

# ECE 741/841

Victor Carreño

27 August 2002

## What is Formal Methods in System Design?

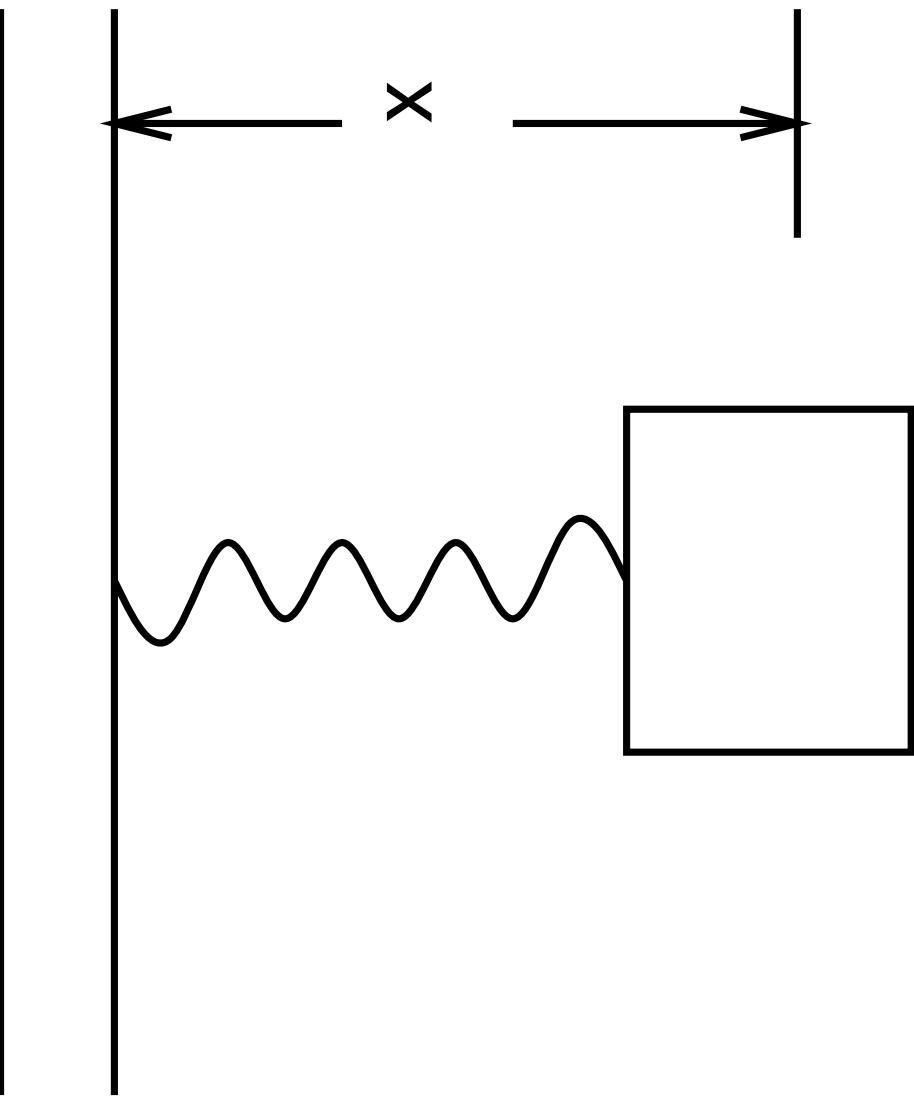
The use of mathematical logic for the specification, refinement, design and verification of digital and hybrid systems.

A hybrid system contains systems that can or must be represented with continuous and discrete mathematics. e.g. physical and digital components.

## **Models in Science and Engineering**

- Scientist establish models of physical phenomena that hold under given constraints.
- This process is largely an inductive process.
- Engineers use mathematical models to the creation of physical systems that will behave in a predetermined and desirable way.
- This process is largely a deductive process.

## Example



## Model

- Algebraic equations and infinitesimal calculus is used to model and analyze continuous systems.

$$\frac{\partial^2 x}{\partial t^2} + C_1 \frac{\partial x}{\partial t} + C_2 = 0$$

- Mathematical logic is used to model and analyze discrete and hybrid systems.

$$f = (a \wedge b) \vee c$$

$$\forall x. \exists y. y > x$$

## Analysis

- Differential equations are "solved" by finding values or expressions which satisfy the equation.
- Logical statements are "solved" by establishing the validity or invalidity (truth or falsehood) of the statement.

