Università degli Studi di Verona

DIPARTIMENTO DI INFORMATICA

Analisi di Sistemi informatici

Riassunto dei principali argomenti

Autore:
Davide Bianchi

Anno Accademico 2017/2018

Indice

1 Introduzione

Argomenti contenuti:

- Interpretazione astratta
- Analisi statica
- Analisi dinamica

2 Preliminari matematici

2.1 Ordini parziali

2.2 Reticoli

2.3 Teoremi di punto fisso

3 Interpretazione astratta

3.1 Introduzione

Lo scopo è quello di trovare un'approssimazione di una semantica $\langle P \rangle$ di $[\![P]\!]$ tale per cui valgano:

- *correttezza:* $[\![P]\!] \subseteq \langle P \rangle$;
- *decidibilità:* $\langle P \rangle \subseteq Q$ è decidibile (Q è un insieme di semantiche che soddisfa la proprietà di interesse).

Se entrambe le proprietà sono soddisfatte, allora vale che

$$(\langle P \rangle \subseteq Q) \Rightarrow ([\![P]\!] \subseteq Q)$$

La semantica è data da una coppia $\langle D, f \rangle$ dove D è una coppia $\langle D, \leq_D$ rappresentante un dominio semantico e $f : D \to D$ è una funzione di trasferimento con una soluzione a punto fisso.

Dato un oggetto concreto, definiamo:

- un **oggetto astratto** come una rappresentazione matematica sovra-approssimata del corrispondente concreto;
- un **dominio astratto** come un insieme di oggetti astratti con delle operazioni astratte, che approssimano quelle concrete;
- una funzione di **astrazione** α che mappa oggetti concreti in oggetti astratti;
- una funzione di **concretizzazione** γ che mappa oggetti astratti in oggetti concreti.

La caratteristica peculiare delle astrazioni è che solo alcune proprietà vengono osservate con esattezza, le altre vengono solo approssimate. In sostanza, dato un dominio astratto A, gli elementi di A sono osservati con esattezza, gli altri sono approssimati o l'informazione è persa del tutto.

Proprietà. L'insieme delle proprietà $\mathcal{P}(\Sigma)$ di oggetti in Σ è l'insieme di elementi che gode di quella proprietà. Questo insieme di proprietà costituisce un reticolo completo

$$\langle \mathcal{P}(\Sigma), \subseteq, \emptyset, \cup, \cap, \neg \rangle$$

dove:

- $\subseteq$ è l'implicazione logica;
- Σ è `true`;
- $\cup$ è la disgiunzione (oggetti che godono di P o di Q appartengono a $P \cup Q$);
- $\cap$ è la congiunzione (oggetti che godono di P e di Q appartengono a $P \cap Q$);
- $\neg$ è la negazione (oggetti che non godono di P stanno in $\Sigma \setminus P$).

Direzione dell'astrazione. Quando si approssima una proprietà concreta $P \in \mathcal{P}(\Sigma)$ usando una proprietà astratta $\overline{P}$, deve essere stabilito un criterio per definire quando $\overline{P}$ è un'approssimazione di P.

Si distinguono quindi i seguenti casi:

- approssimazione *da sopra*: $P \subseteq \overline{P}$;
- approssimazione *da sotto*: $P \supseteq \overline{P}$.

Dato un oggetto o, si vuole quindi sapere se $o \in P$:

$$P \supseteq \overline{P} : \begin{cases} \text{"Si"} & o \in \overline{P} \\ \text{"Non lo so"} & o \notin \overline{P} \end{cases} \qquad P \subseteq \overline{P} : \begin{cases} \text{"No"} & o \notin \overline{P} \\ \text{"Non lo so"} & o \in \overline{P} \end{cases}$$

Migliore approssimazione. Definiamo come *migliore approssimazione* di una proprietà P in A il glb delle over-approximation di P in A, ossia:

$$\overline{P} = \bigcap \{\overline{P'} \in A | P \subseteq \overline{P'}\} \in A$$

3.2 Connessione di Galois

Imponiamo il vincolo che α e γ siano monotone, allora concludiamo che:

- $\gamma \circ \alpha : C \to C$ è **estensiva**: $\gamma(\alpha(c)) \geq c$;
- $\alpha \circ \gamma : A \to A$ è **riduttiva**: $\alpha(\gamma(a)) \leq a$.

Le definizioni qui sopra dicono rispettivamente che:

- α perde informazione, e γ non la può recuperare;
- γ non perde informazione.

Definizione 3.2.1. *Dati due poset $\langle A, \leq_A \rangle$ e $\langle C, \leq_C \rangle$, e due funzioni monotone $\alpha : C \to A$ e $\gamma : A \to C$, diciamo che $\langle C, \alpha, \gamma, A \rangle$ è una connessione di Galois se:*

- $\forall c \in \mathcal{C} : c \leq_C \gamma(\alpha(c))$
- $\forall a \in \mathcal{A} : \alpha(\gamma(a)) \leq_A a$

Se inoltre vale che $\forall a \in \mathcal{A} : \alpha(\gamma(a)) = a$, *allora* $\langle C, \alpha, \gamma, A\rangle$ *è un'inserzione di Galois.*

Una connessione e un'inserzione di Galois sono rappresentate rispettivamente come

$$C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} A \qquad C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} A$$

La funzione α è detta *aggiunta sinistra*, mentre la funzione γ è detta *aggiunta destra.*

Definizione 3.2.2. *Data una connessione di Galois* $C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} A$, *sono equivalenti:*

- $C \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} A$;
- α *è suriettiva;*
- γ *è iniettiva.*

Inoltre, dati due domini astratti, non esistono due coppie (α, γ) che formino una connessione di Galois; quindi la connessione di Galois tra due domini è **unica**, e le funzioni sono identificabili attraverso:

$$\alpha(c) = \bigwedge\{a \in A | c \leq_C \gamma(a)\}$$
$$\gamma(a) = \bigvee\{c \in C | \alpha(c) \leq_A a\}$$