

# Programmazione logica

## Analisi statica

- l'interpretazione astratta è molto popolare in programmazione logica
  - Il modello computazionale si presta a varie ottimizzazioni, basate sui risultati dell'analisi
  - è relativamente facile da definire, poiché le semantiche sono naturalmente collecting ed il dominio concreto (insiemi di sostituzioni o insiemi di insiemi di equazioni) è piuttosto semplice
- esistono molte importanti proprietà (groundness, freeness, sharing, *depth* ( $k$ ))
- per alcune proprietà (groundness e sharing) esistono molti domini astratti differenti
  - tecniche per confrontare la precisione relativa di domini astratti important results on techniques for the systematic design domains, which can probably be applied to other paradigms as well
- compilazione astratta in CLP (Giacobazzi, Debray & Levi, JLP 95)
  - la computazione astratta è una computazione CLP standard su un differente sistema di vincoli

# Programmazione logica

Semantica comparativa

$$\alpha(\text{lfp } \mathcal{F}) = \text{lfp } \mathcal{F}^\alpha$$

- nessuno dei due punti fissi è calcolabile in un numero finito di passi

- utile per ragionare su differenti semantiche e per derivare sistematicamente semantiche più astratte

- scelta della semantica più adeguata alla particolare analisi e/o verifica

- $\mathcal{F}^\alpha$  è meno costoso di  $\mathcal{F}$  nel calcolo della proprietà osservabile modellata da  $\alpha$

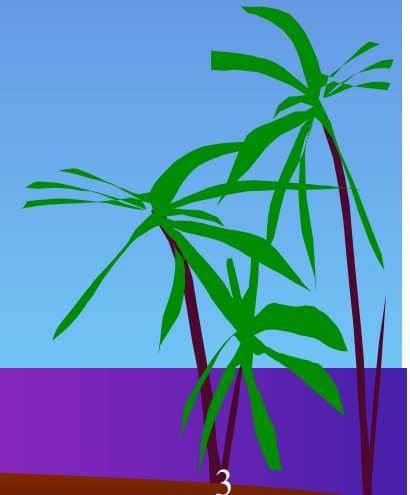
- no junk

- ricostruzione sistematica di diverse semantiche punto fisso

(Comini, Levi & Meo, Info. & Comp. 00)

# Groundness in Programmazione logica

- versione CLP
- dominio concreto
  - $(\mathcal{P}(\mathcal{E}qns), \subseteq)$ , insiemi di insiemi di equazioni in forma risolta
- semantica concreta
  - la versione CLP della s-semantica (vincoli di risposta)
- 3 domini astratti
  - $\mathcal{G}$ : the property of being ground
  - $DEF$ : dipendenze funzionali di groundness
  - $POS$ :  $DEF$  + un po' di informazione disgiuntiva
    - ◆ i reticoli sono mostrati nel caso di 2 variabili



# Un esempio

- programma

$p(X,Y) :- X=a.$

$p(X,Y) :- Y=b.$

$q(X,Y) :- X=Y.$

$r(X,Y) :- p(X,Y),q(X,Y).$

- semantica concreta

$p(X,Y) \rightarrow \{\{X=a\},\{Y=b\}\}$

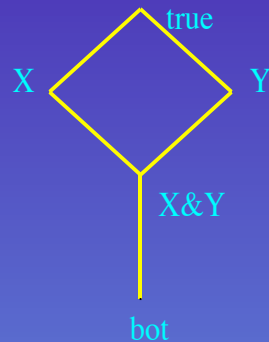
$q(X,Y) \rightarrow \{\{X=Y\}\}$

$r(X,Y) \rightarrow \{\{X=a,Y=a\},\{X=b,Y=b\}\}$

- nella semantica concreta di  $r$

- entrambi gli argomenti sono legati a terminiground (in tutti i vincoli di risposta)

# Il dominio $\mathcal{G}$



$\gamma_{\mathcal{G}}(v) =$

- $\emptyset$ , se  $v = \text{bot}$
- $\{e \in \mathcal{Eqns} \mid X \text{ è legato ad un termine ground in } e\}$ ,  
se  $v = X$   $X$  è sempre ground
- $\mathcal{Eqns}$ , se  $v = \text{true}$  nessuna informazione di groundness

- programma  
 $p(X,Y) :- X=a.$   
 $p(X,Y) :- Y=b.$   
 $q(X,Y) :- X=Y.$   
 $r(X,Y) :- p(X,Y),q(X,Y).$

