Eines Lògiques i Problemes Combinatoris

Repàs de Lògica Proposicional i de Lògica de Primer Ordre

Mateu Villaret

IMA, UdG

13 de febrer del 2010

Resum

Introducció

La **Programació lògica** està basada en:

- Llenguatge Lògic: **Lògica de primer ordre** (Horn)
- Sistema d'Inferència: **Resolució** (SLD)

És un estil **declaratiu**:

- *un* **programa** *serà una transcripció de fets i regles sobre el problema que volem resoldre i que conformaran una teoria*
- *un* **càlcul** *serà una demostració en la teoria del programa*

Per exemple, una teoria sobre els naturals i la relació *suma*, o llistes i la relació *ordenada*, ...

Diferents lògiques

- Lògica proposicional
- **Lògica de predicats (o de primer ordre)**
- Lògica d'ordre superior
- Lògica difusa
- Description Logics (Semantic web)
- Lògica temporal
- ...

Orígens

- Automatitzar la matemàtica, Hilbert (principis XX)
- Fracassa: Gödel, Turing, (30's)
- Algorisme de Resolució/Unificació per a LPO, Robinson (1965)
- PROLOG, Colmerauer, (70's)
- CLP, Colmerauer, Lassez (finals 80's)
- SAT-solvers, SMT, ... (2000's)

Pros i Contres de la programació lògica

Avantatges:

- expressar coneixement independentment de la màquina...
- programes "matemàtics", fàcil raonament sobre les seves propietats
- programes curts, fàcil per al prototipatge
- Constraints

Inconvenients:

- mancances històriques: tipatge, aritmètica, E/S, gràfics, BD ...
- no és pur
- ineficiència en alguns aspectes

Resum

Sintaxi

Fórmula

- tot símbol de predicat $p, q, r, \ldots$ és una fórmula
- si F és una fórmula, llavors $\neg F$ és una fórmula
- si F i G són fórmules, llavors $F \wedge G$ i $F \vee G$ són fórmules
- si F és una fórmula llavors $(\ F\ )$ és una fórmula.
- res més és una fórmula

A part de les **connectives** $\neg$, $\wedge$, i $\vee$, sovint se'n fan servir d'altres com: $\longrightarrow$, $\longleftarrow$, i $\longleftrightarrow$.

Semàntica (i)

Interpretació

Una **interpretació** I sobre $\mathcal{P}$, és una funció

$$I : \mathcal{P} \to \{0, 1\}$$

Avaluació

Definim $eval_I(F)$ com segueix:

- Si F és un símbol de predicat p, $eval_I(F) = I(p)$
- $eval_I(F \wedge G) = 1$ sii $eval_I(F) = 1$ i $eval_I(G) = 1$
- $eval_I(F \vee G) = 1$ sii $eval_I(F) = 1$ o $eval_I(G) = 1$
- $eval_I(\neg(F)) = 1$ sii $eval_I(F) = 0$

Notació: $I \models F$, sii $eval_I(F) = 1$.

Semàntica (ii)

- Una interpretació I és un **model** d'una fórmula F si I satisfà F, és a dir, si $I \models F$.
- Una fórmula F és **satisfactible** si te algun model, per tant, si hi ha alguna interpretació que satisfaci F.
- Una fórmula F és **insatisfactible** (o és una **contradicció**) si no te cap model.
- Una fórmula F és una **tautologia** (o es diu que és **vàlida**) si tota interpretació és model de F.
- Una fórmula F és una **conseqüència lògica** d'una fórmula G si tot model de G també ho és de F. **Implicació lògica**: $G \models F$.
- Una fórmula F és **lògicament equivalent** a una fórmula G si tot model de G també ho és de F i viceversa: $I \models G$ sii $I \models F$.

Semàntica (iii)

Graus de veritat:

F és vàlida sii $\neg F$ és insatisfactible

Vàlides	**Satisfactibles però no vàlides**	**Insatisfactibles**
G	$F \quad \neg F$	$\neg G$

Taules de Veritat

$eval_I(p)$	$eval_I(q)$	$eval_I(\neg p)$	$eval_I(p \wedge q)$	$eval_I(p \vee q)$
1	1	0	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	0

Amb taules de veritat podem demostrar implicacions lògiques, satisfactibilitat de fórmules, contradiccions, tautologies, ...

Equivalències lògiques

$F \wedge F (\vee)$	$\equiv F \quad (\vee)$	idempotència de $\wedge$ (i $\vee$)
$F \wedge G$	$\equiv G \wedge F \quad (\vee)$	commutativitat de $\wedge$ (i $\vee$)
$F \wedge (G \wedge H)$	$\equiv (F \wedge G) \wedge H$	associativitat de $\wedge$
$F \vee (G \vee H)$	$\equiv (F \vee G) \vee H$	associativitat de $\vee$
$(F \wedge G) \vee H$	$\equiv (F \vee H) \wedge (G \vee H)$	distributivitat 1
$(F \vee G) \wedge H$	$\equiv (F \wedge H) \vee (G \wedge H)$	distributivitat 2
$F \wedge (F \vee G)$	$\equiv F$	absorció 1
$F \vee (F \wedge G)$	$\equiv F$	absorció 2
$\neg(F \wedge G)$	$\equiv \neg F \vee \neg G$	De Morgan 1
$\neg(F \vee G)$	$\equiv \neg F \wedge \neg G$	De Morgan 2
$\neg\neg F$	$\equiv F$	doble negació

Regles d'inferència (i)

En *teoria de la demostració* el que es pretén és disposar d'un mecanisme sintàctic que ens permeti, mitjançant les **regles de deducció (o d'inferència)**, obtenir una fórmula (**conclusió**) a partir d'altres (**premisses**).

$$\{F_1, \ldots, F_n\} \vdash_R F_0$$

A les fórmules de l'esquerra les anomenarem **axiomes** i a les fórmules que es poden obtenir a la banda dreta les anomenarem **teoremes**.

Una **derivació** o **demostració** és a una seqüència de fórmules obtingudes a partir dels axiomes inicials, els axiomes lògics o a partir d'aplicacions de les regles d'inferència.

