Interpretazione Astratta

Astrazione:
selezionare una proprieta’

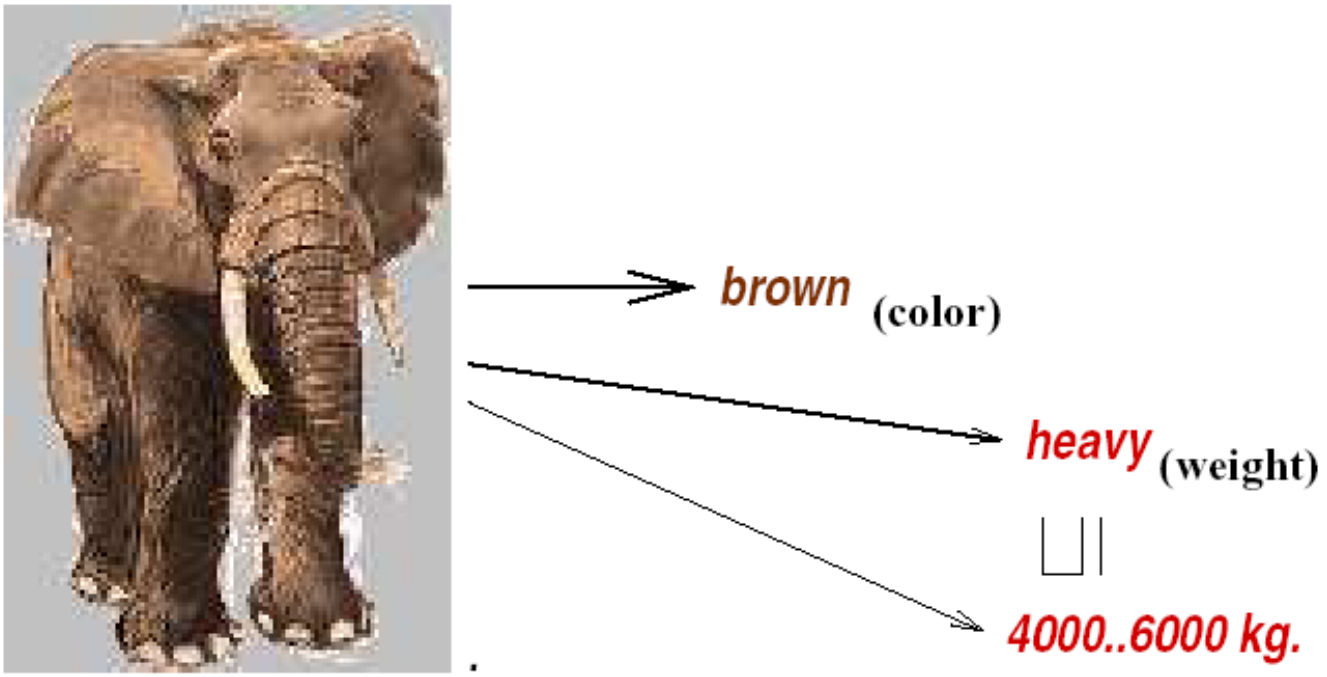
Astrazione:
selezionare una (delle) proprieta’

brown
(color)

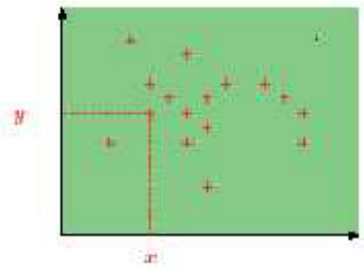
heavy
(weight)

.

Astrazione e correttezza

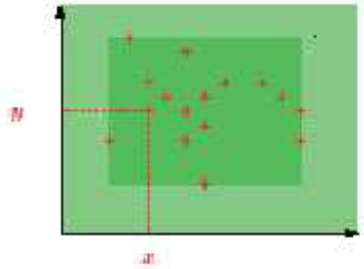


Astrarre un insiemi di punti nel piano



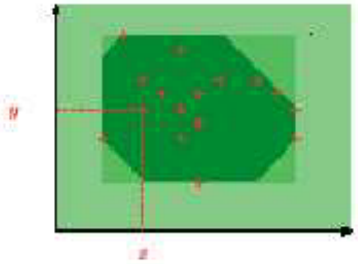
$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases}$$