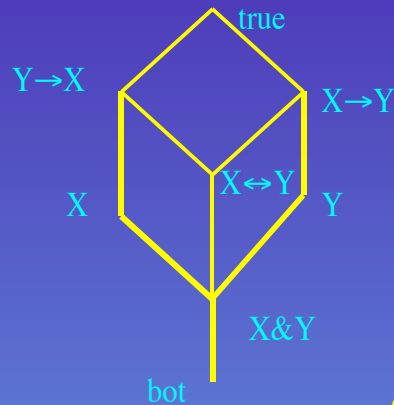
- semantica concreta  
 $p(X,Y) \rightarrow \{\{X=a\},\{Y=b\}\}$   
 $q(X,Y) \rightarrow \{\{X=Y\}\}$   
 $r(X,Y) \rightarrow \{\{X=a,Y=a\},\{X=b,Y=b\}\}$

- astrazione della semantica concreta  
 $p(X,Y) \rightarrow \text{true}$   
 $q(X,Y) \rightarrow \text{true}$   
 $r(X,Y) \rightarrow X \& Y$

- Programma astratto  
 $p(X,Y) :- \text{lub}_{\mathcal{G}}(X,Y).$   
 $q(X,Y) :- \text{true}.$   
 $r(X,Y) :- \text{glb}_{\mathcal{G}}(p(X,Y),q(X,Y)).$

- Semantica astratta  
 $p(X,Y) \rightarrow \text{true}$   
 $q(X,Y) \rightarrow \text{true}$   
 $r(X,Y) \rightarrow \text{true}$

# Il dominio Def



$\gamma_{Def}(v) =$

- $\{e \in \mathcal{Eqns} \mid X = Y \in e\}$ ,  
se  $v = X \leftrightarrow Y$  X is ground if and only if Y is ground
- $\{e \in \mathcal{Eqns} \mid X = t \in e \text{ e } Y \text{ occorre in } t\}$ ,  
se  $v = X \rightarrow Y$  if X is ground then Y is ground
- .....

- programma
  - $p(X,Y) :- X=a.$
  - $p(X,Y) :- Y=b.$
  - $q(X,Y) :- X=Y.$
  - $r(X,Y) :- p(X,Y),q(X,Y).$

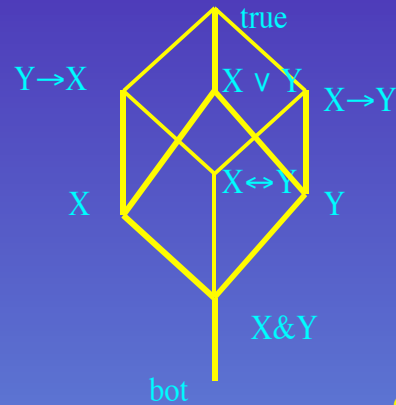
- semantica concreta
  - $p(X,Y) \rightarrow \{\{X=a\},\{Y=b\}\}$
  - $q(X,Y) \rightarrow \{\{X=Y\}\}$
  - $r(X,Y) \rightarrow \{\{X=a,Y=a\},\{X=b,Y=b\}\}$

- astrazione della semantica concreta
  - $p(X,Y) \rightarrow true$
  - $q(X,Y) \rightarrow X \leftrightarrow Y$
  - $r(X,Y) \rightarrow X \& Y$

- programma astratto
  - $p(X,Y) :- lub_{Def}(X,Y).$
  - $q(X,Y) :- X \leftrightarrow Y.$
  - $r(X,Y) :- glb_{Def}(p(X,Y),q(X,Y)).$

- semantica astratta
  - $p(X,Y) \rightarrow true$
  - $q(X,Y) \rightarrow X \leftrightarrow Y$
  - $r(X,Y) \rightarrow X \leftrightarrow Y$

# Il dominio Pos



$$\gamma_{pos}(v) =$$

- $\{e \in \mathcal{Eqns} \mid X \text{ oppure } Y \text{ è legato ad un termine ground in } e\}$ , if  $v = X \vee Y$  either X or Y is ground
- ....

- programma
  - $p(X,Y) :- X=a.$
  - $p(X,Y) :- Y=b.$
  - $q(X,Y) :- X=Y.$
  - $r(X,Y) :- p(X,Y),q(X,Y).$

- semantica concreta
  - $p(X,Y) \rightarrow \{\{X=a\},\{Y=b\}\}$
  - $q(X,Y) \rightarrow \{\{X=Y\}\}$
  - $r(X,Y) \rightarrow \{\{X=a,Y=a\},\{X=b,Y=b\}\}$

- astrazione della semantica concreta
  - $p(X,Y) \rightarrow X \vee Y$
  - $q(X,Y) \rightarrow X \Leftrightarrow Y$
  - $r(X,Y) \rightarrow X \& Y$

- programma astratto
  - $p(X,Y) :- \text{lub}_{pos}(X,Y).$
  - $q(X,Y) :- X \Leftrightarrow Y.$
  - $r(X,Y) :- \text{glb}_{pos}(p(X,Y),q(X,Y)).$

- semantica astratta
  - $p(X,Y) \rightarrow X \vee Y$
  - $q(X,Y) \rightarrow X \Leftrightarrow Y$
  - $r(X,Y) \rightarrow X \& Y$

