

Razonamiento automático

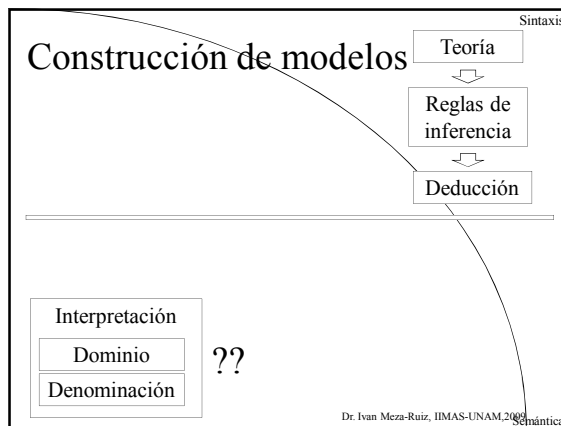
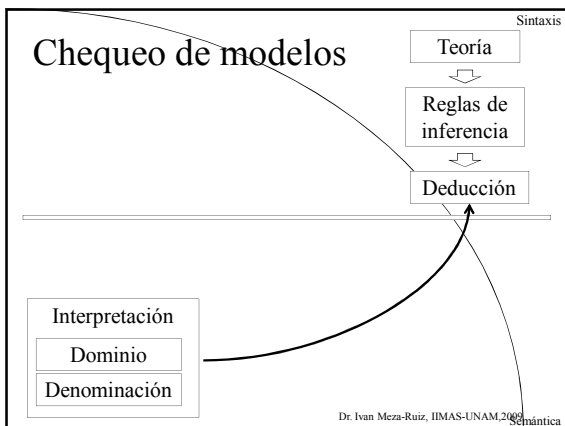
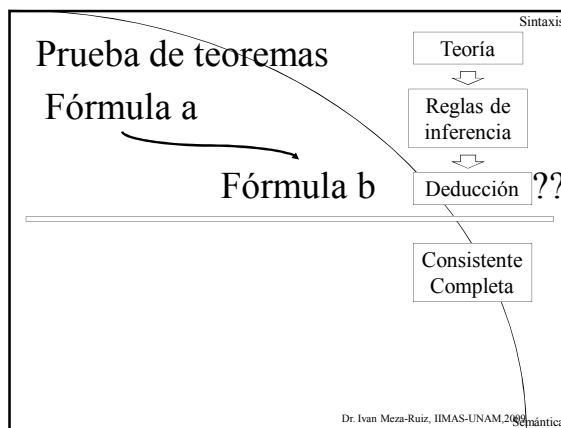
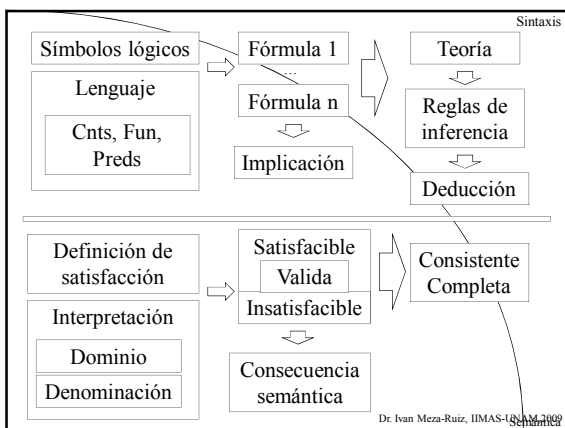
Basado en: Logic in Computer Science,
Hunt & Ryan

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Técnicas

- Prueba de teoremas (Theorem provers)
- Chequeo de modelos (Model checkers)
- Constructores de modelos (Model builders)

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009



Deducción natural

- Un conjunto de reglas de inferencia para lógica proposicional
 - Conjunción
 - Doble negación
 - Implicación
 - Negación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Lógica proposicional

- Sintaxis
 - \neg & \vee \rightarrow \leftrightarrow $()$
 - Variables booleanas
- Propiedades
 - Es completa
 - Es consistente

