Cures}, \forall d \in \text{Diseases} : \text{cure}(c, d)$
  - or "Every disease has a cure"
  - e.g. $\forall d \in \text{Diseases}, \exists\ c \in \text{Cures} : \text{cure}(c, d)$
- Order of quantifiers matters
  - the two statements above mean very different things
  - changing the order affects the meaning
- Order doesn't matter for the same type of quantifier (e.g. $\exists\exists$ or $\forall\forall$)
  - e.g. a disease has a cure = a cure exists for a disease
  - $\exists\ c \in \text{Cures}, \exists\ d \in \text{Diseases} : \text{cure}(c, d)$
  - all diseases are cured by everything = all cures cure everything
  - $\forall\ c \in \text{Cures}, \forall\ d \in \text{Diseases} : \text{cure}(c, d)$

So that was a lot of “basics”



Time to dig in.

Portions of Material from
Rose Gamble – University of Tulsa

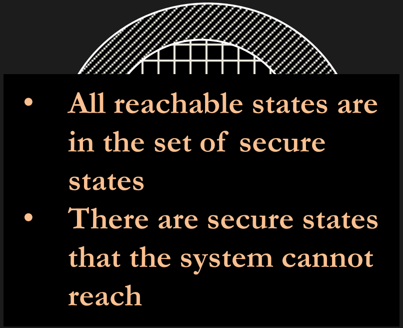
Formal Policy Assumptions

- Policies (ideally)
  - Unambiguously partition system states into secure and nonsecure
  - Correctly capture security requirements
  - Can be enforced
- Mechanisms (ideally)
  - Enforce policy and prevent non-secure states
  - Do not conflict with other mechanisms enforcing other policies
  - Implemented, maintained, and administered correctly
- This is where the numerous documents are used
  - How to define a policy
  - What standard mechanisms are used for each policy property enforcement
  - How a larger mechanism is formed
  - What global compliance issues policies must abide by

Formal Policy Protection States

- Subset of system state that deals with protection
- Let P be all *possible states*. Let Q be *secure states*. Let s be a *system state.* And Let R be the set of reachable states
  - If s is in P - Q, then s is a *non-secure state.*
  - For a secure system, all system states, s, must be in Q, i.e. ∀s ∈ P: s ∈ Q.
- Security policies characterize those s in Q (by defining what Q is)
- Security mechanisms prevent a state s in P-Q from being reached (the set R of reachable states) through some unauthorized transition
  - R ⊆ Q is a secure system
  - R = Q is a precise system
- The result of transforming an authorized state with an allowed transition should always be an authorized state
    - Following an authorization scheme – set of rules that direct the transitions

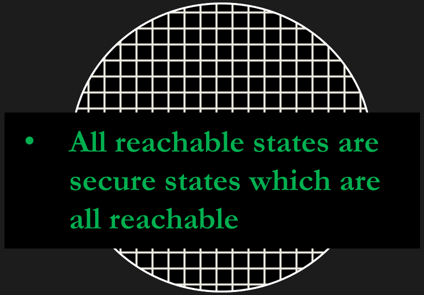
Venn Diagrams of Enforcement Mechanisms



- All reachable states are in the set of secure states
- There are secure states that the system cannot reach

