Exercício 2 da Ficha 4

Relembre a questão da Ficha 1 em que se estendia a linguagem **While** com ciclos *for*:

$$\mathbf{Stm} \ni C ::= \ \ldots \ \mid \ \texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2$$

com a seguinte semântica informal

> *O comando C_1 é executado; em seguida, a expressão booleana b é testada, e caso seja verdadeira é executada uma iteração de C_2, seguida de C_3, seguida de novo teste de b; enquanto b for verdadeiro são executadas iterações de C_2 seguido de C_3; se b for falso termina a execução.*

1. Escreva uma ou mais regras da lógica de Hoare para esta forma de ciclo.
2. Prove a correcção das regras que escreveu usando os seguintes métodos (alternativos)
   (a) directamente utilizando a noção de *regra derivada* na lógica de Hoare, tendo em conta a equivalência provada na Ficha 1

   $$\texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2 \qquad \text{e} \qquad C_1;\ \texttt{while}\ b\ \texttt{do}\ \{C_2\ ;\ C_3\}$$

   (b) utilizando as regras de semântica operacional que definiu para estes ciclos

Resolução

1. Uma regra possível é a seguinte

$$\frac{\{\phi\}\,C_1\,\{\theta\} \qquad \{\theta \wedge b\}\,C_2; C_3\,\{\theta\}}{\{\phi\}\,\texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2\,\{\theta \wedge \neg b\}}$$

2. (a). A regra acima é correcta se a validade das premissas da regra implicar a validade da sua conclusão. Vamos então assumir que

$$\models \{\phi\}\,C_1\,\{\theta\} \tag{1}$$

$$\models \{\theta \wedge b\}\,C_2; C_3\,\{\theta\} \tag{2}$$

tendo por objectivo provar que $\models \{\phi\}\,\texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2\,\{\theta \wedge \neg b\}$.

A equivalência semântica, que vimos na Ficha 1, garante que para todo o $s, s' \in \mathbf{State}$,

$$\langle \texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2, s\rangle \to s' \quad \text{sse} \quad \langle C_1;\ \texttt{while}\ b\ \texttt{do}\ \{C_2\ ;\ C_3\}, s\rangle \to s' \tag{3}$$

Por outro lado, podemos construir a seguinte árvore de derivação

$$\frac{\{\phi\}\,C_1\,\{\theta\} \qquad \dfrac{\{\theta \wedge b\}\,C_2; C_3\,\{\theta\}}{\{\phi\}\,\texttt{while}\ b\ \texttt{do}\ (C_2; C_3)\,\{\theta \wedge \neg b\}}}{\{\phi\}\,C_1;\ \texttt{while}\ b\ \texttt{do}\ (C_2; C_3)\,\{\theta \wedge \neg b\}}$$

Ou seja, podemos derivar a seguinte regra

$$\frac{\{\phi\}\,C_1\,\{\theta\} \qquad \{\theta \wedge b\}\,C_2; C_3\,\{\theta\}}{\{\phi\}\,C_1;\ \texttt{while}\ b\ \texttt{do}\ (C_2; C_3)\,\{\theta \wedge \neg b\}}$$

que é necessáriamente correcta, porque o sistema de inferência da lógica de Hoare é correcto. Logo, com base em (1) e (2), podemos concluir que

$$\models \{\phi\}\,C_1;\ \texttt{while}\ b\ \texttt{do}\ (C_2; C_3)\,\{\theta \wedge \neg b\}$$

e daqui por (3) que

$$\models \{\phi\}\,\texttt{for}\ (C_1; b\,; C_3)\ \texttt{do}\ C_2\,\{\theta \wedge \neg b\}.$$