

Metodi simbolici per migliorare la precisione di domini astratti numerici

Dino Puller

`dino.puller@students.univr.it`

Facoltà di MM.FF.NN.
Università degli studi di Verona

Introduzione

Metodi simbolici per migliorare la precisione di analizzatori statici basati sull'Interpretazione Astratta:

- La linearizzazione: una tecnica per la semplificazione di espressioni
- Propagazione di costanti simboliche

Il linguaggio

Definizione 1. *La grammatica:*

$COM ::= COM\ ASSIGN \mid ASSIGN \mid ASSINT$

$ASSIGN ::= VAR \leftarrow EXP$

$ASSINT ::= VAR \leftarrow [NUM, NUM]$

$EXP ::= EXP + EXP \mid EXP - EXP$

$\mid EXP \times EXP \mid EXP / EXP$

$\mid VAR \mid NUM$

$VAR ::= v \in \mathcal{V}$

$NUM ::= n \in \mathbb{D} \text{ con } \mathbb{D} \in \{\mathbb{R}, \mathbb{Z}, \mathbb{Q}\} \cup \{-\infty, +\infty\}$

Ordine parziale sulle espressioni

Definizione 2.

$$e_1 \sqsubseteq_R e_2 \Leftrightarrow \forall \sigma \in R, \mathcal{A}[[e_1]]\sigma \subseteq \mathcal{A}[[e_2]]\sigma$$

- Valuazione della memoria in un dominio astratto: $\sigma^\# : \mathcal{V} \rightarrow \mathbb{D}^\#$
- Uso degli operatori di Galois: $\sigma^\# = \alpha \circ \sigma$ e $\sigma = \gamma \circ \sigma^\#$

Teorema 1. *Se $e_1 \sqsubseteq_\sigma e_2$ allora il comando $\mathcal{C}[[V \leftarrow e_1]]\sigma^\#$ può essere sostituito da $\mathcal{C}[[V \leftarrow e_2]]\sigma^\#$.*

Gli intervalli

Definizione 3. *Un intervallo è una coppia di valori $[a, b]$ con la relazione $a \leq b$ e $a, b \in \mathbb{Z}$.*

$$\begin{aligned}(\perp \diamond x) \vee (x \diamond \perp) &= \perp & \diamond &= \{+, -, \times, /\} \\ [a, b] + [a', b'] &= [a + a', b + b'] \\ [a, b] - [a', b'] &= [a - b', b - a'] \\ [a, b] \times [a', b'] &= [\min\{aa', ab', ba', bb'\}, \\ & \quad \max\{aa', ab', ba', bb'\}] \end{aligned}$$

La forma Affine

$$[a, b] / [a', b'] = \begin{cases} \perp & \text{se } 0 \in \{a', b'\} \\ [\lfloor \min\{a/a', a/b', b/a', b/b'\} \rfloor, \\ \lceil \max\{a/a', a/b', b/a', b/b'\} \rceil] & \text{altrimenti} \end{cases}$$

Definizione 4. *Una forma affine è una combinazione lineare di intervalli per variabili e ha la forma:*

$$i_0 + \sum_k i_k \times V_k.$$

La forma Affine

Le operazioni sono definite di seguito:

$$(i_0 + \sum_k i_k \times V_k) + (i'_0 + \sum_k i'_k \times V_k) = (i_0 + i'_0) + \sum_k (i_k + i'_k) \times V_k$$

$$(i_0 + \sum_k i_k \times V_k) - (i'_0 + \sum_k i'_k \times V_k) = (i_0 - i'_0) + \sum_k (i_k - i'_k) \times V_k$$

$$i \times (i_0 + \sum_k i_k \times V_k) = ((i \times i_0) + \sum_k (i \times i_k) \times V_k)$$

$$(i_0 + \sum_k i_k \times V_k) / i = ((i_0 / i) + \sum_k (i_k / i) \times V_k)$$