Secure system

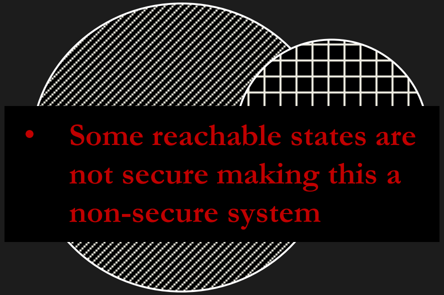
$\mathbf{R} \subseteq \mathbf{Q}$



- All reachable states are secure states which are all reachable

precise

$\mathbf{R} = \mathbf{Q}$



- Some reachable states are not secure making this a non-secure system

broad

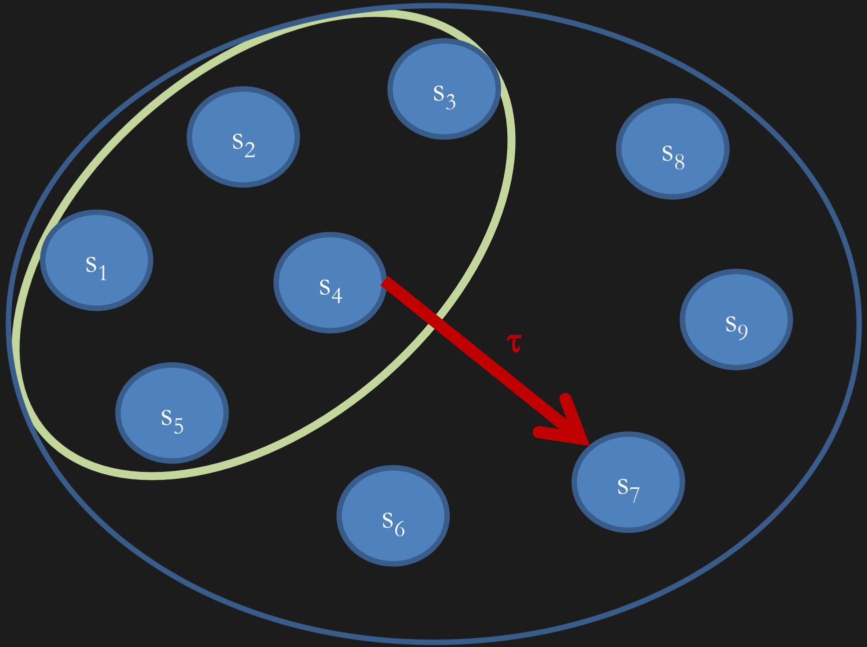
$\exists\ \mathbf{r} \in \mathbf{R} \mid \mathbf{r} \notin \mathbf{Q}$

set of all possible states, **P**

▨ **Q** - set of secure states defined by the policy, where $\mathbf{Q} \subseteq \mathbf{P}$

▦ **R** - set of reachable states by the protection mechanisms, where $\mathbf{R} \subseteq \mathbf{P}$

Example states



- $s_1 - s_9$ are all possible states (P)
- $s_1 - s_5$ are secure states (Q)
- A mechanism is needed to disallow transitions τ from $s_1 - s_5$ to $s_6 - s_9$ i.e. $s_6 - s_9$ should *not* be in R

Security Objectives as logic statements

- Confidentiality
  - Information is confidential with respect to some entity set if no member of the set can obtain the information
  - Top secret documents cannot be viewed by those with a secret clearance, e.g $\forall\ p \in \text{Secret}, \forall\ d \in \text{TSDocs} : \neg\ \text{read}\ (p, d)$
- Integrity
  - Information has integrity if it is not modified by members of unauthorized sets and authorized modifications are logged appropriately
  - Data integrity (conveyance and storage) –
    $\exists\ d \in \text{Docs}, \forall p \in \text{Users} : \text{modify}(p, d) \wedge \text{authorized}(p, d) \Leftrightarrow (d, p, \text{“modify”}) \in \text{auditLog}$
- Availability
  - Information is available with respect to some entity set if all members of the set can access the information
    - Access is granted or not - traditional
    - Access may be associated with a response time – quality of service level agreement
  - $\exists\ obj \in \text{Objects}, \forall\ p \in \text{Users} : \text{“read”} \in A[p, obj]$

Assumptions in the use of Formal Methods

Prove that the information system can be trusted

- Proof has no errors
  - Math can be done incorrectly manually
  - Bugs in automated theorem provers
- Preconditions hold in environment in which S is to be used
  - Stated as local, shared, variables or constants
  - Environment must be equivalent
- S transformed into executable S′ whose actions follow source code
- Hardware executes S′ as intended

Assumptions play a major role and must be understood and made explicit

Security Mechanisms must be precise

- Define allowable state transitions
- Mechanisms must be clear on how they allow/deny the state transition so that its output doesn't provide any information it shouldn't
  - Could create a covert channel
    - Communication path not designed for communication

Simple (Phyiscal Covert Channel)

Common

STAGE 2
Evolves from Metapod
Put Butterfree on the Stage 1 card
Butterfree
70 HP
Butterfly Pokémon. Length: 3' 7", Weight: 71 lbs.
Whirlwind If your opponent has any Benched Pokémon, he or she chooses 1 of them and switches it with the Defending Pokémon. (Do the damage before switching the Pokémon.)
20
Mega Drain Remove a number of damage counters from Butterfree equal to half the damage done to the Defending Pokémon (after applying Weakness and Resistance) (rounded up to the nearest 10).
40
weakness
resistance
-30
retreat cost
In battle, it flaps its wings at high speed to release highly toxic dust into the air. LV. 28 #12
33/64

