Introducción a Logica formal

Prof. Ernesto Rodriguez

Universidad del Itsmo

erodriguez@unis.edu.gt

La Situación:

- Un sistema tiene una lista de requisitos.
- El sistema debe cumplir con reglas, estas se pueden expresar como *invariantes*.
- Cada vez que el sistema cambia su estado, se debe asegurar que las invariantes se cumplan.
- **Ejemplos:**
  - Un usuario transfiere fondos a otro usuario.
    - El saldo de todos los usuarios es mayor o igual a cero.
    - El saldo de todos los usuarios es la suma de las transacciones.
  - Un tren debe ser colocado en el riel que lo lleve a su destino.
    - Jamas deben haber dos trenes en la misma posición.
    - El tren debe alcanzar su destino en tiempo finito.

La Situación:

- El sistema puede tener cientos de requisitos e invariantes.
- En el sistema trabajan muchas personas.
- Es altamente costoso verificar que los requisitos e invariantes se cúmplen cada vez que se actualiza el codigo.
- El sistema esta distribuido.
- El sistema evoluciona constantemente.
- El lenguaje natural es ambigüo

Incluso si el sistema esta bien definido:

- No es possible correr el sistema en todos los casos posibles (no habria necesidad del sistema)
- El halting problem no es decidible.
- Las propiedades de comportamiento de un programa no son decidibles: Teorema de Rice.
- No importa que metodo utilizemos para validar el sistema, el método debe hacerlo en tiempo finito.

¿Podemos hacer algo?


Yes We Can!
WAR PRODUCTION CO-ORDINATING COMMITTEE

Verificación automatizada

- Se ejecutan continuamente.
- Existen varios metodos:
  - Pruebas:
    - Casos individuales
    - Casos aleatoreos
    - Casos construidos inductivamente
  - Verificación formal:
    - Analisis de flujo
    - Theorem provers: Z3, Coq
    - Lenguajes de modelación (Promela)
  - Sistemas de tipos:
    - Sistemas de primer orden
    - Sistemas de orden superior
    - Sistemas de categorias superiores (Higher kinds)
- Pueden validar numerosas condiciones en poco tiempo.

Métodos formales vs. Pruebas automatizadas

Metodos formales	**Pruebas automatizadas**
Verifican todos los casos	Verifican numero finito de casos
No decidibles	Decidibles
Dificiles de implementar	Faciles de implementar
Alto costo a cambios en el sistema	Mediano costo a cambios en el sistema

La base de todo metod de verificación es: **Logica formal**

Logica Formal: Ejemplos

- Lenguaje formal para describir objetos
- Consiste de:
  - Predicados
  - Igualdad
  - Negación
  - Operadores boleanos
  - Cuantificadores
- Ejemplos:
  - Representación de cuentas
  - Representación de un banco
  - Abonar cuenta

Sematicas operacionales

- Se utilizan para describir el comportamiento de un sistema.
- Describen como se transforma el estado de un sistema.
- Ejemplos:
  - Transferir fondos
  - Abonar cuenta
  - Retirar fondos