Fig. 2
SIGNS



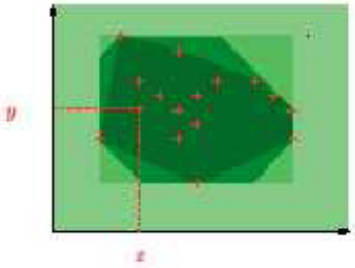
$$\begin{cases} x \in [3,\ 27] \\ y \in [4,\ 32] \end{cases}$$

Fig. 3
INTERVALS



$$\begin{cases} 3 \leq x \leq 27 \\ x + y \leq 88 \\ 4 \leq y \leq 32 \\ x - y \leq 61 \end{cases}$$

Fig. 4
OCTAGONS



$$\begin{cases} 7x + 31y \leq 325 \\ 21x + 7y \geq 0 \end{cases}$$

Fig. 5
POLYHEDRA

Interpretazione Astratta

- Una tecnica utilizzata da circa 30 anni (Patrick e Radhia Cousot, 1977) per trattare in modo sistematico astrazioni e approssimazioni
- Nata per descrivere analisi statiche di programmi imperativi e provarne la correttezza
- Sviluppata per varie classi di linguaggi di programmazione e sistemi reattivi
- Vista oggi come tecnica generale per ragionare su semantiche a diversi livelli di astrazione

L’idea generale

- Il punto di partenza è la semantica concreta, ovvero una funzione che assegna significati ai comandi di un programma in un dominio fissato di computazione.
- Un dominio astratto, che modella alcune proprietà delle computazioni concrete, tralasciando la rimanente informazione (dominio di computazione astratto).
- Derivare una semantica astratta, che permetta di “eseguire astrattamente” il programma sul dominio astratto per calcolare la proprietà che il dominio astratto modella.
- Il calcolo della semantica astratta tipicamente e` un calcolo di punto fisso.
- Sarà inoltre possibile calcolare una approssimazione corretta della semantica astratta.

Semantica concreta

- Considereremo un linguaggio pseudo-funzionale di base piuttosto che un linguaggio imperativo nello stile **While**
- Iniziamo da un linguaggio molto limitato, che permette unicamente di moltiplicare interi.

  Exp $\ni$ e ::= n | e*e
- La semantica di questo linguaggio si può descrivere mediante una funzione η definita da:

  η : **Exp** $\rightarrow \mathbb{Z}$

  $\eta(n) = n$

  $\eta(e_1 * e_2) = \eta(e_1) \times \eta(e_2)$

Semantica astratta

- Possiamo considerare un'astrazione della semantica concreta (semantica astratta) che calcola solo il segno delle espressioni

σ: **Exp** $\rightarrow$ {-,0,+}

$$\sigma(n) = \begin{cases} - & \text{se } n<0 \\ 0 & \text{se } n=0 \\ + & \text{se } n>0 \end{cases}$$

$\times^a$	-	0	+
-	+	0	-
0	0	0	0
+	-	0	+

$$\sigma(e_1 * e_2) = \sigma(e_1) \times^a \sigma(e_2)$$

Correttezza

- Possiamo dimostrare che questa astrazione è corretta, ovvero che prevede correttamente il segno delle espressioni.

- La dimostrazione è per induzione strutturale sull'espressione e semplicemente utilizza le proprietà della moltiplicazione tra interi (il prodotto di due positivi è positivo, etc.).

  Per ogni expressione $e \in$ **Exp**:

  $$\eta(e) < 0 \Leftrightarrow \sigma(e) = -$$
  $$\eta(e) = 0 \Leftrightarrow \sigma(e) = 0$$
  $$\eta(e) > 0 \Leftrightarrow \sigma(e) = +$$

Una prospettiva diversa

- Possiamo associare ad ogni valore astratto l'insieme di valori concreti che esso rappresenta:

γ:{-,0,+} $\rightarrow \mathcal{P}(\mathbb{Z})$

$\gamma(-) = \{x \in \mathbb{Z} \mid x<0\}$

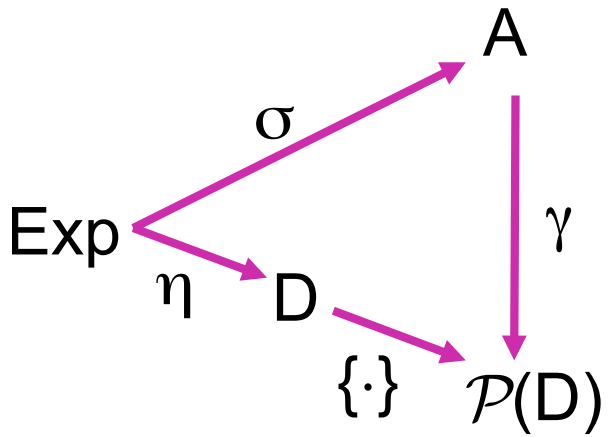
$\gamma(0) = \{0\}$

$\gamma(+) = \{x \in \mathbb{Z} \mid x>0\}$

Concretizzazione

- La funzione di concretizzazione γ mappa un valore astratto in un insieme di valori concreti
- Indichiamo con D il dominio concreto dei valori e con A il dominio astratto

$$\eta(e) \in \gamma(\sigma(e))$$



Interpretazione Astratta

- Abbiamo specificato una interpretazione astratta.
  - Computazioni astratte in un dominio astratto
  - In questo caso, il dominio astratto è {+,0,-}.

- La semantica astratta è corretta
  - è un'approssimazione della semantica concreta

    $\{\eta(e)\} \subseteq \gamma(\sigma(e))$

- La funzione di concretizzazione stabilisce la relazione tra il concetto di approssimazione nei due domini concreto ed astratto

Aggiungiamo -

- Aggiungiamo al nostro tiny language l'operatore unario di cambiamento di segno

  Exp $\ni$ e ::= n | e*e | -e

  $\eta(-e) = -\eta(e)$

  $\sigma(-e) = -^a\sigma(e)$ dove $-^a(-) = +,\ -^a(0) = 0,\ -^a(+) = -$

Aggiungiamo +

- Aggiungere l'addizione è più complesso, in quanto il dominio astratto non è chiuso rispetto a questa operazione

$$\eta(e_1 + e_2) = \eta(e_1) + \eta(e_2)$$

$$\sigma(e_1 + e_2) = \sigma(e_1) +^a \sigma(e_2)$$

$+^a$	-	0	+
-	-	-	?
0	-	0	+
+	?	+	+

- A quale valore astratto corrisponde il risultato della somma di due numeri interi con segno opposto?

Soluzione

- Aggiungiamo un nuovo valore astratto $\top$ che rappresenta un qualsiasi numero intero

$\gamma(\top) = \mathbb{Z}$

$+^a$	-	0	+	$\top$
-	-	-	$\top$	$\top$
0	-	0	+	$\top$
+	$\top$	+	+	$\top$
$\top$	$\top$	$\top$	$\top$	$\top$

Estendere le altre operazioni

- Avendo aggiunto un elemento al dominio astratto, è necessario estendere le operazioni astratte già definite

$\times^a$	-	0	+	$\top$
-	+	0	-	$\top$
0	0	0	0	0
+	-	0	+	$\top$
$\top$	$\top$	0	$\top$	$\top$

$-^a(-) = +,\ -^a(0) = 0,$
$-^a(+) = -,\ -^a(\top) = \top$

Esempi

- In alcuni casi c'è perdita di informazione dovuta alle operazioni

  $\eta((1+2) - 3) = 0$
  $\sigma((1+2)+ -3) = (+ +^a +) +^a - = + +^a - = \top$

- In altri casi non c'è perdita di informazione

  $\eta((5*4) + 6) = 26$
  $\sigma((5*4) + 6) = (+ \times^a +) +^a + = + +^a + = +$

Aggiungiamo la divisione

- Aggiungere la divisione intera / non crea problemi, eccetto il caso della divisione per 0
- Se dividiamo un insieme di interi per 0 che risultato otteniamo? L'insieme vuoto. Quindi la semantica concreta assumera` i propri valori sul powerset di $\mathbb{Z}$, cioe` η:**Exp** $\rightarrow \mathcal{P}(\mathbb{Z})$
- L'insieme vuoto di interi è rappresentato da un nuovo elemento $\perp$ astratto rispetto al quale si devono estendere le altre operazioni