STAGE 2
Evolves from Charmeleon
Put Charizard on the Stage 1 card
Charizard
120 HP
Flame Pokémon. Length: 5' 7", Weight: 200 lbs.
Pokémon Power: Energy Burn As often as you like during your turn (before your attack), you may turn all Energy attached to Charizard into Energy for the rest of the turn. This power can't be used if Charizard is Asleep, Confused, or Paralyzed.
Fire Spin Discard 2 Energy cards attached to Charizard in order to use this attack.
100
weakness
resistance
-30
retreat cost
Spits fire that is hot enough to melt boulders. Known to unintentionally cause forest fires. LV. 76 #6
4/102

Holographic
(10 micrometers thicker)

Simple (Phyiscal Covert Channel)

=> Weigh booster packs and get more foil cards

Simple Auth Example

Inputs name, password => output Good or Bad
If name invalid, immediately print Bad; else access database

Problem: time output of Bad outputs, can allow an attacker to determine if name valid. This means timing can be a covert channel

Mechanisms and Covert Channels

- Mechanisms must be clear on how they allow/deny the state transition so that its output doesn't provide any information it shouldn't
- For a program and security policy, there exists a precise, security mechanism that minimizes the number of denials to legitimate actions
- There is no effective procedure to determine a maximally precise, security mechanism for any policy and program.
- Good policies attempt to limit covert channels through clear and effective mechanisms

Map our student parking policy

I. STUDENT PARKING POLICY

A. STUDENT: The term ‘student’ refers to anyone who is currently enrolled (registered) for classes held on or off the UNO Campus, either part or full-time, whether or not it leads to an academic degree.

B. Individuals who work for the University as student workers and are registered for classes are considered students.

C. Students desiring to park at the UNO Dodge, Pacific or Center locations must purchase and display a valid parking permit.

D. Student parking areas are designated by parking lot signs red in color. Specific student lots are as follows: Lots A, D, F, G, H, K, N, T, V, X, St. Margaret Mary’s Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area) at the Dodge campus; Lots 2, 5, 8, 9 (South portion) and 14 at the Pacific campus and Lot 20 at the Center campus. Permits can also be purchased for the East and West Garage, check on availability.

E. Students are restricted to student lots from 7 a.m. to 2:30 p.m., Monday through Friday. After 2:30 p.m., vehicles bearing valid parking permits may park in Student Lots and designated Faculty/Staff Lots as follows: G, H, M, S , X at the Dodge campus, and Lot 6 at the Pacific campus.

F. After 7 p.m., vehicles bearing valid parking permits may park in designated Faculty/Staff Lots R and W at the Dodge campus, and Lot 4 at the Pacific campus.

G. Students with “Night Only” parking permits may park on campus after 2:30 p.m. in the lots specified above. If you need to park on campus before 2:30 p.m., you may park in the Crossroads Mall Parking Garage and take the free shuttle bus which runs from 7 a.m. until 6 p.m., or stop by Parking Services and obtain a Temporary Parking Permit for one or two consecutive days to allow your vehicle on campus prior to 2:30 p.m. Only four free temporary permits issued per academic year.

H. Graduate Teaching Assistants may apply for G.T.A. parking privileges. G.T.A. permits are restricted to Faculty/Staff lots only.

I. Parking is also available in the Crossroads Mall Parking Garage from 7 a.m. - 7 p.m. when classes are in session during fall and spring semesters. No parking permit is required to park at the Crossroads Mall Parking Garage. (See Crossroads Mall Parking Garage for more details).

Map our student parking policy

I. STUDENT PARKING POLICY

A. STUDENT: The term ‘student’ refers to anyone who is currently enrolled (registered) for classes held on or off the UNO Campus, either part or full-time, whether or not it leads to an academic degree.

..

P := all possible persons

S := students

$\forall p \in P$, $isStudent(p) \Leftrightarrow isRegistered(p) \Leftrightarrow p \in S$

Formally Modelling Policy

Example: Map our student parking policy

I. STUDENT PARKING POLICY

B. Individuals who work for the University as student workers and are registered for classes are considered students.

..

$\forall p \in P$, $isStudentWorker(p) \wedge isRegistered(p) \Rightarrow isStudent(p) \wedge p \in S$

(from this we know the policy is redundant, since $isStudent(p) \Leftrightarrow isRegistered(p)$ is established by A)

Example: Map our student parking policy

I. STUDENT PARKING POLICY
C. Students desiring to park at the UNO Dodge, Pacific or Center locations must purchase and display a valid parking permit.