Regles d'inferència (ii)

Algunes regles d'inferència

- MP:
$$\{A, A \to B\} \vdash_{MP} B$$
- MT:
$$\{\neg A, B \to A\} \vdash_{MT} \neg B$$
- MM:
$$\{A, B \to A\} \vdash_{MM} B$$

Quines de les anteriors regles són "*correctes*"?

Regles d'inferència (iii)

Solidesa

Una regla R és **sòlida** quan:

$$\textit{si } \{F_1, \ldots, F_n\} \vdash_R F_0 \textit{ llavors } \{F_1, \ldots, F_n\} \models F_0$$

Completesa

Un sistema d'inferència[a] R és **complet** quan

$$\textit{si } \{F_1, \ldots, F_n\} \models F_0 \textit{ llavors } \{F_1, \ldots, F_n\} \vdash_R F_0$$

[a] Conjunt de regles + estratègia d'utilització.

En general ens interessarà un sistema d'inferència complet basat en regles sòlides.

Resolució (i)

Clàusules

- Un **literal** és o bé un símbol de predicat o bé un símbol de predicat negat: p o $\neg p$.
- Una **clàusula** és una disjunció de literals: $\neg p_1 \vee \ldots \vee \neg p_i \vee p_{i+1} \vee \ldots \vee p_n$
- Una fórmula està en **forma normal conjuntiva (CNF)** si és una conjunció de clàusules:

$$(l_1^1 \vee l_2^1 \vee \cdots \vee l_{k_1}^1) \wedge \ldots \wedge (l_1^n \vee l_2^n \vee \cdots \vee l_{k_n}^n)$$

  es pot veure també com un conjunt de clàusules.
- Les clàusules també es poden veure com un conjunt, però de literals. La **clàusula buida** $\square$ és una clàusula insatisfactible especial.

Resolució (ii)

Tota fórmula té una corresponent CNF:

1. passar a fórmula escrita només per $\vee, \wedge, \neg$
2. passar les $\neg$ fins als símbols de predicats
3. aplicar distributivitat

Compte, la distributibitat pot fer "explotar" el tamany de les fórmules...

Resolució (iii)

Resolució

Sigui p un símbol proposicional i C i D clàusules, definim la regla d'inferència **Resolució** com:

$$\{p \vee C, \quad \neg p \vee D\} \vdash_{Res} \{C \vee D\}$$

Habitualment es representa així:

$$\frac{p \vee C \qquad \neg p \vee D}{C \vee D}$$

Resolució (iv)

Completesa refutacional

Una regla de deducció R sobre clàusules, és **refutacionalment completa** si, per a tot conjunt insatisfactible de clàusules S, la clàusula buida apareix a la clausura sota R de S.

- La resolució[1] és refutacionalment completa, per tant

$$\text{si } S \text{ és insatisfactible, llavors } \Box \in Res^*(S)$$

- Però com ens ho farem per demostrar amb resolució:

$$\models \ (p \rightarrow (q \rightarrow p)) \qquad ?$$

- i per demostrar: $\{A_1, \ldots, A_n\} \models F \qquad ?$

[1] $Res^*(S)$ és resolució sistemàtica, és a dir, fer resolució de "tots amb tots", afegir-hi les clàusules resultants i iterar fins a trobar el punt fix.

Resolució (v)

Tenim que:$\{A_1, \ldots, A_n\} \models F$ sii $\{A_1, \ldots, A_{n-1}\} \models A_n \rightarrow F$ passant totes les premisses a l'altre costat, obtenim:

$$\models A_1 \rightarrow (A_2 \ldots \rightarrow (A_n \rightarrow F) \ldots)$$

i com que: $A \rightarrow (B \rightarrow C) \equiv (A \wedge B) \rightarrow C$, podem escriure:

$$\models (A_1 \wedge A_2 \wedge \ldots \wedge A_n) \rightarrow F$$

comprovem que la fórmula de dalt negada és insatisfactible:

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge \neg F) \models \Box$$

Com que la resolució és refutacionalment completa:

$$\{A_1, \ldots, A_n\} \models F \text{ sii } \{A_1, \ldots, A_n, \neg F\} \vdash_{Res} \Box$$

Estratègies de Resolució

Resolució sistemàtica

$$
\begin{array}{lcll}
Res^0(S) & = & S & \\
Res^1(S) & = & S \cup & \{ \text{ resolents de cada parell possible de clàusules de } S \} \\
\dots & & & \\
Res^{n+1}(S) & = & Res^n(S) \cup & \{ \text{ resolents possibles de cada parell de clàusules de } Res^n(S) \}
\end{array}
$$

La resolució sistemàtica acaba: $\exists k.\ Res^k(S) = Res^{k+1}(S)$.

Millores: obtenir clàusules sense literals repetits, eliminació de tautologies, eliminació de repetides, eliminar subsumides: si tenim $(p \vee q) \wedge (p \vee q \vee r)$ ens quedem amb $(p \vee q)$.

Clàusules de Horn (i)

Clàusules de Horn

Una clàusula és de **Horn** si te com a molt un literal positiu.

- Habitualment, els programes lògics estan escrits amb clàusules de Horn:
  - Fets: un sol literal positiu.
  - Regles: una clàusula amb un literal positiu i algun de negatiu.
  - Queries: una clàusula amb només literals negatius.
- **Resolució Unitària** és la que en cada pas de resolució, una de les premises és sempre una clàusula unitaria positiva. Aquesta estratègia fa obtenir resolents més petits...

Clàusules de Horn (ii)

TEOREMA: La resolució unitària és refutacionalment completa per a clàusules de Horn.

DEMOSTRACIÓ (sketch):

1. $S = Res^*(S_0)$ on S_0 són de Horn. Construirem una I tal que si $\square \notin S$ llavors $I \models S$. Definim $I(p) = 1$ sii $p \in S$.
2. Red. Absurd. Per a veure que si $\square \notin S$ llavors $I \models S$, suposarem $I \not\models S$ i trobarem contradicció.
3. Sigui $C \in S$ la més petita tal que $I \not\models C$.
4. $C = \neg q \vee C'$, però $I(q) = 1$ i per tant podem fer resolució i tindrem $C' \in S$ i $I \not\models C'$ contradint que C era la més petita...