$\gamma(\perp)=\emptyset$

$/^a$	-	0	+	$\top$	$\perp$
-	+	0	-	$\top$	$\perp$
0	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$
+	-	0	+	$\top$	$\perp$
$\top$	$\top$	0	$\top$	$\top$	$\perp$
$\perp$	$\perp$	$\perp$	$\perp$	$\perp$	$\perp$

$\perp +^a x = \perp = x +^a \perp$

$\perp \times^a x = \perp = x \times^a \perp$

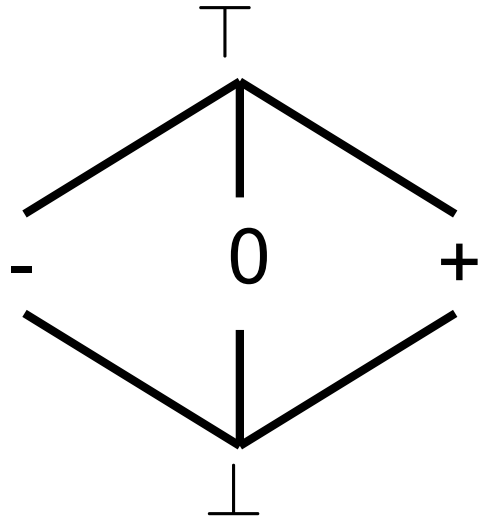
$-^a (\perp) = \perp$

Il dominio astratto

- Il dominio astratto è un poset in cui l'ordine parziale rappresenta la nozione di approssimazione/ precisione
- L'ordine parziale è coerente con la funzione di concretizzazione:

$$x \leq y \Leftrightarrow \gamma(x) \subseteq \gamma(y)$$

- Ogni sottoinsieme ha un lub ed un glb: è quindi un reticolo completo



La funzione di astrazione

- Alla funzione di concretizzazione γ corrisponde una funzione di astrazione α.
- La funzione α mappa un insieme S di valori concreti nel piu` preciso valore astratto che rappresenta S.
- Nel nostro esempio

$$\alpha:\mathcal{P}(\mathbb{Z}) \rightarrow A \qquad \alpha(S) = \begin{cases} \bot & \text{se } S = \emptyset \\ - & \text{se } S \neq \emptyset,\ S \subseteq \mathbb{Z}_{<0} \\ 0 & \text{se } S = \{0\} \\ + & \text{se } S \neq \emptyset,\ S \subseteq \mathbb{Z}_{>0} \\ \top & \text{altrimenti} \end{cases}$$

Definizione Generale

- Una Interpretazione Astratta consiste in:
  - Un dominio astratto A ed un dominio concreto C
  - A e C reticoli completi. L'ordine riflette la precisione/ approssimazione (più piccolo = più preciso)
  - Funzioni di concretizzazione e di astrazione monotone, che formano una inserzione di Galois.
  - Operazioni astratte che astraggono correttamente su A la semantica concreta su C.

- Inserzione di Galois: funzioni monotone α:C$\rightarrow$A e γ:A$\rightarrow$C tali che:

  $\forall c \in C.\ c \leq_C \gamma(\alpha(c))$

  $\forall a \in A.\ a = \alpha(\gamma(a))$

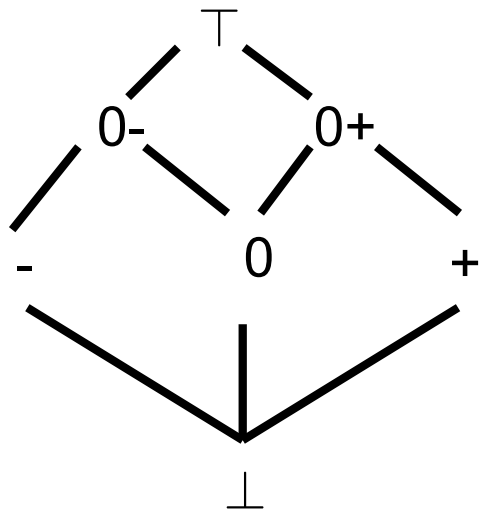
Altro esempio

$\gamma_{sign}(x) =$

- $\emptyset$, se $x = \bot$
- $\{y \in \mathbb{Z} | y > 0\}$, se $x = +$
- $\{y \in \mathbb{Z} | y \geq 0\}$, se $x = 0+$
- $\{0\}$, se $x = 0$
- $\{y \in \mathbb{Z} | y \leq 0\}$, se $x = 0-$
- $\{y \in \mathbb{Z} | y < 0\}$, se $x = -$
- $\mathbb{Z}$, se $x = \top$