$\text{DesignatedAreas} := \{\text{Dodge, Pacific, Center}\}$
$\forall x \in \text{DesignatedAreas},\ s \in S,\ \text{park}(s, x) \Leftrightarrow \text{hasPermit}(s) \land \text{displaysPermit}(s)$

Example: Map our student parking policy

I. STUDENT PARKING POLICY

D. Student parking areas are designated by parking lot signs red in color. Specific student lots are as follows: Lots A, D, F, G, H, K, N, T, V, X, St. Margaret Mary's Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area) at the Dodge campus; Lots 2, 5, 8, 9 (South portion) and 14 at the Pacific campus and Lot 20 at the Center campus. Permits can also be purchased for the East and West Garage, check on availability.

…

studentLotsDodge := {A, D, F, G, H, K, N, T, V, X, St. Margaret Mary's Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area)}

studentLotsPacific := {2, 5, 8, 9(south portion), 14}

studentLotsCenter := {20}

specialLots := {East Garage, West Garage} OR {East/West} - this is an ambiguity in the policy

$\text{studentLots} = \text{studentLotsDodge} \cup \text{studentLotsPacific} \cup \text{studentLotsCenter}$

$\text{studentLots} \subset \text{campusLots}$

Example: Map our student parking policy

I. STUDENT PARKING POLICY

E. Students are restricted to student lots from 7 a.m. to 2:30 p.m., Monday through Friday. After 2:30 p.m., vehicles bearing valid parking permits may park in Student Lots and designated Faculty/Staff Lots as follows: G, H, M, S , X at the Dodge campus, and Lot 6 at the Pacific campus.

…

$\text{facultyLots} := \{G, H, M, S, X, 6\}$

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$\qquad (t \in \{7\text{am},\ldots,2{:}30\text{pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots}) \vee$

$\qquad (t \in \{2{:}30\text{pm},\ldots 7\text{am}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots})$

Example: Map our student parking policy

I. STUDENT PARKING POLICY

F. After 7 p.m., vehicles bearing valid parking permits may park in designated Faculty/Staff Lots R and W at the Dodge campus, and Lot 4 at the Pacific campus.

$\text{facultyLotsNight} := \{R, W, 4\}$ or $\{R, W, 4\} \cup \text{facultyLots}$? – another ambiguity

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$\quad (t \in \{7am,\ldots,2{:}30pm\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots}) \vee$

$\quad (t \in \{2{:}30pm,\ldots 7pm\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots}) \vee$

$\quad (t \in \{7pm,\ldots,7am\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight})$

Example: Map our student parking policy

I. STUDENT PARKING POLICY

G. Students with “Night Only” parking permits may park on campus after 2:30 p.m. in the lots specified above. If you need to park on campus before 2:30 p.m., you may park in the Crossroads Mall Parking Garage and take the free shuttle bus which runs from 7 a.m. until 6 p.m., or stop by Parking Services and obtain a Temporary Parking Permit for one or two consecutive days to allow your vehicle on campus prior to 2:30 p.m. Only four free temporary permits issued per academic year.

…

changes previous statements by adding a permit type check adds new night student constraint and…

$\text{maxTemporaryPermits} = 4/\text{yr}$

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$((\text{permitType}(s) = \text{“normal”} \lor \text{hasTemporaryPass}(s)) \land t \in \{\text{7am},\ldots,\text{2:30pm}\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots}) \lor$

$((\text{permitType}(s) = \text{“night only”}) \land t \in \{\text{7am},\ldots,\text{2:30pm}\} \land d \in \{M, T, W, Th, F\} \land l = \text{“Crossroads”}) \lor$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \land t \in \{\text{2:30pm},\ldots\text{7pm}\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots} \cup \text{facultyLots}) \lor$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \land t \in \{\text{7pm},\ldots,\text{7am}\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight})$

Example: Map our student parking policy

I. STUDENT PARKING POLICY

H. Graduate Teaching Assistants may apply for G.T.A. parking privileges. G.T.A. permits are restricted to Faculty/Staff lots only.

…

$GTA \subset S$

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$((\text{permitType}(s) = \text{“normal”} \lor \text{hasTemporaryPass}(s)) \land t \in \{7am,\ldots,2{:}30pm\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots}) \lor$

$((\text{permitType}(s) = \text{“night only”}) \land t \in \{7am,\ldots,2{:}30pm\} \land d \in \{M, T, W, Th, F\} \land l = \text{“Crossroads”}) \lor$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \land t \in \{2{:}30pm,\ldots 7pm\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots} \cup \text{facultyLots}) \lor$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \land t \in \{7pm,\ldots,7am\} \land d \in \{M, T, W, Th, F\} \land l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight}) \lor$

$(\text{permitType}(s) = GTA \land l \in \text{facultyLots})$

Formally Modelling Policy

Example: Map our student parking policy

I. STUDENT PARKING POLICY

I. Parking is also available in the Crossroads Mall Parking Garage from 7 a.m. - 7 p.m. when classes are in session during fall and spring semesters. No parking permit is required to park at the Crossroads Mall Parking Garage. (See Crossroads Mall Parking Garage for more details).

