Logistics

- Assignment each week starting with Assignment 2
- The proposal for a final project is due in approximately a month
  - New project ideas were added on the class website
  - For Network Security and System Security type projects see the projects under Dr. Rick Skowrya
  - For simpler topics see the Mark Reynolds topics
  - The Andrei Lapets topics discuss SMT solvers.

Handout 07

- SAT Solvers are an efficient way of deciding if a WFF is satisfiable
- SMT stands for Satisfiability Modulo Theory
- What is theory?
  - Formal first order theory which is propositional logic extended
- SMT solver = SAT solver + ? (? = fragments of first order)
- First Order Logic
  - In any formal logic you have formal syntax, formal proof theory, and formal semantics.
  - At a minimum formal proof theory and formal semantics must hold the condition of soundness
  - In First order logic it’s beyond hope to have completeness as well.
  - Propositional logic is a subset of First Order Logic
- Predicate Logic aka First Order
  - for all x, if x is a bird then x has wings $\forall x(B(x) \rightarrow W(x))$
  - for all x, if x has wings then x can fly $\forall x(W(x) \rightarrow F(x))$
  - Coco is a bird $B(c)$
  - Coco has wings $W(c)$
  - Coco’s mother can fly $F(m(c))$
  - it is not the case that for all x $\neg(\forall x(B(x) \rightarrow W(x)))$
  - There exists an x such $\exists x(B(x) \rightarrow W(x))$
• As you can see with the above examples, predicate logic is a way of formally encoding English logic.

• It is comprised of quantifiers such as \( \forall, \exists \).

• The variable \( c \) is a constant.

• And \( \neg \) is an assertion.

• Vocabulary
  
  - The vocabulary of predicate logic consists of:
  - Set \( P \) of predicate symbols, each of arity \( n \geq 0 \)
  - Set \( F \) of function symbols each of arity \( n \geq 1 \)
  - Set \( C \) of constant symbols arity = 0
  - Arity is the number of operands that a function takes.

• Terms
  
  - A variable \( x \) is a term.
  - A constant \( c \in C \) is a term.
  - if \( t_1, \ldots, t_n \) are terms and \( f \in F \) is a \( n \)-ary \( f(t_1, \ldots, t_n) \) is a term.
  - In BNF notation the above translates to:
    - \( t ::=} x | c | f(t_1, \ldots, t_n) \)

• Well Formed Formulas aka WFF’s
  
  - if \( t_1, \ldots, t_n \) are terms and \( p \in t \) has arity \( n = 0 \) then \( P(t_1, \ldots, t_n) \) is a WFF (an atomic WFF)
  - if \( \varphi \) is a WFF then so is \( \neg \varphi \)
  - if \( \varphi \) and \( \psi \) are both WFF’s then so are \( (\varphi \lor \psi) \), \( (\varphi \land \psi) \), and \( (\varphi \rightarrow \psi) \).
  - if \( \varphi \) is a WFF and \( x \) is a variable then so are \( (\forall x \varphi) \) and \( (\exists x \varphi) \)
  - In BNF that looks like:
    - \( \varphi ::=} P(t_1, \ldots, t_n) | \neg \varphi | (\varphi \lor \varphi) | (\varphi \land \varphi) | (\forall x \varphi) | (\exists x \varphi) \)

• To turn Propositional logic into First Order, change all atoms into zero-ary predicates.

• Free and Bound variables
  
  - a variable \( x \) may occur free or bound in a WFF \( \varphi \)
  - if \( x \) is bound in \( \varphi \) then there are \( \geq 0 \) bound occurrences of \( x \) and \( \geq 1 \) binding occurrences of \( x \) in \( P \).
  - a binding occurrence of \( x \) is of form \( \forall x \) or \( \exists x \)
  - if a binding occurrence of \( x \) occurs as \( (Qx \varphi) \) where \( Q \in \{\forall, \exists\} \) then \( \varphi \) is the scope of the binding occurrence.
  - The scope of two binding occurrences may be disjoint, nested but cannot overlap.
  - Assumption every variable \( x \) has \( \leq 1 \) binding occurrence in any WFF
  - See page 6 of HD 07 for an example.
- $\varphi$ is closed iff $FV(\varphi) = \emptyset$
- You can rename the same variable $x$ in different scopes. (See HD 07 for examples).

- **Equivalence Relations**
  - $\forall x \ x \sim x$ reflexivity
  - $\forall x \forall y \ x \sim y \rightarrow y \sim x$ symmetry
  - $\forall x \forall y \forall z \ (x \sim y \land y \sim z \rightarrow x \sim z)$ transitivity