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Conjunción

$$\frac{\alpha \quad \beta}{\alpha \& \beta}$$

Introducción

$$\frac{\alpha \& \beta}{\alpha}$$

$$\frac{\alpha \& \beta}{\beta}$$

Eliminación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Doble negación

$$\frac{\alpha}{\neg\neg\alpha}$$

Introducción

$$\frac{\neg\neg\alpha}{\alpha}$$

Eliminación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Implicación

$$\frac{\begin{array}{c} \boxed{\alpha} \\ \vdots \\ \boxed{\beta} \end{array}}{\alpha \rightarrow \beta}$$

Introducción

$$\frac{\alpha \quad \alpha \rightarrow \beta}{\beta}$$

Eliminación
Modus ponens

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Modus tollens

$$\frac{\alpha \rightarrow \beta \quad \neg\beta}{\neg\alpha}$$

Eliminación
Modus tollens

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Disyunción

$$\frac{\alpha}{\alpha \vee \beta}$$

$$\frac{\beta}{\alpha \vee \beta}$$

Introducción

$$\alpha \vee \beta$$

$$\begin{array}{c} \alpha \\ \vdots \\ \chi \end{array}$$

$$\begin{array}{c} \beta \\ \vdots \\ \chi \end{array}$$

Eliminación

$$\chi$$

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Contradicción

$$\begin{array}{c} \alpha \\ \vdots \\ \perp \end{array}$$

Introducción

$$\frac{\perp}{\alpha}$$

$$\frac{\alpha \quad \neg \alpha}{\perp}$$

Eliminación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Deducción

1			$p \ \& \ q \ \rightarrow \ r$	Premisa					
	2		p	Asumción					
		3	q	Asumción					
		4	$p \ \& \ q$	$\&i \ 2,3$					
		5	r	$\rightarrow e \ 1,4$					
	6		$q \rightarrow r$	$\rightarrow i \ 3-5$					
7			$p \rightarrow (q \rightarrow r)$	$\rightarrow i \ 2-6$					

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

El reto es...

1			$p \ \& \ q \ \rightarrow \ r$	Premisa					
...							
m			$p \rightarrow (q \rightarrow r)$...					

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

- ### Formas normales
- Permiten evaluar rápidamente la validez de una fórmula:
 - $q \vee a \vee c \vee \neg q$
 - CNF (Conjunctive Normal Form)
 - Literales: átomo o negación
 - CNF formula: conjunción de clausulas formadas por disyunción de literales
 - $L ::= p \mid \neg p$
 - $D ::= L \mid L \vee D$
 - $C ::= D \mid D \ \& \ C$
- Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

- ### De fórmula prop. a CNF
- Eliminar las implicaciones
 - $p \rightarrow q = \neg p \vee q$
 - Transformar a Negation Normal Form
 - $\neg \neg p = p$
 - $\neg(p \ \& \ q) = \neg p \vee \neg q$
 - $\neg(p \vee q) = \neg p \ \& \ \neg q$
- Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

De fórmula prop. a CNF (cont.)

Def CNF(ϕ)

If es_literal(ϕ) return ϕ
 If es_con(ϕ) return CNF(fst(ϕ)) & CNF(snd(ϕ))
 If es_dis(ϕ) return
 DISTR(CNF(fst(ϕ)),CNF(snd(ϕ)))

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

De fórmula prop. a CNF (cont.)