La linearizzazione

Esempio 1. Prendiamo i seguenti comandi ed il dominio astratto \mathbb{I} :

$$X \leftarrow [-10, 10]$$

$$Y \leftarrow X - 2 \times X$$

$$Y \leftarrow [-10, 10] - [-20, 20]$$

Otteniamo $\sigma^\# = \{Y \mapsto [-30, 30]\}$, ma con:

$$Y \leftarrow -X$$

in questo caso: $Y \in [-10, 10]$

ι e π

Definizione 5 (Per gli intervalli). *L'operatore di proiezione $\pi : \mathcal{V} \rightarrow \mathbb{I}$*

$$\pi(x) = \sigma^\#(x)$$

Definizione 6 (Per gli intervalli).

$$\iota(i_0 + \sum_k i_k \times V_k) \sigma = i_0 + \sum_k i_k \times \pi(V_k) \text{ con } \sigma \in \Sigma^\#.$$

Teorema 2. *La linearizzazione ι è corretta:*

$$\forall \text{exp} \forall \sigma \text{exp} \sqsubseteq_\sigma \iota(\text{exp}) \sigma.$$

L'assegnazione

Le espressioni sono valutate grazie a π , nel dominio degli intervalli. C'è quindi bisogno dell'operazione inversa:

- l'assegnamento, che oltre quindi a valutare una espressione, dovrà tradurla in un elemento in $D^\#$.
- Per il dominio astratto \mathbb{I} faremo uso di ι .

La linearizzazione

La linearizzazione di una espressione e in un ambiente astratto $\sigma^\#$: $(|e|)\sigma^\#$ è definita tramite induzione strutturale come segue:

Definizione 7.

$$\begin{aligned}(|a|)\sigma^\# &= [a, a] \\(|V|)\sigma^\# &= [1, 1] \times V \\(|e_1 + e_2|)\sigma^\# &= (|e_1|)\sigma^\# + (|e_2|)\sigma^\# \\(|e_1 - e_2|)\sigma^\# &= (|e_1|)\sigma^\# - (|e_2|)\sigma^\# \\(|e_1 \times e_2|)\sigma^\# &= \iota((|e_1|)\sigma^\#)\sigma^\# \times (|e_2|)\sigma^\# \\(|e_1 / e_2|)\sigma^\# &= (|e_2|)\sigma^\# / \iota((|e_2|)\sigma^\#)\sigma^\#\end{aligned}$$

La linearizzazione

Teorema 3. *La linearizzazione di espressioni è corretta: $\forall exp \ exp \sqsubseteq_{\sigma} (|exp|)\sigma^{\#}$. Ipotizzando che tutte le variabili dell'espressione exp siano definite in $\sigma^{\#}$.*

Definizione 8 (Per gli intervalli). *Data una espressione exp qualunque:*

$$\mathcal{C}[[V \leftarrow exp]]\sigma^{\#} = \mathcal{C}[[V \leftarrow \iota((|exp|)\sigma^{\#})\sigma^{\#}]]\sigma^{\#}$$

Esempio completo

Esempio 2.

$$X \leftarrow [-10, 10]$$

$$Y \leftarrow X - 2 \times X$$

Applichiamo la linearizzazione al comando di assegnamento con stato

$$\sigma^\# = \{X \mapsto [-10, 10]\}:$$

$$\mathcal{C}[[Y \leftarrow X - 2 \times X]]\sigma^\# = \mathcal{C}[[Y \leftarrow \iota(|X - 2 \times X|)\sigma^\#)\sigma^\#]]\sigma^\#$$

Esaminiamo ogni passaggio:

$$\begin{aligned}(|X - 2 \times X|)\sigma^\# &= ((|X|)\sigma^\# - (|2 \times X|)\sigma^\#)\sigma^\# \\ &= (([0,0] + [1,1] \times X - \iota((|2|))\sigma^\#)^\# \times (|X|)\sigma^\#)\sigma^\# \\ &= (([0,0] + [1,1] \times X - [2,2] \times [0,0] + [1,1] \times X))\sigma^\# \\ &= (([0,0] + [1,1] \times X - [0,0] + [-2,-2] \times X))\sigma^\# \\ &= [0,0] + [-1,-1] \times X\end{aligned}$$