# Verifica di programmi **Verifica** con Interpretazione Astratta

- $\mathcal{F}$  = funzione di valutazione semantica concreta
  - abbastanza concreta per poter osservare la proprietà
  - la proprietà è modellata da un dominio astratto  $(\mathcal{A}, \leq)$  e da una inserzione di Galois  $\alpha, \gamma$

- se  $\mathcal{F}^\alpha(S^\alpha) \leq S^\alpha$
- allora  $S^\alpha$  è un pre-puntofisso di  $\mathcal{F}^\alpha$
- quindi

$$\alpha(\text{lfp } \mathcal{F}) \leq \text{lfp } \mathcal{F}^\alpha \leq S^\alpha$$

- $\mathcal{F}^\alpha$  = funzione di valutazione semantica astratta
- $S^\alpha$  = specifica della proprietà, cioè astrazione della semantica concreta intesa

- correttezza parziale:  $\alpha(\text{lfp } \mathcal{F}) \leq S^\alpha$

- condizione sufficiente per la correttezza parziale:

$$\mathcal{F}^\alpha(S^\alpha) \leq S^\alpha$$

- (Comini, Levi, Meo & Vitiello, JLP 99)



## Analisi e Verifica

- $\mathcal{F}$  = funzione di valutazione semantica concreta
- $\mathcal{F}^\alpha$  = funzione di valutazione semantica astratta
- **analisi:** calcola lfp  $\mathcal{F}^\alpha$ 
  - dobbiamo calcolare un punto fisso
  - dominio noetheriano oppure widening
- $S^\alpha$  = specifica della proprietà
- **verifica:** dimostra  $\mathcal{F}^\alpha(S^\alpha) \leq S^\alpha$ 
  - niente calcolo di punto fisso, nessuna necessità di domini noetheriani
  - rappresentazione finita della specifica
  - decidibilità di  $\leq$

# Progetto sistematico di domini astratti

- una volta che abbiamo il dominio astratto, il progetto della semantica astratta è sistematico
- l'interpretazione astratta fornisce anche risultati che possono essere sfruttati per rendere (più) sistematico il progetto di domini astratti
  - per confrontare e combinare domini
  - per raffinare domini con il fine di migliorarne la precisione

- prodotto ridotto (dei domini  $\mathcal{A}$  e  $\mathcal{B}$ )
  - permette di analizzare (insieme) le proprietà modellate da  $\mathcal{A}$  e  $\mathcal{B}$
  - spesso fornisce risultati migliori delle due analisi separate
    - ◆ per l'interazione fra domini

- lifting al powerset (e completamento disgiuntivo )
  - più o meno, trasforma  $\mathcal{A}$  in  $\mathcal{P}(\mathcal{A})$
  - maggiore precisione
    - ◆ nessuna perdita di informazione nel calcolo dei lub's

# Operazioni sui Domini Astratti

- molti utili operatori su domini astratti (raffinamenti)
  - **un survey in** (File', Giacobazzi & Ranzato, ACM Comput. Surv. 96)

- **Completamento lineare**  
(Giacobazzi, Ranzato & Scozzari, SAS 98)

- **dipendenze funzionali modellate dall'implicazione di logica lineare**

- **ricostruzione di tutti i domini noti per l'analisi di groundness** (Scozzari, SAS 97)

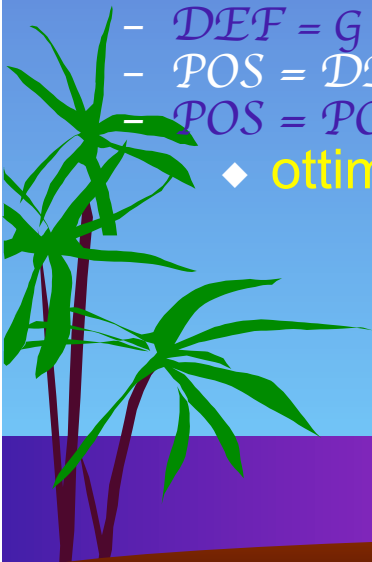
- $DEF = \mathcal{G} \rightarrow \mathcal{G}$
- $POS = DEF \rightarrow DEF$
- $POS = POS \rightarrow POS$
- ◆ **ottimalità di POS**

**poi applicata con successo ad altri domini in programmazione logica**

- **tipi** (Levi & Spoto, PLILP 98)
- **sharing e freeness**  
(Levi & Spoto, PEPM 00)

**problemi aperti**

- **gli stessi raffinamenti si applicano anche ad altri paradigmi o ai sistemi di tipo?**



# Interpretazione astratta

- una teoria matematica semplice e solida su cui basare
  - semantica comparativa
  - analisi statica
  - verifica
  - una metodologia per la derivazione sistematica di
    - domini astratti a partire dalla proprietà
    - semantica astratta a partire dalla semantica concreta e dal dominio astratto