- DISTR usa la equivalencia distributiva para eliminar conjunciones dentro de disyunciones
 - $p1 \& p2 \vee q = p1vq \& p2 \vee q$

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Ejemplo

CNF (NNF (IMPL_FREE ($\neg p \wedge q \rightarrow p \wedge (r \rightarrow q)$)))

IMPL_FREE(ϕ) = \neg IMPL_FREE($\neg p \wedge q$) \vee IMPL_FREE($p \wedge (r \rightarrow q)$)
 = \neg ((IMPL_FREE $\neg p$) \wedge (IMPL_FREE q)) \vee IMPL_FREE($p \wedge (r \rightarrow q)$)
 = \neg (($\neg p$) \wedge IMPL_FREE q) \vee IMPL_FREE($p \wedge (r \rightarrow q)$)
 = \neg ($\neg p \wedge q$) \vee IMPL_FREE($p \wedge (r \rightarrow q)$)
 = \neg ($\neg p \wedge q$) \vee ((IMPL_FREE p) \wedge IMPL_FREE($r \rightarrow q$))
 = \neg ($\neg p \wedge q$) \vee ($p \wedge$ IMPL_FREE($r \rightarrow q$))
 = \neg ($\neg p \wedge q$) \vee ($p \wedge$ (\neg (IMPL_FREE r) \vee (IMPL_FREE q)))
 = \neg ($\neg p \wedge q$) \vee ($p \wedge$ ($\neg r \vee$ (IMPL_FREE q)))
 = \neg ($\neg p \wedge q$) \vee ($p \wedge$ ($\neg r \vee$ (IMPL_FREE q)))
 = \neg ($\neg p \wedge q$) \vee ($p \wedge$ ($\neg r \vee q$)).

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Ejemplo (cont.)

NNF (IMPL_FREE ϕ) = NNF (\neg ($\neg p \wedge q$)) \vee NNF ($p \wedge$ ($\neg r \vee q$))
 = NNF (\neg ($\neg p$) \vee $\neg q$) \vee NNF ($p \wedge$ ($\neg r \vee q$))
 = (NNF (\neg $\neg p$)) \vee (NNF ($\neg q$)) \vee NNF ($p \wedge$ ($\neg r \vee q$))
 = ($p \vee$ (NNF ($\neg q$))) \vee NNF ($p \wedge$ ($\neg r \vee q$))
 = ($p \vee$ $\neg q$) \vee NNF ($p \wedge$ ($\neg r \vee q$))
 = ($p \vee$ $\neg q$) \vee ((NNF p) \wedge (NNF ($\neg r \vee q$)))
 = ($p \vee$ $\neg q$) \vee ($p \wedge$ (NNF ($\neg r$) \vee (NNF ($\neg q$)))
 = ($p \vee$ $\neg q$) \vee ($p \wedge$ ((NNF ($\neg r$)) \vee (NNF q)))
 = ($p \vee$ $\neg q$) \vee ($p \wedge$ ($\neg r \vee$ (NNF q)))
 = ($p \vee$ $\neg q$) \vee ($p \wedge$ ($\neg r \vee q$)).

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Ejemplo (cont. 2)

CNF (NNF (IMPL_FREE ϕ)) = CNF (($p \vee$ $\neg q$) \vee ($p \wedge$ ($\neg r \vee q$)))
 = DISTR (CNF ($p \vee$ $\neg q$), CNF ($p \wedge$ ($\neg r \vee q$)))
 = DISTR ($p \vee$ $\neg q$, CNF ($p \wedge$ ($\neg r \vee q$)))
 = DISTR ($p \vee$ $\neg q$, $p \wedge$ ($\neg r \vee q$))
 = DISTR ($p \vee$ $\neg q$, p) \wedge DISTR ($p \vee$ $\neg q$, $\neg r \vee q$)
 = ($p \vee$ $\neg q \vee p$) \wedge DISTR ($p \vee$ $\neg q$, $\neg r \vee q$)
 = ($p \vee$ $\neg q \vee p$) \wedge ($p \vee$ $\neg q \vee$ $\neg r \vee q$).