Ottenendo infine applicando $\iota(\cdot)\sigma^\#$:

$$\sigma'^\# = \{X \mapsto [-10, 10], Y \mapsto [-10, 10]\}$$

Applicazione ad un dominio numerico

Esempio 3. *Dominio astratto del segno:*

$$\pi(x) = [\lfloor \sigma(x) \rfloor, \lceil \sigma(x) \rceil]$$

Consideriamo il seguente programma:

$$X \leftarrow 3.14$$

$$Y \leftarrow X - 2 \times X$$

Nel dominio dei segni:

$$X \leftarrow +$$

$$Y \leftarrow + - + \times +$$

$$\sigma^\# = \{Y \mapsto \top\}$$

Applicazione ad un dominio numerico

Come risultato otterremo un allarme. Invece con la linearizzazione:

$$X \leftarrow +$$

$$Y \leftarrow -\pi(X) \quad \text{dove } \pi(X) = [3, 4]$$

ora $Y \mapsto [-4, -3]$ nel dominio degli intervalli, ma grazie alla funzione di trasferimento nel dominio dei segni abbiamo:

$$\sigma^\# = \{Y \mapsto -\}$$

Strategie

I punti deboli:

1. τ fa perdere traccia delle operazioni svolte.
2. La moltiplicazione aggiunge incertezza.

Strategie:

- Intervallo minore
- Ampiezza relativa
- Linearizza tutto
- Tendi a semplificare
- Omogeneità

Intervallo minore

Intervallo minore: $[a, b] \leq [a', b'] \equiv b - a \leq b' - a'$

$$(|e_1 \times e_2|) \sigma^\# =$$

$$\begin{cases} \iota(|e_1|) \sigma^\# \times (|e_2|) \sigma^\# & \iota(|e_1|) \sigma^\# \leq \iota(|e_2|) \sigma^\# \\ \iota(|e_2|) \sigma^\# \times (|e_1|) \sigma^\# & \text{altrimenti} \end{cases}$$

Ampiezza relativa:

Usiamo la differenza relativa tra due intervalli:

$$[a, b] \leq [a', b'] \equiv \frac{b - a}{|b + a|} \leq \frac{b' - a'}{|b' + a'|}$$

Linearizza tutto

1. Linearizziamo ambedue le espressioni del prodotto
2. Analizziamo separatamente ogni risultato ottenuto
3. Intersechiamo \cap in $\mathbb{D}^\#$ i risultati.

Ha costo esponenziale sul numero di moltiplicazioni.

Tendi a semplificare

Nell'espressione: $X - (Y \times X)$ se applichiamo ι su X andremo a perdere una successiva semplificazione.

- Manteniamo in forma simbolica le variabili che compaiono in altre sotto-espressioni di *exp*

Omogeneità

$$X \leftarrow [0, 1] \quad Y \leftarrow [0, 10] \quad Z \leftarrow [0, 20]$$
$$T \leftarrow X \times Y - X \times Z + Z$$

La strategia precedente fallisce.

- Applichiamo la linearizzazione al più piccolo insieme di variabili che rendono l'espressione risultante con tutti i monomi dello stesso grado.

Linearizzando X : $T \leftarrow [0, 1] \times Y + [0, 1] \times Z$ e
 $T \in [0, 30]$

Propagazioni di costanti simboliche

Esempio 4.

$$X \leftarrow [0, 5]$$

$$T \leftarrow X$$

$$Y \leftarrow T - 2 \times X$$

Con la linearizzazione ottengo:

$$T \leftarrow [1, 1] \times T - [2, 2] \times X$$

$$\sigma^\# = \{Y \mapsto [-10, 5]\}$$

Poteva essere riscritto come: $Y \leftarrow -X$ ottenendo lo stato: $\sigma^\# = \{Y \mapsto [-5, 0]\}$

Dominio di costanti simboliche

Denotiamo con \mathcal{C} l'insieme di tutte le espressioni sintattiche più \top e \perp

Definizione 9. *La funzione $occ : \mathcal{C} \rightarrow \mathcal{P}(\mathcal{V})$ restituisce l'insieme delle variabili che occorrono in una espressione.*

Definizione 10. *La funzione $subst : \mathcal{C} \times \mathcal{V} \times \mathcal{C} \rightarrow \mathcal{C}$ sostituisce nel primo argomento, ogni occorrenza della variabile V , con l'espressione data dal terzo.*

Dominio di costanti simboliche

Definizione 11. *Dominio di costanti simboliche*

1. È l'insieme $\mathbb{D}^{\mathcal{C}} = \mathcal{V} \rightarrow \mathcal{C}$ senza dipendenze cicliche
2. L'ordine parziale \sqsubseteq su $\mathbb{D}^{\mathcal{C}}$ è un ordinamento piatto.
3. Ogni elemento $S \in \mathbb{D}^{\mathcal{C}}$ rappresenta l'insieme degli ambienti compatibili con l'informazione simbolica:

$$\gamma(S) = \{ \sigma \in (\mathcal{V} \rightarrow \mathbb{D}) \mid \forall k, \sigma(V_k) \in \mathcal{A}[[S(V_k)]] \sigma \}$$

Correttezza della sostituzione

Teorema 4 (Correttezza della sostituzione).