Resum

El preu de la potència

Sobre l'expressivitat

TEORIA: *Tenim una classe amb el professor, la maria i en pere. La maria coneix a tothom. El professor coneix a tothom. En pere coneix a algú si la maria també el coneix.*
PREGUNTA: *En pere es coneix?*

- Guany expressiu, gràcies a: $\exists$, $\forall$, $\mathcal{X}$, permet parlar de relacions entre entitats no necessàriament finites.
  - afirmar l'existència d'objectes que satisfan cert predicats
  - descriure propietats globals, universals.
- Pèrdua de decidibilitat en les qüestions lògiques més interessants.
- De totes maneres tindrem "semi-decidibilitat".

Sintaxi (i)

Disposem de:

- un conjunt de **símbols de funció** $\mathcal{F} = f, g, h, \ldots, a, b, \ldots, successor, zero$... amb una **aritat**
- un conjunt de **símbols de variable** $\mathcal{X} = X, Y, Z, \ldots$

Terme: $\mathcal{T}(\mathcal{F}, \mathcal{X})$:

$$\begin{array}{lll} T & :: & f(T_1, \ldots, T_n) \\ & \mid & X \end{array}$$

on $f \in \mathcal{F}$,f té aritat n (f és n-ària)
$T_1, \ldots, T_n$ són termes i $X \in \mathcal{X}$

Sintaxi (i)

Disposem de:

- un conjunt de **símbols de funció** $\mathcal{F} = f, g, h, \ldots, a, b, \ldots, successor, zero\ldots$ amb una **aritat**
- un conjunt de **símbols de variable** $\mathcal{X} = X, Y, Z, \ldots$

Terme: $\mathcal{T}(\mathcal{F}, \mathcal{X})$:

$$\begin{array}{lll} T & :: & f(T_1, \ldots, T_n) \quad \text{on } f \in \mathcal{F}, f \text{ té aritat } n \text{ } (f \text{ és } n\text{-ària}) \\ & | & X \qquad\qquad\qquad\quad T_1, \ldots, T_n \text{ són termes i } X \in \mathcal{X} \end{array}$$

Sigui $\mathcal{F} = \{f, g, a, b\}$ i $\mathcal{X} = \{X, Y\}$ on f té aritat 1, g aritat 2, a, b aritat 0.

$$\begin{array}{l|l} 1 & a \quad b \quad X \quad Y \\ 2 & f(a) \quad f(b) \quad f(X) \quad f(Y) \\ 3 & g(a, a) \quad g(a, X) \quad g(X, Y) \quad f(f(a)) \quad \ldots \\ 4 & g(f(a), X) \quad f(g(a, X)) \quad f(g(Y, b)) \quad g(X, f(b)) \quad \ldots \\ 5 & g(g(a, b), X) \quad g(f(f(a)), b) \quad \ldots \end{array}$$

Sintaxi (ii)

Disposem també

- d'un conjunt de **símbols de predicat (relacions)**
  $\mathcal{P} = \mathtt{p}, \mathtt{q}, \mathtt{r}, \ldots, \mathtt{esparell}, \mathtt{home}, \ldots$ amb una **aritat**

Àtom: $\mathtt{p}(T_1, \ldots, T_n)$ si $\mathtt{p} \in \mathcal{P}$, n-àri i $T_1, \ldots, T_n$ són termes

Sintaxi (ii)

Disposem també

- d'un conjunt de **símbols de predicat (relacions)** $\mathcal{P} = \mathtt{p}, \mathtt{q}, \mathtt{r}, \ldots, \mathtt{esparell}, \mathtt{home}, \ldots$ amb una **aritat**

Àtom: $\mathtt{p}(T_1, \ldots, T_n)$ si $\mathtt{p} \in \mathcal{P}$, n-àri i $T_1, \ldots, T_n$ són termes

Sigui $\mathcal{P} = \{\mathtt{suma}, \mathtt{esparell}\}, \mathcal{F} = \{\mathit{succ}, \mathit{zero}\}$ i $\mathcal{X} = \{X, Y\}$ on $\mathtt{esparell}$ i succ tenen aritat 1, $\mathtt{suma}$ aritat 3 i zero aritat 0.

$\mathtt{esparell}(\mathit{zero})$ $\mathtt{esparell}(\mathit{succ}(\mathit{succ}(X)))$
$\mathtt{suma}(\mathit{zero}, \mathit{succ}(\mathit{zero}), \mathit{succ}(\mathit{zero}))$ $\mathtt{suma}(X, \mathit{zero}, \mathit{succ}(\mathit{zero}))$
$\mathtt{suma}(\mathit{zero}, \mathit{succ}(\mathit{zero}), \mathit{zero})$

Sintaxi (iii)

Fórmules:

- tot àtom és una fórmula,
- si F i G són fórmules, llavors $\neg(F), (F \wedge G)$ i $(F \vee G)$ són fórmules,
- si F és una fórmula, llavors $\forall X\ (F)$ i $\exists X\ (F)$, són fórmules si X apareix lliure a F,
- res més és una fórmula.

Sintaxi (iii)

Fórmules:

- tot àtom és una fórmula,
- si F i G són fórmules, llavors $\neg(F), (F \wedge G)$ i $(F \vee G)$ són fórmules,
- si F és una fórmula, llavors $\forall X\ (F)$ i $\exists X\ (F)$, són fórmules si X apareix lliure a F,
- res més és una fórmula.

Sigui $\mathcal{P} = \{\mathtt{suma}, \mathtt{esparell}\}, \mathcal{F} = \{succ, zero\}$ i $\mathcal{X} = \{X, Y\}$ on $\mathtt{esparell}$ i *succ* tenen aritat 1, $\mathtt{suma}$ aritat 3 i *zero* aritat 0.

$$\mathtt{esparell}(succ(succ(zero))) \quad \forall X.\mathtt{esparell}(X)$$
$$\exists X\ \exists Y \mathtt{suma}(X, Y, succ(zero))$$

Semàntica (i)

Interpretació, I:

- Un conjunt no buit D, anomenat **domini** de I,
- per cada símbol $f^n \in \mathcal{F}$, una funció $f_I : D \times \overset{n}{\ldots} \times D \rightarrow D$,
- per cada símbol $\mathrm{p}^n \in \mathcal{P}$, una funció $p_I : D \times \overset{n}{\ldots} \times D \rightarrow \{0, 1\}$.