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$((\text{permitType}(s) = \text{“normal”} \vee \text{hasTemporaryPass}(s)) \wedge t \in \{\text{7am},\ldots,\text{2:30pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots}) \vee$

$((\text{permitType}(s) = \text{“night only”}) \wedge t \in \{\text{7am},\ldots,\text{2:30pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l = \text{“Crossroads”}) \vee$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{\text{2:30pm},\ldots\text{7pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots}) \vee$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{\text{7pm},\ldots,\text{7am}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight}) \vee$

$(\text{permitType}(s) = \text{GTA} \wedge l \in \text{facultyLots}) \vee$

$(l = \text{“Crossroads”} \wedge t \in \{\text{7am},\ldots,\text{7pm}\})$

going to ignore the “fall and spring” part

Example: resolve conflicts, eliminate redundancy

I. STUDENT PARKING POLICY (formalized)

P := all possible persons

S := students

$\forall p \in P, \text{isStudent}(p) \Leftrightarrow \text{isRegistered}(p) \Leftrightarrow p \in S$

~~DesignatedAreas := {Dodge, Pacific, Center}~~

~~$\forall x \in \text{DesignatedAreas}, s \in S, \text{park}(s, x) \Leftrightarrow \text{hasPermit}(s) \wedge \text{displaysPermit}(s)$~~

studentLotsDodge := {A, D, F, G, H, K, N, T, V, X, St. Margaret Mary’s Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area)}

studentLotsPacific := {2, 5, 8, 9(south portion), 14}

studentLotsCenter := {20}

specialLots := {East Garage, West Garage} ~~OR {East/West} - this is an ambiguity in the policy~~

$\text{studentLots} = \text{studentLotsDodge} \cup \text{studentLotsPacific} \cup \text{studentLotsCenter}$

$\text{studentLots} \subset \text{campusLots}$

facultyLots := {G, H, M, S, X, 6}

$\text{facultyLotsNight} := \{R, W, 4\} \text{ or } \{R, W, 4\} \cup \text{facultyLots}$

maxTemporaryPermits = 4/yr

$\text{GTA} \subset S$

$\forall t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \text{park}(s, l) \Leftrightarrow$

$((\text{permitType}(s) = \text{“normal”} \vee \text{hasTemporaryPass}(s)) \wedge t \in \{\text{7am},\ldots,\text{2:30pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots}) \vee$

~~$((\text{permitType}(s) = \text{“night only”}) \wedge t \in \{\text{7am},\ldots,\text{2:30pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l = \text{“Crossroads”}) \vee$~~

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{\text{2:30pm},\ldots\text{7pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots}) \vee$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{\text{7pm},\ldots,\text{7am}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight}) \vee$

$(\text{permitType}(s) = \text{GTA} \wedge l \in \text{facultyLots}) \vee$

$(l = \text{“Crossroads”} \wedge t \in \{\text{7am},\ldots,\text{7pm}\})$

Formally Modelling Policy

Example: Final result – No ambiguity

I. STUDENT PARKING POLICY (formalized)

P := all possible persons

S := students

$\forall p \in P$, $\text{isStudent}(p) \Leftrightarrow \text{isRegistered}(p) \Leftrightarrow p \in S$

studentLotsDodge := {A, D, F, G, H, K, N, T, V, X, St. Margaret Mary’s Church lot (West area, East/West Drive South of the church unless otherwise posted), First Christian Church lot (West area)}

studentLotsPacific := {2, 5, 8, 9(south portion), 14}

studentLotsCenter := {20}

specialLots := {East Garage, West Garage}

studentLots = studentLotsDodge $\cup$ studentLotsPacific $\cup$ studentLotsCenter

studentLots $\subset$ campusLots

facultyLots := {G, H, M, S, X, 6}

facultyLotsNight := {R, W, 4} or {R, W, 4} $\cup$ facultyLots

maxTemporaryPermits = 4/yr

GTA $\subset$ S

$\forall$t $\in$ Time, d $\in$ Weekdays, s $\in$ S, l $\in$ campusLots, park(s, l) $\Leftrightarrow$