$subst(exp, V, \sigma^\#(V))$ sovra approssima exp rispetto \sqsubseteq_σ :

$$\forall exp, \sigma^\#, V, \quad exp \sqsubseteq_\sigma subst(exp, V, \sigma^\#(V))$$

Definizione 12. $\mathcal{C} [[V \leftarrow e]] (S^\mathcal{C})(V_k) =$

$$\begin{cases} subst(e, V, S^\mathcal{C}(V)) & \text{se } V = V_k \\ subst(S^\mathcal{C}(V_k), V, S^\mathcal{C}(V)) & \text{se } V \neq V_k \end{cases}$$

Esempio

Esempio 5.

$$X \leftarrow [0, 5] \quad \sigma^\# = \{X \mapsto [0, 5]\}$$

$$T \leftarrow X \quad \sigma^\# = \{X \mapsto [0, 5], T \mapsto X\}$$

$$Y \leftarrow T - 2 \times X \quad \sigma^\# = \{X \mapsto [0, 5], T \mapsto X\}$$

$$Y \leftarrow X - 2 \times X \quad \sigma^\# = \{X \mapsto [0, 5], T \mapsto X\}$$

A questo punto $\mathbb{D}^{\mathcal{C}}$ si ferma, c'è bisogno di un altro dominio astratto per proseguire la computazione.

Strategie

- Sostituisci sempre
- Mai espressioni senza variabili
- Determinismo
- Ottenere maggior precisione

Sostituisci sempre, Solo le variabili

- Sostituisci sempre:
Grazie alla non ciclicità di $\mathbb{D}^{\mathcal{L}}$ possiamo sostituire $e \mapsto \text{subst}(e, V, S^{\mathcal{L}}(V))$ per ogni variabile V in qualunque ordine, senza temere che il processo non termini.
- Mai espressioni senza variabili:
Evitiamo le sostituzioni di espressioni libere da variabili. Impediamo così di perdere correlazioni tra le occorrenze delle variabili.

Determinismo e l'ottimo

- Dovremmo evitare sostituzioni tali per cui $|\llbracket S^{\mathcal{L}}(V) \rrbracket \circ \gamma| > 1$.
- Ottenere maggior precisione:
 1. Effettuiamo ogni sostituzione
 2. Analizziamo separatamente ogni risultato
 3. Intersechiamo \cap in $\mathbb{D}^{\#}$ i risultati.

Purtroppo però questa strategia ha un costo esponenziale sul numero di sostituzioni.

Integrazione con un dominio numerico

$\mathbb{D}^\#$ e $\mathbb{D}^\mathcal{C}$ sono indipendenti eccetto per ciò che riguarda il comando di assegnamento:

$$\mathcal{C} \llbracket V \leftarrow exp \rrbracket^{\# \times \mathcal{C}} (R^\#, S^\mathcal{C}) =$$

$$(\mathcal{C} \llbracket V \leftarrow subst(exp, V, S^\mathcal{C}) \rrbracket, \mathcal{C} \llbracket V \leftarrow e \rrbracket (S^\mathcal{C}))$$

Sfruttando una qualsiasi strategia di sostituzione per *subst* vista in precedenza.

Conclusione

Si comporta come una lazy-evaluation.

Vantaggi:

1. Tecniche semplici ed efficienti
2. Migliora domini astratti già presenti

Svantaggi:

1. Inutile con espressioni ben scritte.
2. Il prodotto tra due forme affini non è una forma affine

Lavori futuri

1. Tenderei ad abbandonare la forma affine.
2. Punterei alla semplificazione delle espressioni tramite l'algebra simbolica.
3. Analisi in real-time.