Semàntica (i)

Interpretació, I:

- Un conjunt no buit D, anomenat **domini** de I,
- per cada símbol $f^n \in \mathcal{F}$, una funció $f_I : D \times \overset{n}{\ldots} \times D \to D$,
- per cada símbol $\mathrm{p}^n \in \mathcal{P}$, una funció $p_I : D \times \overset{n}{\ldots} \times D \to \{0, 1\}$.

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ i sigui $D = \{*, \sharp\}$ on s, q tenen aritat 1 i a, b aritat 0.

Podem donar diverses interpretacions, p.ex:

$$
\begin{array}{ll}
a_I = * & \\
b_I = \sharp & \\
s_I(\sharp) = * & s_I(*) = \sharp \\
q_I(*) = 1 & q_I(\sharp) = 0
\end{array}
$$

Semàntica (ii)

- Donada I, una **assignació** α és una funció $\alpha : \mathcal{X} \rightarrow D_I$. $\alpha[X \rightarrow d]$ és una assignació idèntica en tot a α menys en que associa d a X.
- **Avaluació d'un terme** t segons una interpretació I i una assignació α:

$$eval_I^\alpha(t) :: Termes \rightarrow D$$

  - si $X \in \mathcal{X}$ llavors $eval_I^\alpha(X) = \alpha(X)$,
  - si $f \in \mathcal{F}$ llavors $eval_I^\alpha(f(t_1, \ldots, t_n)) = f_I(eval_I^\alpha(t_1), \ldots, eval_I^\alpha(t_n))$
- **Avaluació d'una fórmula** F segons una interpretació I:

$$eval_I^\alpha(F) :: Formules \rightarrow \{0, 1\}$$

  - si $\mathrm{p}^n \in \mathcal{P}$ llavors $eval_I^\alpha(\mathrm{p}(t_1, \ldots, t_n)) = p_I(eval_I^\alpha(t_1), \ldots, eval_I^\alpha(t_n))$
    ...

Semàntica (iii)

- ...
  - $eval_I^\alpha(F \wedge G) = 1$ sii $eval_I^\alpha(F) = 1$ i $eval_I^\alpha(G) = 1$
  - $eval_I^\alpha(F \vee G) = 1$ sii $eval_I^\alpha(F) = 1$ o $eval_I^\alpha(G) = 1$
  - $eval_I^\alpha(\neg(F)) = 1$ sii $eval_I^\alpha(F) = 0$
  - $eval_I^\alpha(\forall X\ F) = 1$ sii $eval_I^{\alpha[X \to d]}(F) = 1$ per a tot $d \in D$
  - $eval_I^\alpha(\exists X\ F) = 1$ sii $eval_I^{\alpha[X \to d]}(F) = 1$ per algun $d \in D$

Normalment treballarem sense variables “lliures” per tant no es tindran en conte les assignacions.
Així, I **satisfà** F, $I \models F$, si i només si $eval_I(F) = 1$.
Les nocions semàntiques de lògica proposicional s'hereden.
Amb les propietats computacionals no passarà el mateix...

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^\alpha(\forall X\ \mathrm{q}(s(X)))}$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))}$$

$$\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))}$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))}$$

$$\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))}$$

$$q_I(\underline{eval_I^{\alpha[X=*]}(s(X))}) \wedge q_I(\underline{eval_I^{\alpha[X=\sharp]}(s(X))})$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))}$$
$$\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))}$$
$$q_I(\underline{eval_I^{\alpha[X=*]}(s(X))}) \wedge q_I(\underline{eval_I^{\alpha[X=\sharp]}(s(X))})$$
$$q_I(s_I(\underline{eval_I^{\alpha[X=*]}(X)})) \wedge q_I(s_I(\underline{eval_I^{\alpha[X=\sharp]}(X)}))$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))}$$
$$\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))}$$
$$q_I(\underline{eval_I^{\alpha[X=*]}(s(X))}) \wedge q_I(\underline{eval_I^{\alpha[X=\sharp]}(s(X))})$$
$$q_I(s_I(\underline{eval_I^{\alpha[X=*]}(X)})) \wedge q_I(s_I(\underline{eval_I^{\alpha[X=\sharp]}(X)}))$$
$$q_I(\underline{s_I(*)}) \wedge q_I(\underline{s_I(\sharp)})$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *, b_I = \sharp, s_I(\sharp) = *, s_I(*) = \sharp, q_I(*) = 1, q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))}$$
$$\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))}$$
$$q_I(\underline{eval_I^{\alpha[X=*]}(s(X))}) \wedge q_I(\underline{eval_I^{\alpha[X=\sharp]}(s(X))})$$
$$q_I(s_I(\underline{eval_I^{\alpha[X=*]}(X)})) \wedge q_I(s_I(\underline{eval_I^{\alpha[X=\sharp]}(X)}))$$
$$q_I(\underline{s_I(*)}) \wedge q_I(\underline{s_I(\sharp)})$$
$$\underline{q_I(\sharp)} \wedge \underline{q_I(*)}$$

Semàntica (iii)

Sigui $\mathcal{P} = \{\mathrm{q}\}$ i $\mathcal{F} = \{s, a, b\}$ on s, q tenen aritat 1 i a, b aritat 0. Sigui la interpretació I tal que, $D = \{*, \sharp\}$ i $a_I = *$, $b_I = \sharp$, $s_I(\sharp) = *$, $s_I(*) = \sharp$, $q_I(*) = 1$, $q_I(\sharp) = 0$ i sigui α una assignació qualsevol.