## Induction

- From the instance to the rule.

Ex.:

I have observed 1258 dogs and they all have four legs.  
rule(law) All dogs have four legs.

## Deduction

- From the rule to the instance.

Ex.:

All dogs have four legs.

This is a dog, therefore, it must have four legs.

## The Name Formal

- Formal comes from form.
- The validity of a statement is based on its form:

all  $\Diamond$  are  $\gamma$

This is a  $\Diamond$  therefore it must be a  $\gamma$

## Rules of Inference

- Truth preserving rules.
- We are already familiar with some truth preserving rules.
- From algebra:

$$x = y$$

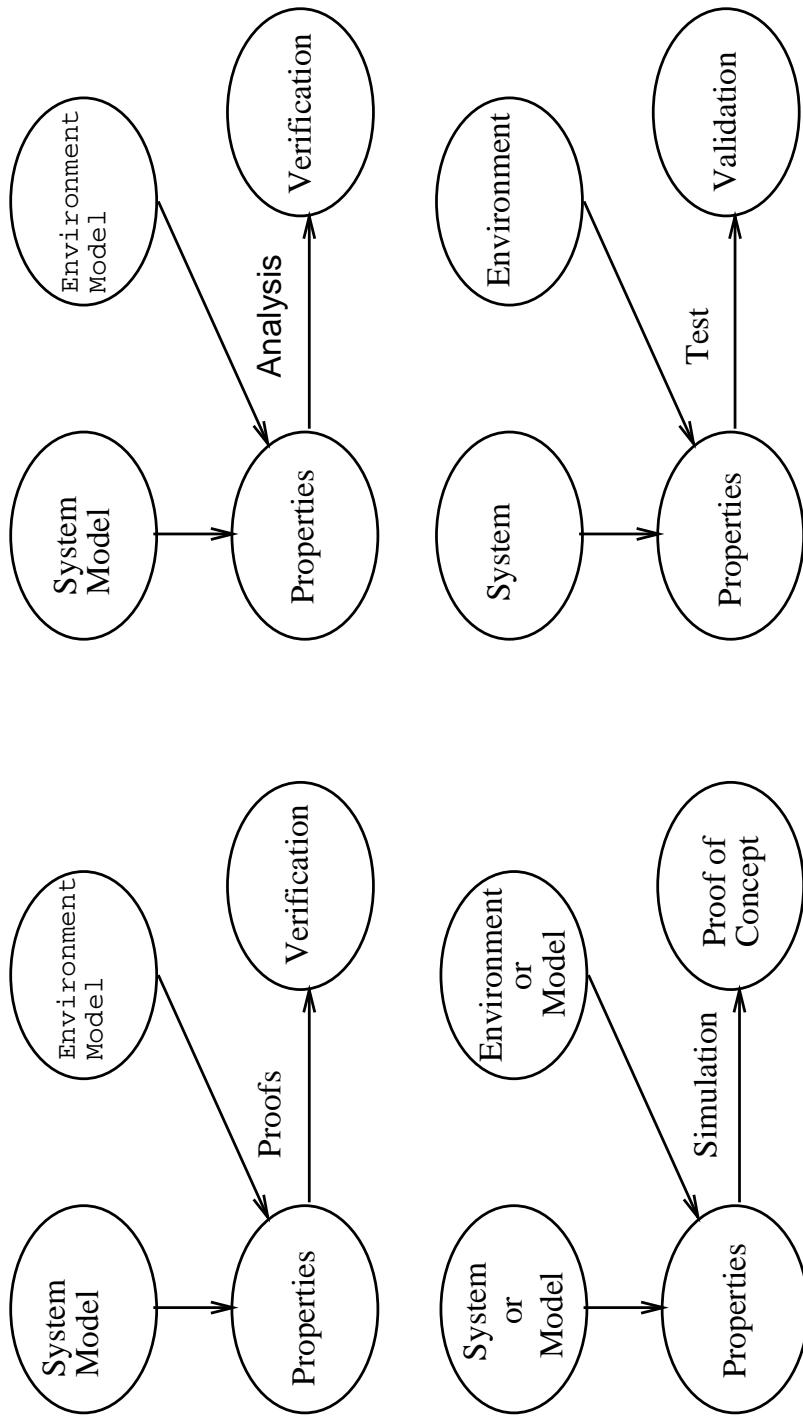
add 2 to each side of the equation

$$x + 2 = y + 2$$

- In logic, from premises and using deduction, we can infer a conclusion.