$\alpha_{sign}(S) =$ glb di

- $\bot$, se $S = \emptyset$
- -, se $S \subseteq \{z \in \mathbb{Z} | z < 0\}$
- 0-, se $S \subseteq \{z \in \mathbb{Z} | z \leq 0\}$
- 0, se $S = \{0\}$
- 0+, se $S \subseteq \{z \in \mathbb{Z} | z \geq 0\}$
- +, se $S \subseteq \{z \in \mathbb{Z} | z > 0\}$
- $\top$, se $S \subseteq \mathbb{Z}$



$\alpha_{sign}(\{0,1,3\}) = 0+$

$\gamma_{sign}(0+) \supseteq \{0,1,3\}, \{3,5,2\}, \ldots$

$\gamma_{sign}(\alpha_{sign}(\{0,1,3\})) \supseteq \{0,1,3\}$

$\alpha_{sign}(\gamma_{sign}(0+)) = 0+$

Connessione di Galois

(α, C, A, γ) GC (Galois connection) se

1) A e C poset
2) α:C $\rightarrow$ A monotona (funzione di astrazione)
3) γ : A $\rightarrow$ C monotona (funzione di concretizzazione)
4) $\forall c \in C.\ c \leq_C \gamma(\alpha(c))$
5) $\forall a \in A.\ \alpha(\gamma(a)) \leq_A a$

Inserzione di Galois

(α, C, A, γ) GC e` una Galois insertion (GI) se vale una delle seguenti condizioni equivalenti:

1) α suriettiva
2) γ iniettiva
3) $\forall a \in A.\ \alpha(\gamma(a)) = a$

Aggiunzioni

(α, C, A, γ) aggiunzione se

1) A e C poset
2) α:C $\rightarrow$ A (astrazione)
3) γ : A $\rightarrow$ C (concretizzazione)
4) $\forall c \in C.\ \forall a \in A.\ \alpha(c) \leq_A a \Leftrightarrow c \leq_C \gamma(a)$

FATTO: (α,C,A,γ) GC $\Leftrightarrow$ (α,C,A,γ) aggiunzione

Galois Insertion: proprieta`

(α, C, A, γ) GI tra reticoli completi

(1) $\alpha(c) = \wedge\{a \in A \mid c \leq_C \gamma(a)\}$
(2) $\gamma(a) = \vee\{c \in C \mid \alpha(c) \leq_A a\}$
(3) **QUINDI**: α determina γ e viceversa
(4) α preserva i lub's
(5) γ preserva i glb's
(6) $\alpha(\bot_C) = \bot_A$ e $\gamma(\top_A) = \top_C$
(7) se una funzione $\alpha : C \rightarrow A$ tra reticoli completi preserva i lub's allora posso definire la γ come in (2) che forma con α una GI
(8) se una funzione $\gamma : A \rightarrow C$ preserva i glb's allora posso definire la α come in (1) che forma con γ una GI

Galois Insertion: proprieta`

Come "trasformare" una GC (α, C, A, γ) in una GI eliminando i valori astratti "inutili"?

Semplicemente considero come dominio astratto "ridotto" (reduced) $A^{red} = \alpha(C)$ e considero le restrizioni delle medesime funzioni di astrazione e concretizzazione:

$\alpha^{red} : C \rightarrow A^{red}$ dove $\alpha^{red}(c) = \alpha(c)$

$\gamma^{red} : A^{red} \rightarrow C$ dove $\gamma^{red}(a) = \gamma(a)$

Banalmente, (α^{red}, C, A^{red}, γ^{red}) e' diventata una GI con lo stesso "potere espressivo" della GC di partenza.