Avaluem $\forall X\ \mathrm{q}(s(X))$:

$$\begin{array}{c}
\underline{eval_I^{\alpha}(\forall X\ \mathrm{q}(s(X)))} \\
\underline{eval_I^{\alpha[X=*]}(\mathrm{q}(s(X)))} \wedge \underline{eval_I^{\alpha[X=\sharp]}(\mathrm{q}(s(X)))} \\
q_I(\underline{eval_I^{\alpha[X=*]}(s(X))}) \wedge q_I(\underline{eval_I^{\alpha[X=\sharp]}(s(X))}) \\
q_I(s_I(\underline{eval_I^{\alpha[X=*]}(X)})) \wedge q_I(s_I(\underline{eval_I^{\alpha[X=\sharp]}(X)})) \\
q_I(\underline{s_I(*)}) \wedge q_I(\underline{s_I(\sharp)}) \\
\underline{q_I(\sharp)} \wedge \underline{q_I(*)} \\
\underline{0 \wedge 1} \\
0
\end{array}$$

Més equivalències lògiques

$$\begin{array}{lll}
\neg\forall X\ H(X) & \equiv \exists X\ \neg H(X) & \text{De Morgan 3} \\
\neg\exists X\ H(X) & \equiv \forall X\ \neg H(X) & \text{De Morgan 4} \\
(\forall X\ F \wedge G) & \equiv \forall X\ (F \wedge G) & \text{si } X \text{ no apareix a } G \\
(\forall X\ F \wedge \forall X\ G) & \equiv \forall X\ (F \wedge G) & \\
(\exists X\ F \vee \exists X\ G) & \equiv \exists X\ (F \vee G) &
\end{array}$$

Compte amb les següents *no-equivalències*:

$$(\forall X\ F \vee \forall X\ G) \not\equiv \forall X\ (F \vee G)$$

$$(\exists X\ F \wedge \exists X\ G) \not\equiv \exists X\ (F \wedge G)$$

Conseqüència lògica

- Què podem dir de la satisfactibilitat de $\neg \mathrm{p}(a) \wedge \mathrm{p}(b)$.
- Amb un nombre infinit de possibles termes...

$$\left\{ \begin{array}{l} \forall X \ \mathtt{sum}(X, 0, X), \\ (\forall X \forall Y \forall Z \ \mathtt{sum}(X, Y, Z) \rightarrow \mathtt{sum}(X, s(Y), s(Z))) \end{array} \right\}$$

$$\models^{?}$$

$$\mathtt{sum}(s(0), s(0), s(s(0)))$$

Què podem dir de la implicació lògica?

- Com comprovar que **tot** model de les premises ho és de la conclusió?
- Quants models poden tenir les premises?
- Ens serveix: negar la conclusió i intentar demostrar insatisfactibilitat?

Pas a CNF (i)

La transformació d'una fórmula F a un conjunt de clàusules S preserva satisfactibilitat (equivalència no):

- F és satisfactible si i només si ho és S
- $S \models F$ (però no necessàriament $F \models S$)

Passos:

1. Eliminar els símbols condicionals com $\rightarrow$.
2. Moure les negacions cap als símbols de predicat.
3. Eliminar els $\exists$ (**Skolemització**): Tota occurrència d'X lligada per $\exists X$ es substitueix per $f_X(Y_1, \ldots, Y_n)$, on Y_i són les variables quantificades universalment per sobre de l'$\exists X$, a més f_X és nou per a cada lligam.
4. Universals cap enfora evitant conflictes de noms de variables.
5. Distribució de $\wedge$ sobre $\vee$.

Pas a CNF (ii)

Obtenim:

$$\forall X_1 \ldots \forall X_m (l_1^1 \vee l_2^1 \vee \cdots \vee l_{k_1}^1) \wedge \ldots \wedge (l_1^n \vee l_2^n \vee \cdots \vee l_{k_n}^n)$$

Pas a CNF

$$\forall X \; (\; \forall Y \; (\mathrm{p}(Y) \rightarrow \mathrm{q}(X, Y)) \; \rightarrow \; \exists Y \; \mathrm{q}(Y, X) \;)$$
$$\forall X \; (\; \neg\forall Y \; (\neg\mathrm{p}(Y) \vee \mathrm{q}(X, Y)) \; \vee \; \exists Y \; \mathrm{q}(Y, X) \;)$$
$$\forall X \; (\; \exists Y \; \neg(\neg\mathrm{p}(Y) \vee \mathrm{q}(X, Y)) \; \vee \; \exists Y \; \mathrm{q}(Y, X) \;)$$
$$\forall X \; (\; \exists Y \; (\mathrm{p}(Y) \wedge \neg\mathrm{q}(X, Y)) \; \vee \; \exists Y \; \mathrm{q}(Y, X) \;)$$
$$\forall X \; (\; \exists Y \; (\mathrm{p}(Y) \wedge \neg\mathrm{q}(X, Y)) \; \vee \; \exists Z \; \mathrm{q}(Z, X) \;)$$
$$\forall X \; (\; (\mathrm{p}(f_Y(X)) \wedge \neg\mathrm{q}(X, f_Y(X))) \; \vee \; \mathrm{q}(f_Z(X), X) \;)$$
$$(\; (\mathrm{p}(f_Y(X)) \vee \mathrm{q}(f_Z(X), X)) \wedge (\neg\mathrm{q}(X, f_Y(X)) \; \vee \; \mathrm{q}(f_Z(X), X)) \;)$$

Interpretació d'Herbrand (i)

- **Domini d'Herbrand (o Univers d'Herbrand)**. Donat un conjunt de símbols $\mathcal{F}$, l'univers o domini d'Herbrand H és el conjunt de tots els **termes ground** de $\mathcal{F}$: $\mathcal{T}(\mathcal{F}, \emptyset)$.

Per a $\mathcal{F} = \{s, 0\}$:

$$H = \{0, s(0), s(s(0)), s(s(s(0))), s(s(s(s(0)))), \ldots\}$$

Interpretació d'Herbrand (i)

- **Domini d'Herbrand (o Univers d'Herbrand)**. Donat un conjunt de símbols $\mathcal{F}$, l'univers o domini d'Herbrand H és el conjunt de tots els **termes ground** de $\mathcal{F}$: $\mathcal{T}(\mathcal{F}, \emptyset)$.

Per a $\mathcal{F} = \{s, 0\}$:

$$H = \{0, s(0), s(s(0)), s(s(s(0))), s(s(s(s(0)))), \dots\}$$

- **Base d'Herbrand**. Donat un conjunt de símbols $\mathcal{F}$, i un conjunt de símbols de predicats $\mathcal{P}$, la base d'Herbrand B és el conjunt de tots els **àtoms ground** fets amb $\mathcal{P}$ i $\mathcal{F}$.