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Satisfacible, Válida y Insatisfacible

- Si α es válida es satisfacible
- Si α es satisfacible no es insatisfacible
- Si α es válida entonces $\neg\alpha$ es insatisfacible
- Si $\neg\alpha$ es valida entonces α insatisfacible
- Si $\neg\alpha$ es in satisfacible entonces α es válida

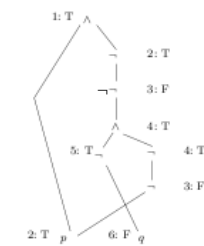
Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

SAT solvers

- Tratan de asignar a las variables de una lógica proposicional valores de falso y verdadero que hagan a la fórmula verdadera
- Es decir si tienen éxito muestran que la fórmula es satisfacible, caso contrario insatisfacibles.

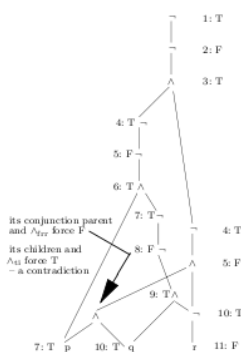
Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Linear solver



$p \ \& \ \neg(\neg q \ \& \ \neg p)$

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009



Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

$\neg(p \ \& \ q)$

- Nuestro método falla para estos casos

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Salidas de este método

- Se encuentra una asignación en todos los nodos: satisfacible
- Se encuentra que una asignación es contradictoria con una previa: insatisfacible
- No todos los nodos tienen asignación:
 - ☹

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Cuantificador universal

$$\frac{\begin{matrix} x_0 \\ \vdots \\ \alpha\{x_0/\tau\} \end{matrix}}{\forall x \alpha}$$

Introducción

$$\frac{\forall x \alpha}{\alpha\{x/\tau\}}$$

Eliminación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Cuantificador existencial

$$\frac{\alpha\{x/\tau\}}{\exists x \alpha}$$

Introducción

$$\frac{\exists x \alpha \quad \begin{matrix} x_0 & \alpha\{x_0/\tau\} \\ \vdots \\ \chi \end{matrix}}{\chi}$$

Eliminación

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Deducción

1			$\exists P(x)$	Premisa	
2			$\forall x \forall y (P(x) \rightarrow Q(y))$	Premisa	
3		y_0			
4	x_0	$P(x_0)$		Asumción	
5		$\forall y (P(x_0) \rightarrow Q(y))$		$\forall x e 2$	
6		$P(x_0) \rightarrow Q(y_0)$		$\forall y e 5$	
7		$Q(y_0)$		$\rightarrow i 6,4$	
8		$Q(y_0)$		$\exists x e 1,4-7$	
7		$\forall y Q(y)$		$\forall y i 3-8$	

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

El reto

1			$\exists P(x)$	Premisa	
2			$\forall x \forall y (P(x) \rightarrow Q(y))$	Premisa	
...			
7			$\forall y Q(y)$...	

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

- ### ¿Dónde estamos?
- FOL es más expresivo
 - Pero, FOL, agrega aspectos de indecidibilidad
- Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

- ### Prover9
- Prover9 es un TP
 - Recibe una teoría y un objetivo y llena la parte de en medio.
 - Todo es manipulación sintáctica
- Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Otra opción

- SAT solvers manipulan una fórmula tratando de aplicar una interpretación.
- TP manipulan una teoría para identificar que sigue de ellas para, generalmente siguen un objetivo.
- Qué tal si tengo una interpretación y checo si la fórmula la satisface.
- Como estamos en FOL la interpretación es más compleja que una tabla de verdad

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Aplicaciones

- Dado un modelo checar que la fórmula se satisfaga
 - SQL
 - Xqueries
- ¿Qué tal modelos de software, estándares de diseño y modelos de ejecución?
 - Se abstraen usando gráficas dirigidas
 - Fórmula que representa ir de un estado bueno a uno malo

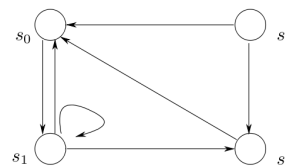
Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Gráficas dirigidas

- Fórmulas para describir propiedades deseables de las gráficas requieren de fórmulas variables en FOL
 - Constantes: Nodos
 - Predicados: Links
 - Fórmula de paths:
 - Caso el nodo es el mismo
 - Caso hay un nodo en medio
 - Caso hay dos nodos en medio
 - etc