Astrazioni come chiusure

- Il dominio astratto specificato come una GI (α,C,A,γ) induce una partizione del dominio concreto:

  $$c_1 \sim c_2 \Leftrightarrow \alpha(c_1) = \alpha(c_2)$$

- Per ogni classe di equivalenza $[c]_\sim$ esiste il lub, cioe' ogni classe di equivalenza ha un rappresentante canonico
- La funzione ρ:C$\rightarrow$ C che mappa un valore concreto c a questo rappresentante $\vee_c[c]_\sim$ e` un operatore di chiusura su C

Chiusure

- Un operatore $\rho : C \rightarrow C$ su un poset C e` una chiusura se:
  - ρ e` monotona
  - ρ e` crescente: $x \leq \rho(x)$
  - ρ e` idempotente: $\rho(\rho(x)) = \rho(x)$
- uco(C) denota l'insieme di tutte le chiusure su C

Chiusure e GI

- Una GI (α,C,A,γ) induce una chiusura $\rho_A:C\to C$ definita come:

  $\rho_A(c) \triangleq \gamma\circ\alpha(c) = \vee_C\{x\in C \mid \alpha(x)\leq\alpha(c)\} = \vee_c[c]_\sim$
- Una chiusura $\rho:C \to C$ su un reticolo completo C induce una GI $(\rho,C,img_\rho(C),id)$
- Queste due trasformazioni sono una l'inversa dell'altra
- **QUINDI**: la specifica di un dominio astratto puo` essere data equivalentemente tramite una GI o una chiusura

Proprieta` delle Chiusure

1. Una chiusura $\rho \in$ uco(C) (con C reticolo completo) e` univocamente determinata dalla sua immagine
   $$\mathrm{img}_\rho(C) \triangleq \{\rho(x) \mid x \in C\}$$
2. $\rho(x) = \wedge\{y \in \mathrm{img}_\rho(C) \mid x \leq y\}$
3. $\mathrm{img}_\rho(C) = \mathrm{fix}(\rho) \triangleq \{x \in C \mid \rho(x)=x\}$
4. $X \subseteq C$ e` l'immagine di una chiusura $\rho_X$ su C iff X e` una Moore-family di C, cioe` $X=\mathcal{M}(X) \triangleq \{\wedge S \mid S \subseteq X\}$ (dove $\top = \wedge\varnothing \in \mathcal{M}(X)$)
5. Quindi, se X e` una Moore-family allora $\rho_X \triangleq \lambda x.\wedge\{y \in X \mid x \leq y\}$ e` la corrispondente chiusura
6. $\mathcal{M}(X)$ e` detta la chiusura di Moore (Moore-closure) di X in C, cioe` $\mathcal{M}(X)$ e` il piu` piccolo sottoinsieme di C che contiene X ed e` una Moore-family
7. **VALE**: $\rho_{\mathrm{img}_\rho} = \rho$ e $\mathrm{img}(\rho_X)=X$
8. **QUINDI**: chiusure su C sono in biezione con Moore-families di C

Proprieta` delle Chiusure

Teorema: Se C e` un reticolo completo allora uco(C) e` un reticolo completo $(uco(C), \sqsubseteq, \sqcup, \sqcap, \lambda x.\top_C, \lambda x.x)$ dove:

- $\mu \sqsubseteq \rho$ iff $\forall y \in C.\ \mu(y) \leq_C \rho(y)$ iff $img(\rho) \subseteq img(\mu)$
- $\sqcap_{i \in I} \rho_i = \lambda x. \wedge_{i \in I} \rho_i(x)$ e $img(\sqcap_{i \in I} \rho_i) = \mathcal{M}(\cup_{i \in I} img(\rho_i))$
- $img(\sqcup_{i \in I} \rho_i) = \cap_{i \in I} img(\rho_i)$
- $\lambda x.\top_C$ e` la chiusura top mentre $\lambda x.x$ e` la chiusura bottom