Per a $\mathcal{F} = \{s, 0\}$ i $\mathcal{P} = \{\mathtt{suma}\}$:

$$B = \left\{ \begin{array}{lll} \mathtt{suma}(0,0,0) & \mathtt{suma}(s(0),0,0) & \mathtt{suma}(0,s(0),0) \\ \mathtt{suma}(0,0,s(0)) & \mathtt{suma}(s(0),s(0),0) & \mathtt{suma}(0,s(0),s(0)) \\ \dots & & \end{array} \right.$$

Interpretació d'Herbrand (ii)

- **Interpretació d'Herbrand**. Donada una teoria, una iterpretació d'Herbrand és tota aquella interpretació que te com a domini el domini d'Herbrand de manera que l'avaluació d'un terme és ell mateix.

Per a la teoria de la suma:

Una **interpretació d'Herbrand** que a més seria model podria ser:
Per als termes:

$$\{0_I = 0, s_I(0) = s(0), s_I(s(0)) = s(s(0)), \dots\}$$

Per al predicat $\mathtt{sum}(\_,\_,\_)$:

$$\left\{ \begin{array}{ll} sum_I(0,0,0) = 1, & sum_I(0,0,s(0)) = 0 \\ sum_I(s(0),0,0) = 0, & sum_I(s(0),0,s(0)) = 1 \\ sum_I(0,s(0),0) = 0, & sum_I(0,s(0),s(0)) = 1 \\ \dots & \end{array} \right\}$$

Procediment d'Herbrand (i)

TEOREMA

Tota fórmula en CNF (Skolemitzada) és satisfactible si i només si té un model d'Herbrand.

TEOREMA

Una teoria és satisfactible si i només si tot subconjunt finit és satisfactible.

Gràcies a aquests teoremes i a que la resolució proposicional és refutacionalment completa, es poden definir els **procediments d'Herbrand** basats en la idea de treballar amb les instanciacions ground de les fórmules i la resolució proposicional.

Procediment d'Herbrand (ii)

Atès que sabem com trobar la clàusula buida en lògica proposicional, la intenció és la següent:

- Passar la nostra teoria a forma clausal.
- Fer la instanciació de les clàusules. (Obtenir totes les clàusules on substituïm les variables pels valors, d'acord amb el quantificador).
- Buscar la clàusula buida...

Teorema d'Herbrand: Dels teoremes anteriors + Completesa Resolució Proposicional

Un conjunt de clàusules C en CNF és insatisfactible
si i només si
algun subconjunt **finit** de la instanciació ground
de C és insatisfactible

Procediment d'Herbrand (iii)

Per a completar el procediment i poder demostrar la implicació lògica $P \models^? A$ en primer ordre, necessitem ser capaços d'enumerar els possibles subconjunts finits de la **instanciació Ground**.

$$Ground(P \cup \{\neg A\}) = \{g_1, g_2, \ldots\}$$

Així, si $P \models A$, ha d'existir una k tal que de $\{g_1, g_2, \ldots, g_k\}$ en poguem trobar la clàusula buida.

Procediment d'Herbrand (iv)

De la teoria de la suma s'en deriva $\mathtt{suma}(s(0), s(0), s(s(0)))$?

Al passar a ground, podem passar a proposicional...

Primer Ordre	Proposicional
suma(0,0,0)	s0i0es0
suma(s(0),0,s(0))	s1i0es1
...	...
¬ suma(0,0,0)∨ suma(0,s(0),s(0))	¬ s0i0es0 ∨ s0i1es1
¬ suma(s(0),0,s(0))∨ suma(s(0),s(0),s(s(0)))	¬ s1i0es1 ∨ s1i1es2
...	...
¬suma(s(0),s(0),s(s(0)))	¬s1i1es2

Procediment d'Herbrand (v)

- L'anterior procediment és extremadament ineficient!!!
- Usarem resolució de primer ordre que és sòlida i refutacionalment completa:
  - cal passar a CNF en lògica de primer ordre
  - cal definir una noció de resolució en per a la lògica de primer ordre
  - cal una eina per a la instanciació universal: unificació

Com definir una resolució per a la lògica de primer ordre?

Per fer la següent resolució de primer ordre passarem a proposicional.

$$\frac{\mathrm{p}(t) \vee Q \quad \neg\mathrm{p}(t') \vee R}{???}$$

Regla de deducció sòlida: instanciació universal

$$\forall X \; W(X) \vdash \forall X_0 \ldots \forall X_n \; \sigma(W(X))$$

on $\sigma = \{X \mapsto s\}$ i $X_0, \ldots, X_n$ són variables de s.

Per tant instanciarem universalment les dues clàusules amb una substitució σ que iguala (**unifica**) els literals que volem i farem com en resolució proposicional:

$$\frac{\mathrm{p}(r) \vee \sigma(Q) \qquad \neg\mathrm{p}(r) \vee \sigma(R)}{\sigma(Q) \vee \sigma(R)}$$

on $\sigma(\mathrm{p}(t)) = \sigma(\mathrm{p}(t')) = \mathrm{p}(r)$

Unificació (i)

- La **substitució**: $\sigma = \{X_1 \mapsto t_1, \ldots, X_n \mapsto t_n\}$ (o $\{t_1/X_1, \ldots, t_n/X_n\}$) on $X_i \neq X_j$ i les X_i són el domini $Dom(\sigma)$ de la substitució.
- L'**aplicació** de σ a t consisteix en substituir simultàniament cada ocurrència d'X_i a t per t_i. El resultat de la substitució es denota com a $\sigma(t)$ (o $t\sigma$). Es pot extendre naturalment a literals i clàusules.

  La **composició** de substitucions σ i σ' es denota com $\sigma' \circ \sigma$ i és aquella substitució tal que $\sigma' \circ \sigma(t) = \sigma'(\sigma(t)) = t\sigma\sigma'$.