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Ejemplo



Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Lógica de Segundo Orden

- $\exists P\alpha$
- $\forall P\alpha$
- LSO permite definir paths para gráficas dirigidas
- ¿Qué hay de Lógica de tercer orden?
 - HOL usadas extensivamente en TP

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Estado del arte TP

- <http://www.cs.miami.edu/~tptp/CASC/22/>
- <http://www.cs.miami.edu/~tptp/>

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Verificación

- Verificar que un modelo cumpla con una especificación (conjunto de propiedades).

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Criterios verificación

- Basados en pruebas: Especificación (fórmula) sigue a sistema (teoría)
- Basados en modelos: Sistema (FSM) satisface a especificación (fórmula)
- Automático: Automático o interactivo?
- Alcance: propiedades o sistemas completos
- Dominio: software o hardware
- Pre vs pos desarrollo

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Chequeo de modelos

- Automático
- Basados en modelos
- Verifica propiedades
- Técnicas
 - Buscar contra ejemplos
 - Partir de la especificación y checar si son válidos

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

¿Qué tan importante es?

- Clarke, Emerson, and Sifakis ganaron el Turing Award 2007
- Busca responder:
 - $M, s \models \alpha$

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Lógica para MC

- Usa lógica temporal: HOL
- Busca responder:
 - $M \models \alpha$
- Se modela el sistema para crear el modelo M
- Se codifica la especificación/propiedades usando HOL
- Se ejecuta el sistema

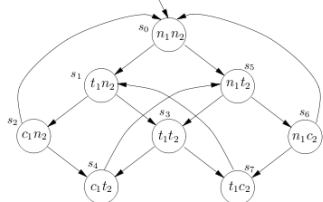
Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Lógica temporal lineal LTL

- El valor de verdad depende del tiempo
- L. propocional más nuevos conectivos para representar
 - Siguiete estado (N)
 - Algún futuro estado (F)
 - Todos los estados (G)
 - Hasta el estado (U)
 - Otros...

Dr. Ivan Meza-Ruiz, IIMAS-UNAM, 2009

Ejemplo



n – Estado no crítico
t – Estado tratando de entrar en estado crítico
c – En estado crítico

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Especificación

- Propiedades
 - Solamente un proceso está en estado crítico
 - Si un proceso necesita entrar en su estado crítico debe lograrlo eventualmente
 - Un proceso puede pedir en estado crítico
 - No existe una secuencia definida para entrar al estado crítico

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Especificación en LTL

- $G\neg(c1 \ \& \ c2)$
- $G(t1 \ \rightarrow \ Fc1)$
- No se puede, no existen
- No se puede, pero complemento sí:
 - $G(c1 \ \rightarrow \ c1 \ W(\neg c1 \ \& \ \neg c1 \ W \ c2))$

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Estado del arte en MC

- <http://nusmv.fbk.eu/>

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Model building

- ¿Qué pasa si no tengo el modelo/interpretación?
- Model building busca crear una interpretación para una especificación dada.

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

Mace4

- Mace4 es un model builder que viene con Prover9

Dr. Ivan Meza-Ruiz, IIMAS-UNAM,2009

En la práctica

- En entendimiento del habla
 - Se tiene un discurso (Teoría y modelo)
 - Se tiene una oración
 - Se obtiene una representación semántica (Fórmulas)
 - Se prueba que formula sigue a la teoría (TP)

Dr. Ivan Meza-Ruiz, HIMAS-UNAM,2009

En la práctica (cont.)

- TP busca satisfacibilidad puede que nunca regrese
 - Se busca que formula regresa modelo para teoria+formula+modelo inicial (MC)
- Se utilizan ambos en paralelos, el primero en regresar nos da una respuesta
- Si ninguno regresa, se considera a la fórmula incoherente

Dr. Ivan Meza-Ruiz, HIMAS-UNAM,2009