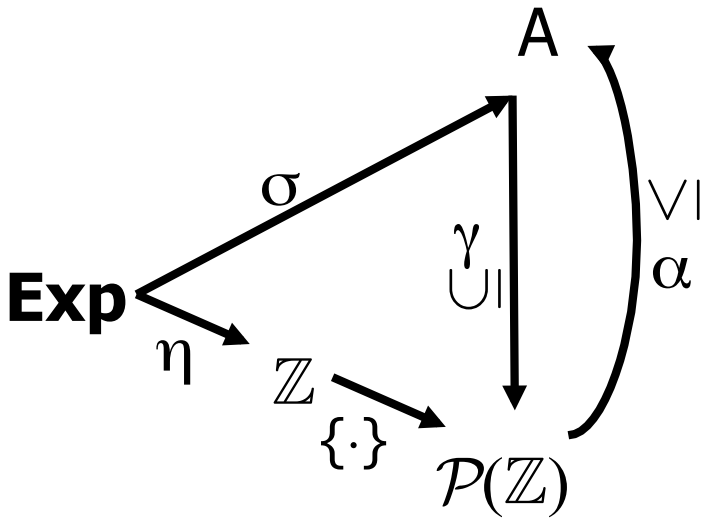
Il Reticolo dei Domini Astratti

- uco(C) viene detto il reticolo dei domini astratti
- se A_1 e A_2 sono due astrazioni di un dominio concreto comune C, specificate mediante GI, allora A_1 e` piu` preciso (o piu` concreto, o meno approssimato) di A_2, denotato da $A_1 \sqsubseteq A_2$, quando $\rho_{A_1} \sqsubseteq \rho_{A_2}$ (come chiusure)
- A_1 e A_2 si dicono astrazioni equivalenti quando $\rho_{A_1}=\rho_{A_2}$
- Lub's and glb's in uco(C) si possono quindi interpretare nel seguente modo: sia $\{A_i\}_{i\in I}$ una famiglia qualsiasi di astrazioni di C
  - $\sqcup_{i\in I}A_i$ e` il piu` concreto tra i domini che sono astrazioni di tutti gli A_i
  - $\sqcap_{i\in I}A_i$ e` il piu` astratto tra tutti i domini che sono piu` precisi di tutti gli A_i

Astrazione e Concretizzazione

- In una interpretazione astratta ci aspettiamo che il seguente diagramma commuti:

$$\{\eta(e)\} \subseteq \gamma(\sigma(e))$$
$$\alpha(\{\eta(e)\}) \leq \sigma(e)$$



Correttezza

- Per la correttezza dell'analisi sono necessarie le seguenti condizioni
- (α,C,A,γ) e` una GI
- Le operazioni astratte op^a (che sono supposte essere monotone) sono corrette rispetto alle corrispondenti operazioni concrete op (che sono pure supposte essere monotone): per ogni $\langle a_1,...,a_n\rangle \in A^n$

