

Modelli della concorrenza - Formulario

Alessandro Vasquez

November 9, 2016

Indice

1	Logica di Hoare	3
1.1	Correttezza parziale	3
1.1.1	Regole di derivazione primitive	3
1.1.2	Regole di derivazione ottenibili induttivamente	4
1.2	Correttezza totale	5
1.2.1	Definizioni e notazioni	5
1.2.2	Determinare la preconditione	6

1 Logica di Hoare

1.1 Correttezza parziale

1.1.1 Regole di derivazione primitive

Istruzione vuota Sia data una formula proposizionale α . Allora:

$$\frac{}{\{\alpha\} skip \{\alpha\}}$$

Assegnamento Sia data una formula proposizionale α , una variabile x e un'espressione E . Allora:

$$\frac{}{\{\alpha \left[\frac{E}{x} \right]\} x := E \{\alpha\}}$$

Conseguenza Siano date le formule proposizionali p , q , p_1 , q_1 e il programma P . Allora:

$$\frac{p_1 \rightarrow p \quad \{p\} P \{q\}}{\{p_1\} P \{q\}} \quad \frac{\{p\} P \{q\} \quad q \rightarrow q_1}{\{p\} P \{q_1\}}$$

Dalle ultime due deduzioni si ottiene induttivamente la seguente:

$$\frac{p_1 \rightarrow p \quad \{p\} P \{q\} \quad q \rightarrow q_1}{\{p_1\} P \{q_1\}}$$

Sequenza Siano date le formule proposizionali p , q , r e le istruzioni C_1 , C_2 . Allora:

$$\frac{\{p\} C_1 \{q\} \quad \{q\} C_2 \{r\}}{\{p\} C_1 ; C_2 \{r\}}$$

La regola di sequenza è utile nei cicli il cui corpo presenta istruzioni diverse che coinvolgono le stesse variabili.

Iterazione Siano dati un ciclo iterativo, la relativa condizione B , una sua invariante i , e il corpo del ciclo C . Allora:

$$\frac{\{i \wedge B\} C \{i\}}{\{i\} \text{ while } B \text{ do } C \text{ od } \{i \wedge \neg B\}}$$

1.1.2 Regole di derivazione ottenibili induttivamente

Siano date le formule proposizionali p , q , r e il programma P . Allora:

$$\frac{\{p\} P \{q\} \quad \{r\} P \{q\}}{\{p \vee r\} P \{q\}}$$

Nel caso in cui $r = \neg p$, la preconditione nella conclusione della deduzione diventa una tautologia:

$$\frac{\{p\} P \{q\} \quad \{\neg p\} P \{q\}}{\{p \vee \neg p\} P \{q\}}$$

Controllo di flusso Siano date le formule proposizionali p , q . Siano dati inoltre una condizione B , un blocco P (eseguito solo se B è verificata) e un blocco Q (eseguito altrimenti). Sia infine R il blocco che include l'istruzione di controllo su B e i blocchi P e Q . Vale la seguente deduzione:

$$\frac{\{p \wedge B\} P \{q\} \quad \{p \wedge \neg B\} Q \{q\}}{\{p\} R \{q\}}$$

1.2 Correttezza totale

Si vuole verificare la terminazione di un programma dato. La non-terminazione può avvenire solo in presenza di cicli: ci si concentrerà sullo studio di programmi iterativi. Si supponga di avere un programma P che presenta un ciclo while W il cui corpo è denotato con C .

Si supponga di aver determinato un invariante i del ciclo. Dimostrare che il P termina significa determinare una espressione E e un invariante p , indipendente da E e da i , tali che:

1. $p \rightarrow E \geq 0$
2. $\vdash_p \{p \wedge B \wedge E = K\} C \{E < K\}$

1.2.1 Definizioni e notazioni

Definizione 1.1. Sia V l'insieme delle variabili di un programma P . Uno stato σ di P è una funzione

$$\sigma : V \rightarrow \mathbb{Z}.$$

Definizione 1.2. L'insieme di tutti gli stati di un programma è l'insieme:

$$\Sigma\{\sigma : V \rightarrow \mathbb{Z}\}.$$

Definizione 1.3. L'insieme di tutte le formule proposizionali costruite a partire da V di chiama Π .

Dati $\sigma \in \Sigma$ e $p \in \Pi$, si dirà che la formula p è valida nello stato σ usando la notazione

$$\sigma \models p.$$

Definizione 1.4. L'insieme di tutte le possibili asserzioni vere per lo stato σ è l'insieme

$$t(\sigma) = \{p \in \Pi : \sigma \models p\}.$$

Definizione 1.5. L'insieme degli stati che rendono vera la formula p è l'insieme

$$m(p) = \{\sigma \in \Sigma : \sigma \models p\}.$$

Tale insieme è definito come l'estensione della formula p .

Lemma 1.1. Siano $S \subseteq \Sigma$ e $F \subseteq \Pi$. Allora

$$t(S) = \{p \in \Pi : \forall s \in S : s \models p\} = \bigcap_{s \in S} t(s),$$

$$m(F) = \{\sigma \in \Sigma : \forall p \in F : \sigma \models p\} = \bigcap_{p \in F} m(p).$$

Lemma 1.2. Siano $A, B \subseteq \Sigma$ tali che $A \subseteq B$. Allora

$$t(A) \supseteq t(B).$$

Lemma 1.3. Siano $A, B \in \Pi$ tali che $A \subseteq B$. Allora

$$m(A) \supseteq m(B).$$

Lemma 1.4. Siano p, q formule proposizionali. Grazie alla definizione ricorsiva di formula proposizionale, valgono le seguenti proprietà:

- $m(\neg p) = \Sigma \setminus m(p)$
- $m(p \vee q) = m(p) \cup m(q)$
- $m(p \wedge q) = m(p) \cap m(q)$
- $m(p \rightarrow q) = (\Sigma \setminus m(p)) \cup m(q)$

in cui l'ultima uguaglianza è data dal fatto che $p \rightarrow q \equiv \neg p \vee q$ ¹.

1.2.2 Determinare la preconditione

Si supponga di avere una tripla di Hoare priva della preconditione: $P\{q\}$. Si rende necessario trovare un metodo per determinarne la preconditione. Tramite l'assioma dell'assegnamento è possibile ottenere la preconditione più debole possibile.

Esempio 1.1. Si supponga di avere la seguente tupla:

$$C_1; C_2\{q\}.$$

Tramite l'assioma dell'assegnamento posso ottenere la tripla

$$\vdash \{wp(C_2, q)\} C_2 \{q\}$$
².

Applicando gli assiomi di assegnamento e di sequenza, ottengo la tripla

$$\{wp(C_1, wp(C_2, q))\} C_1; C_2 \{q\},$$

che è la più debole preconditione della tupla iniziale.

¹Si veda la definizione di β -formula.

²wp = weakest precondition