Sigui $\sigma = \{X \mapsto f(a, Y), Y \mapsto Z\}$ i $\sigma' = \{Y \mapsto b, Z \mapsto c\}$ sigui $t = f(X, f(Y, Z))$

$$\begin{aligned}
\sigma(t) &= f(f(a, Y), f(Z, Z)) \\
\sigma'(t) &= f(X, f(b, c)) \\
\sigma' \circ \sigma(t) &= f(f(a, b), f(c, c)) \\
\sigma \circ \sigma'(t) &= f(f(a, Y), f(b, c))
\end{aligned}$$

Unificació (ii)

- **Unificació** és, donats dos termes $s \stackrel{?}{=} t$, decidir si existeix alguna substitucion (**unificador**) σ tal que $\sigma(s) = \sigma(t)$.
- La unificabilitat es pot decidir en temps polinòmic.
- Donada una equació solucionable $s \stackrel{?}{=} t$, l'**unificador més general** ($\sigma = mgu(s,t)$) és aquell tal que qualsevol altre unificador σ' d's i t, és una particularització de σ, és a dir, que existeix una substitució ρ tal que: $\sigma' = \rho \circ \sigma$.
- Generalitzem els conceptes a problemes d'unificació: conjunts d'equacions $\{s_1 \stackrel{?}{=} t_1, \ldots, s_n \stackrel{?}{=} t_n\}$.

Unificació (iii)

Procediment d'unificació, (si unifica dóna el mgu):

1. $P \cup \{t \stackrel{?}{=} t\} \Longrightarrow P$
2. $P \cup \{f(t_1, \ldots, t_n) \stackrel{?}{=} f(s_1, \ldots, s_n)\} \Longrightarrow P \bigcup_{1 \leq i \leq n} \{t_i \stackrel{?}{=} s_i\}$
3. $P \cup \{f(t_1, \ldots, t_n) \stackrel{?}{=} g(s_1, \ldots, s_n)\} \Longrightarrow$ **CLASH** $(f \neq g)$
4. $P \cup \{X \stackrel{?}{=} t\} \Longrightarrow P\{X \mapsto t\} \cup \{X \stackrel{?}{=} t\}$ si $X \in vars(P)$ i $X \notin vars(t)$. Si $t = Y$ i X o Y no apareixen a la resta del problema, no aplicarem la regla.
5. $P \cup \{X \stackrel{?}{=} t\} \Longrightarrow$ **OCCUR-CHECK** (si $X \in vars(t)$ i $X \neq t$)

El procés acaba quan produïm un OCCUR-CHECK o un CLASH, no unificables; o quan no es poden aplicar més regles i llavors l'unificador es pot obtenir del que ha quedat que naturalment tindrà la forma:

$$\{X_1 \stackrel{?}{=} t_1, \ldots, X_m \stackrel{?}{=} t_m\}$$

on les variables són resoltes...

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X, g(X)), h(Y), V) \stackrel{?}{=} \mathrm{p}(Y, h(V), f(g(Z), W)))}\}$$

Unificació (iv)

Unifiquem:

$\{\underline{\mathrm{p}(f(X, g(X)), h(Y), V) \stackrel{?}{=} \mathrm{p}(Y, h(V), f(g(Z), W)))}\}$

$\{\underline{f(X, g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z), W)\}$

Unificació (iv)

Unifiquem:

$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W))}\}$

$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$

$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W)))}\}$$
$$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} V}, V \stackrel{?}{=} f(g(Z),W)\}$$

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W)))}\}$$
$$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} V}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} f(g(Z),W)}\}$$

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W))}\}$$
$$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} V}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} f(g(Z),W)}\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{X \stackrel{?}{=} g(Z)}, g(X) \stackrel{?}{=} W\}$$

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W))}\}$$
$$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} V}, V \stackrel{?}{=} f(g(Z),W)\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} f(g(Z),W)}\}$$
$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{X \stackrel{?}{=} g(Z)}, g(X) \stackrel{?}{=} W\}$$
$$\{Y \stackrel{?}{=} f(g(Z),g(g(Z))), V \stackrel{?}{=} f(g(Z),g(g(Z))), X \stackrel{?}{=} g(Z), \underline{g(g(Z)) \stackrel{?}{=} W}\}$$

Unificació (iv)

Unifiquem:

$$\{\underline{\mathrm{p}(f(X,g(X)),h(Y),V) \stackrel{?}{=} \mathrm{p}(Y,h(V),f(g(Z),W))}\}$$

$$\{\underline{f(X,g(X)) \stackrel{?}{=} Y}, h(Y) \stackrel{?}{=} h(V), V \stackrel{?}{=} f(g(Z),W)\}$$

$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{h(f(X,g(X))) \stackrel{?}{=} h(V)}, V \stackrel{?}{=} f(g(Z),W)\}$$

$$\{Y \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} V}, V \stackrel{?}{=} f(g(Z),W)\}$$

$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{f(X,g(X)) \stackrel{?}{=} f(g(Z),W)}\}$$

$$\{Y \stackrel{?}{=} f(X,g(X)), V \stackrel{?}{=} f(X,g(X)), \underline{X \stackrel{?}{=} g(Z)}, g(X) \stackrel{?}{=} W\}$$

$$\{Y \stackrel{?}{=} f(g(Z),g(g(Z))), V \stackrel{?}{=} f(g(Z),g(g(Z))), X \stackrel{?}{=} g(Z), \underline{g(g(Z)) \stackrel{?}{=} W}\}$$

$$\{Y \stackrel{?}{=} f(g(Z),g(g(Z))), V \stackrel{?}{=} f(g(Z),g(g(Z))), X \stackrel{?}{=} g(Z), W \stackrel{?}{=} g(g(Z))\}$$

Resolució i Factorització (i)

Sistema de demostració refutacionalment complet

1. **Resolució**.

$$\frac{A \vee C \qquad \neg A' \vee D}{C\sigma \vee D\sigma} \text{ on } \sigma = mgu(A, A')$$

2. **Factorització**.

$$\frac{A \vee A' \vee C}{A\sigma \vee C\sigma} \text{ on } \sigma = mgu(A, A')$$

Per tant podem definir (com abans) $ResFact^*(S)$ d'un conjunt de clàusules S de manera que: si $T \models F$ llavors $\Box \in Resfact^*(S)$ on S és la CNF de $T \wedge \neg F$.