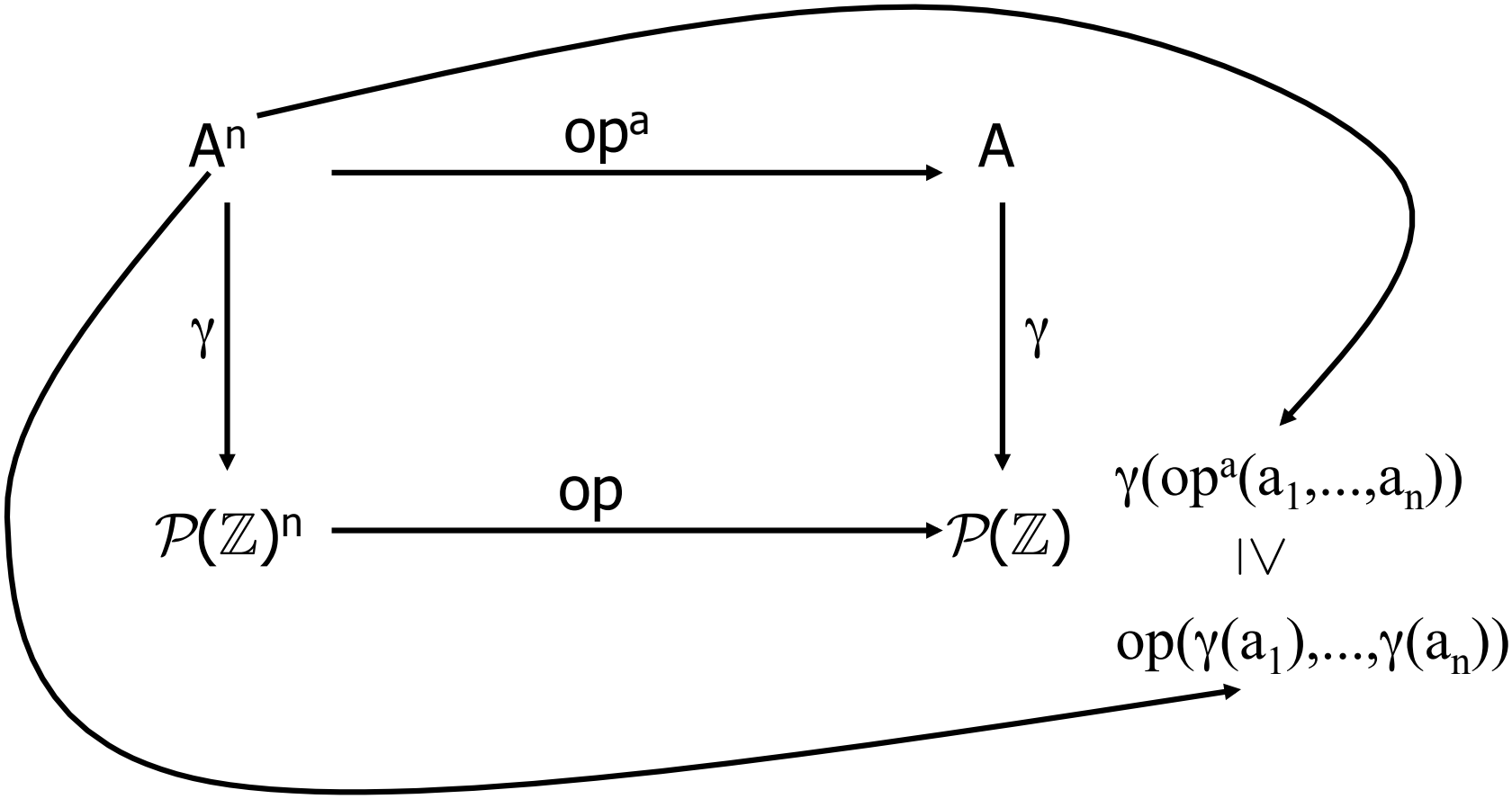
  $op(\gamma(a_1),...,\gamma(a_n)) \leq_C \gamma(op^a(a_1,...,a_n))$
- La correttezza di un'operazione astratta op^a puo` essere equivalentemente definita come: per ogni $\langle c_1,...,c_n\rangle \in C^n$

  $\alpha(op(c_1,...,c_n)) \leq_A op^a(\alpha(c_1),...,\alpha(c_n))$

Migliore approssimazione

- La condizione di correttezza garantisce quindi che il risultato dell'applicazione dell'operazione astratta sia una corretta approssimazione del risultato dell'applicazione della corrispondente operazione concreta.
- Per ogni operazione concreta op, possiamo sempre definire la cosiddetta migliore approssimazione corretta di op sul dominio astratto A.
- $op^A(a_1,...,a_n) \triangleq \alpha(op(\gamma(a_1),...,\gamma(a_n))$

Correttezza



Prova di correttezza

- Proviamo per induzione sulla struttura di $e \in$ **Exp** che $\{\eta(e)\} \subseteq \gamma(\sigma(e))$
- **Passo base**:
  $\{\eta(n)\} = \{n\} \subseteq \gamma(\alpha(\{n\})) = \gamma(\sigma(n))$
- **Passo induttivo**:

  $\{\eta(e_1 \text{ op } e_2)\} = \{\eta(e_1) \text{ op } \eta(e_2)\} \subseteq$

  [per ipotesi induttiva su e_1 ed e_2 e per monotonia di op]

  $\gamma(\sigma(e_1)) \text{ op } \gamma(\sigma(e_2)) \subseteq$

  [per correttezza]

  $\gamma(\sigma(e_1) \text{ op}^a \sigma(e_2)) = \gamma(\sigma(e_1 \text{ op } e_2))$

Correttezza

- Possiamo definire la correttezza utilizzando l'astrazione al posto della concretizzazione

$$\{\eta(e)\} \subseteq \gamma(\sigma(e)) \;\Leftrightarrow\; \alpha(\{\eta(e)\}) \leq \sigma(e)$$

- Deriva dal fatto che una GI e` equivalente ad una aggiunzione