## Verification

The use of Formal Techniques is similar to the analysis performed in other disciplines:

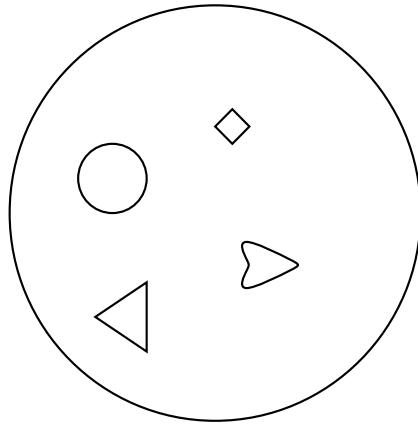
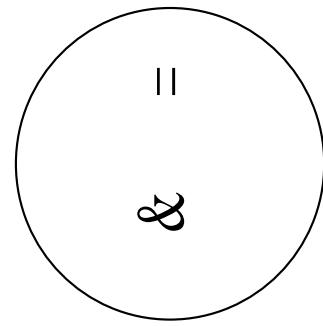


## Syntax

Definition:

- syntax*, n. 1. *Gram.* a. the patterns of formation of sentences and phrases from words in a particular language. 2. *Logic.* a. that branch of modern logic which studies the various kinds of signs that occur in a system and the possible arrangements of those signs, complete abstraction being made of the meaning of the signs.

## Syntactic System



$\triangle \& \heartsuit = \triangle$

$\circ \& \heartsuit = \circ$

$\triangle \& \circ = \diamond$

## Syntax

Because we can separate syntax and semantics, we can manipulate symbols syntactically and preserve "validity" (as long as the system is sound).

## Semantics

semantics, n. 1. *Linguistics*: the study of meaning and changes of meaning. 2. that branch of modern logic which studies the relations between signs and what they denote or signify.

## **Objective of the Course**

Take a system which is sound and complete (propositional logic, first order logic and higher-order logic) and use it to represent (model) and analyze problems of interest.

## The Model

”The suitability of a mathematical model depends strongly on the problem at hand. Ideally, we want a model to represent everything that is important about the process and ignore everything else. It is difficult to realize this ideal, because we are often not sure what aspects of the real world are important. In Fact, the process of deciding which aspects are important can be one of the most difficult and rewarding steps in specifying a mathematical model.”

Stanat and McAllister, *Discrete Mathematics in Computer Science*, Prentice-Hall, 1977.

## Example

I am having a party. There are males and females coming to the party. There are 48% males and 52% females. I will serve roasted chicken for dinner. Each person will eat  $1/3$  of a chicken.  $1/5$  of people coming to the party are vegetarian and will not eat chicken.

If I make a model for this system, what would the purpose of the model? what am I trying to obtain or calculate from the model?

## Atomic Sentences

It will rain today.

It will not rain tomorrow.

Symbols to represent atomic sentences:

$p, q, r, \dots$  or  $p_1, p_2, p_3, \dots$

## Connectives and More Complex Sentences

If it rains today, then it will also rain tomorrow.

¬ The negation of  $p$  is denoted by  $\neg p$ .

∨ Given  $p$  and  $q$  the disjunction  $p \vee q$  denotes that  $p$  is true or  $q$  is true or **both**  $p$  and  $q$  are true.

∧ Given  $p$  and  $q$  the conjunction  $p \wedge q$  denotes that both  $p$  and  $q$  are true.

→ Given  $p$  and  $q$  the implication  $p \rightarrow q$  denotes that if  $p$  is true then  $q$  is true.

Logical implication does not mean causality.

## Binding Priorities for Connectives

$\neg$  binds more tightly than  $\vee$  and  $\wedge$ , and disjunction and conjunction bind more tightly than  $\rightarrow$ .

$\neg p \vee q$  means  $(\neg p) \vee q$

$p \wedge q \rightarrow r$  means  $(p \wedge q) \rightarrow r$

$p \rightarrow q \wedge r$  means  $p \rightarrow (q \wedge r)$

## **Examples and Homework**