- Cada vegada que fem servir una clàusula reanomenarem variables per evitar confusió.

Resolució i Factorització (ii)

TEOREMA: Church

El problema de la validesa de les fórmules de primer ordre és indecidible.
El problema de la satisfactibilitat de les fórmules de primer ordre és indecidible.

- Fer $ResFact^*(S)$ segueix essent molt car...
- Com demostrar que les següents fórmules no són insatisfactibles...?

$$\{\ \mathrm{p}(a), \neg\mathrm{p}(X) \vee \mathrm{p}(f(X))\ \}$$

- Com fer el nombre mínim de passos de resolució per a arribar a la clàusula buida?

Resolució i Factorització (iii)

- De demostracions a càlculs!!!

$$\{ \quad \begin{array}{l} (1)\ \mathtt{sum}(X, 0, X), \\ (2)\ \neg\mathtt{sum}(X, Y, Z) \vee \mathtt{sum}(X, s(Y), s(Z)), \\ (3)\ \neg\mathtt{sum}(s(0), s(s(0)), \mathit{Resultat}) \end{array} \quad \}$$

- Com garantir que es miren tots els camins quan ens cal? (múltiples respostes)

Per exemple:

$$\{ \quad \begin{array}{l} (C1)\ \mathtt{append}(\mathit{nil}, W, W), \\ (C2)\ \neg\mathtt{append}(X, Y, Z) \vee \mathtt{append}(U \cdot X, Y, U \cdot Z), \\ (Q3)\ \neg\mathtt{append}(V \cdot L1, L2, V \cdot a \cdot \mathit{nil}) \end{array} \quad \}$$

Millores en la resolució

- La explosió combinatòria de la resolució sistemàtica és massa gran!
- S'afegeixen més i més clàusules i de vegades més i més grans.

Com millorar-ne l'eficiència ?

- **Estratègies**: regles heurístiques que determinen l'ordre en que s'ha d'explorar "l'espai de cerca": mateix espai de cerca però potser t'estalvies de mirar-lo tot. Per exemple la *unit preference*...
- **Restriccions**: prohibicions de certs passos de resolució depenent de la forma dels resolents. Decreix l'espai de cerca... Però la completesa no està sempre garantida

Restriccions (i)

1. **P-resolució:** Un resolent sempre positiu. (Completa)
2. **Resolució lineal:** Si donada una clàusula C, el procés de resolució fa el primer pas amb C i tots els passos següents tenen com a mínim un "descendent" de C. (Completa)
3. **Conjunt de Suport:** Cal conèixer un subconjunt T de la teoria F tal que $F \setminus T$ sigui satisfactible. Llavors es prohibeixen els passos de resolució entre clàusules de $F \setminus T$. Per exemple Per saber si una fórmula és conseqüència lògica d'una teoria. (Completa)

Restriccions (ii)

4. **Restricció d'entrada:** Cada pas de resolució ha d'utilitzar un resolent de la teoria inicial. (No complet) (Horn Complet)
5. **Resolució unitària:** Cada pas de resolució ha d'utilitzar un resolent unitari, per tant es generen clàusules més petites. (No complet) (Horn Complet)
6. **Resolució SLD:** Lineal + Restricció d'entrada. La clàsula base ha de ser negativa i a cada pas de resolució l'altra resolent ha de ser no negativa i del conjunt d'entrada. (No complet) (Horn Complet)

SLD-Resolució (i)

Linear Resolution for Definite Clauses with Selection Rule

- Programa= Regles + fets. Un sol literal positiu.

Forma Original	Forma Clausal
$P_1^1 \wedge P_1^2 \wedge \cdots \wedge P_1^{n_1} \rightarrow C_1$	$\neg P_1^1 \vee \neg P_1^2 \vee \cdots \vee \neg P_1^{n_1} \vee C_1$
...	...
$P_m^1 \wedge P_m^2 \wedge \cdots \wedge P_m^{n_m} \rightarrow C_m$	$\neg P_m^1 \vee \neg P_m^2 \vee \cdots \vee \neg P_m^{n_m} \vee C_m$
F_1	F_1
...	...
F_k	F_k

- Queries (Objectius): Cap literal positiu.

Pregunta Original	Al passar negat a la teoria
$G_1 \wedge \cdots \wedge G_q$	$\neg G_1 \vee \cdots \vee \neg G_q$

SLD-Resolució (ii)

1. Agafem la clàusula Objectiu i en triem un àtom a resoldre (G_i).
2. Triem una clàusula de P amb la que fer-hi resolució per exemple $A_k^1 \vee \neg A_k^2 \ldots \neg A_k^{n_k}$:

$$\frac{\neg G_1 \vee \ldots \vee \neg G_k \qquad A_k^1 \vee \neg A_k^2 \ldots \neg A_k^{n_k}}{(\neg G_1 \vee \ldots \vee \neg G_{i-1} \vee \neg A_k^2 \ldots \neg A_k^{n_k} \vee \neg G_{i+1} \vee \ldots \vee \neg G_k)\sigma}$$

   on $\sigma = mgu(\neg G_i, A_k^1)$

3. Ara el nou objectiu és el resolent...

SLD-Resolució (iii)

El Prolog usa una mena d'SLD Resolució però no és completa:

- Sempre tria el literal de més a l'esquerra de l'objectiu.
- Sempre usa la primera regla aplicable del programa per a fer resolució.
  Per exemple:

$$\begin{array}{l} \mathrm{p}(X) :- \mathrm{p}(X). \\ \mathrm{p}(X) :- \mathrm{q}(X). \\ \mathrm{q}(a). \\ ?\ \mathrm{p}(Y). \end{array}$$

- Prolog no controla *occur-check*!!
- Proporciona aspectes extra-logics per a controlar l'eficiència...

Resum

Punts essencials

- Lògica proposicional: raonament sobre conjunts finits. SAT decidible. Resolució, refutacionalment completa.
- Lògica de primer ordre: raonament sobre conjunts infinits. SAT semi-decidible. Resolució (+factorització), refutacionalment completa.
- Programació Lògica: basada en SLD-resolució. Turing completa.

Bibliografia

"Logic for Computer Scientists", `Uwe Schöning`, (Birkäuser).