((permitType(s) = “normal” $\vee$ hasTemporaryPass(s)) $\wedge$ t $\in$ {7am,…,2:30pm} $\wedge$ d $\in$ {M, T, W, Th, F} $\wedge$ l $\in$ studentLots) $\vee$

(permitType(s) $\in$ {“normal”, “night only”} $\wedge$ t $\in$ {2:30pm,…7pm} $\wedge$ d $\in$ {M, T, W, Th, F} $\wedge$ l $\in$ studentLots $\cup$ facultyLots) $\vee$

(permitType(s) $\in$ {“normal”, “night only”} $\wedge$ t $\in$ {7pm,…,7am} $\wedge$ d $\in$ {M, T, W, Th, F} $\wedge$ l $\in$ studentLots $\cup$ facultyLots $\cup$ facultyLotsNight)$\vee$

(permitType(s) = GTA $\wedge$ l $\in$ facultyLots) $\vee$

(l = “Crossroads” $\wedge$ t $\in$ {7am,…,7pm})

Formally Modelling Policy

Notice, we can now state what policy violations look like.
Simply negate the policy statement

Example: Final result – violation enumeration

I. STUDENT PARKING POLICY Violation cases

¬[∀t ∈ Time, d ∈ Weekdays, s ∈ S, l ∈ campusLots, park(s, l) ⇔

((permitType(s) = “normal” ∨ hasTemporaryPass(s)) ∧ t ∈ {7am,…,2:30pm} ∧ d ∈ {M, T, W, Th, F} ∧ l ∈ studentLots) ∨

(permitType(s) ∈ {“normal”, “night only”} ∧ t ∈ {2:30pm,…7pm} ∧ d ∈ {M, T, W, Th, F} ∧ l ∈ studentLots ∪ facultyLots) ∨

(permitType(s) ∈ {“normal”, “night only”} ∧ t ∈ {7pm,…,7am} ∧ d ∈ {M, T, W, Th, F} ∧ l ∈ studentLots ∪ facultyLots ∪ facultyLotsNight)∨

(permitType(s) = GTA ⇒ l ∈ facultyLots) ∨

(l = “Crossroads” ∧ t ∈ {7am,…,7pm})]

Example: Final result – violation enumeration

I. STUDENT PARKING POLICY Violation cases

$\exists\, t \in \text{Time}, d \in \text{Weekdays}, s \in S, l \in \text{campusLots}, \neg\, [\text{park}(s, l) \Leftrightarrow$

$((\text{permitType}(s) = \text{“normal”} \vee \text{hasTemporaryPass}(s)) \wedge t \in \{7\text{am},\ldots,2{:}30\text{pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots}) \vee$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{2{:}30\text{pm},\ldots 7\text{pm}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots}) \vee$

$(\text{permitType}(s) \in \{\text{“normal”}, \text{“night only”}\} \wedge t \in \{7\text{pm},\ldots,7\text{am}\} \wedge d \in \{M, T, W, Th, F\} \wedge l \in \text{studentLots} \cup \text{facultyLots} \cup \text{facultyLotsNight}) \vee$

$(\text{permitType}(s) = \text{GTA} \wedge l \in \text{facultyLots}) \vee$

$(l = \text{“Crossroads”} \wedge t \in \{7\text{am},\ldots,7\text{pm}\}\ )]$

can distribute the negation further following De Morgan’s laws… its nice this way to say “find me a t, d, s, l such that these conditions aren’t met

e.g.

$\text{permitType}(s) = \text{“night only”} \wedge t \in \{7\text{am},\ldots,2{:}30\text{pm}\} \wedge d \in \{M, T, W, Th, F\}$ and $l \in \text{studentLots}$

[night student parking in the day]

$\text{permitType}(s) = \text{“normal”} \wedge t \in \{7\text{am},\ldots,2{:}30\text{pm}\} \wedge d \in \{M, T, W, Th, F\}$ and $l \in \text{facultyLots}$

[student parking in faculty lots at an unacceptable time]

Despite sounding hard – policies stated this way can be enumerated by a machine automatically.

Reading

Optional Reading:

Using First-Order Logic to Reason about Policies

Joseph Y. Halpern and Vicky Weissman Cornell University

http://arxiv.org/pdf/cs/0601034.pdf

Homework

Work on Project

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics
mlhale@unomaha.edu

Twitter: @mlhale_