Esercizi

1. È vera la formula

$$\{\textbf{true}\}\ u := t\ \{u = t\}\ ?$$

2. È vera la formula

$$\{\forall x.x = 1\}\ x := 2\ \{\forall x.x = 1\}\ ?$$

3. Dimostrare che il seguente assioma per l'assegnamento **forward**

$$\{p\}\ u := t\ \{\exists y :\ (p[u := y]\ \wedge\ u = t[u := y])\}$$

   - è vero;
   - può essere derivato in *PD*;
   - l'assioma di assegnamento backward può essere derivato dall'assioma forward utilizzando la regola di conseguenza logica.

Completezza

Definizione.
Sia G unsistema formale per derivare formule per la correttezza di programmi in C.

- G è **completo** rispetto alla **correttezza parziale** di programmi se

$$\models \{p\}\ S\{q\} \implies \vdash_G \{p\}\ S\{q\}$$

- G è **completo** rispetto alla **correttezza totale** di programmi se

$$\models_{tot} \{p\}\ S\{q\} \implies \vdash_G \{p\}\ S\{q\}$$

I sistemi PD e TD sono completi?

- Per il teorema di Incompletezza di Gödel, non esiste un sistema completo per le asserzioni della regola di coseguenza. Per evitare questa forma di incompletezza, estendiamo i sistemi *PD* e *TD* con tutte le asserzioni vere.

- Il linguaggio per le asserzioni e le espressioni è sufficiente per descrivere tutti gli stati e le funzioni di complessità che servono nelle dimostrazioni di correttezza?
  Si, per gli stati.
  Per le funzioni di complessità serve estendere il linguaggio.

- Una volta esteso il sistema PD/TD con le asserzioni vere ed esteso il linguaggio delle asserzioni per catturare tutte le funzioni di complessità, il sistema PD/TD cattura tutte le formule vere?
  Si.

Analisi dell'espressività di asserzioni ed espressioni

Weakest (Liberal) Precondition

Definition.

- **Weakest liberal precondition**:

$$wlp(S, \Phi) = \{\sigma \mid \mathcal{M}[\![S]\!](\sigma) \subseteq \Phi\} \ .$$

- **Weakest precondition**:

$$wp(S, \Phi) = \{\sigma \mid \mathcal{M}_{tot}[\![S]\!](\sigma) \subseteq \Phi\} \ .$$

Definibilità

Teorema.
Per ogni S, q:

- esiste p tale che $[\![p]\!] = wlp(S, [\![q]\!])$;

- esiste p tale che $[\![p]\!] = wp(S, [\![q]\!])$.

Completezza di PD

Lemma.

1. $wlp(skip, q) \leftrightarrow q$

2. $wlp(u := t, q)) \leftrightarrow q[u := t]$

3. $wlp(S_1; S_2, q) \leftrightarrow wlp(S_1, wlp(S_2, q))$

4. $wlp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow (B \wedge wlp(S_1, q)) \ \vee \ (\neg B \wedge wlp(S_2, q))$

5. $wlp(S, q) \wedge B \rightarrow wlp(S_1, wlp(S, q))$,
   where $S \equiv \textbf{while } B \textbf{ do } S_1 \textbf{ od}$

6. $wlp(S, q) \wedge \neg B \rightarrow q$,
   where $S \equiv \textbf{while } B \textbf{ do } S_1 \textbf{ od}$

7. $\models \{p\} \ S \ \{q\}$ sse $p \rightarrow wlp(S, q)$.

Completezza di PD

Teorema.
Il sistema *PD* è completo rispetto alla correttezza parziale, cioè:

$$\models \{p\}\ S\{q\} \implies \vdash_{PD} \{p\}\ S\ \{q\}\ .$$

Completezza di TD

Esprimibilità delle funzioni di complessità

Definizione.
Sia $S \equiv$ **while** B **do** S_1 **od** e sia x una variabile intera non in S. Definiamo

$$S_x \equiv x := 0;\ \textbf{while}\ B\ \textbf{do}\ x := x + 1;\ S_1\ \textbf{od}\ .$$

Sia σ tale che $\mathcal{M}_{tot}[\![S]\!](\sigma) \neq \{\perp\}$. Allora $\mathcal{M}_{tot}[\![S_x]\!](\sigma) \neq \{\tau\}$, $\tau \neq \perp$. Definiamo il numero di iterazioni di S a partire da σ

$$iter(S, \sigma) = \tau(x)\ .$$

$iter(S, \sigma)$ è una funzione parziale in σ **computabile**.

Definizione.
L'insieme delle espressioni intere è **espressivo** se per ogni programma **while** S esiste un'espressione intera t tale che, per ogni σ tale che $\mathcal{M}_{tot}[\![S]\!](\sigma) \neq \{\perp\}$,

$$\sigma(t) = iter(s, \sigma)\ .$$

Il linguaggio per le espressioni intere comprendente gli operatori $+$, $\cdot$ permette di rappresentare solo espressioni polinomiali. Ma esistono programmi **while** per i quali il numero di iterazioni è esponenziale.

Per poter rappresentare la funzione $iter(s, \sigma)$ è necessario estendere il linguaggio delle espressioni con tutte le funzioni computabili parziali.

Lemma.

1. $wp(skip, q) \leftrightarrow q$

2. $wp(u := t, q)) \leftrightarrow q[u := t]$

3. $wp(S_1; S_2, q) \leftrightarrow wp(S_1, wp(S_2, q))$

4. $wp(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}, q) \leftrightarrow (B \wedge wp(S_1, q)) \ \vee \ (\neg B \wedge wp(S_2, q))$

5. $wp(S, q) \wedge B \rightarrow wp(S_1, wp(S, q))$,
   where $S \equiv \textbf{while } B \textbf{ do } S_1 \textbf{ od}$

6. $wp(S, q) \wedge \neg B \rightarrow q$,
   where $S \equiv \textbf{while } B \textbf{ do } S_1 \textbf{ od}$

7. $\models_{tot} \{p\} \ S \ \{q\}$ sse $p \rightarrow wp(S, q)$.

Completezza di TD

Teorema.
Il sistema TD è completo rispetto alla correttezza totale, cioè:

$$\models_{tot} \{p\}\ S\{q\} \implies \vdash_{TD} \{p\}\ S\ \{q\}\ .$$