Verificação Formal de Software
Quarto Trabalho Prático

1. Considera a linguagem **While** com extensões e as regras para a lógica de Hoare de asserções de correcção parcial. Para cada uma das asserções abaixo:

   1) deduz a asserção usando *tableaux* e indicando qual a regra usada em cada passo
   2) indica em cada passo quais as condições de verificação associadas

   (a) $\{\top\}\texttt{if } x > 0 \texttt{ then } y := x \texttt{ else } y := -x \ \{y = abs(x)\}$.

   (b) $\{a[x] = x \ \wedge \ a[y] = y\} \ r := a[x]; \ a[x] := a[y]; \ a[y] := r \ \{a[x] = y \ \wedge \ a[y] = x\}$.

2. Considera a linguagem **While** e as regras para a lógica de Hoare de asserções de correcção total. Deduz as seguintes asserções usando precondições fracas e *tableaux*. Indica os variantes e invariantes utilizados.

   (a) $\{x \geq 0\}z := x; y := 0, \ \texttt{while } \neg z = 0 \texttt{ do } (y := y + 1; z := z - 1)\{x = y\}$.

   (b) $\{y = y_0 \ \wedge \ y \geq 0\} \ z := 1; \ \texttt{while } \neg y = 0 \texttt{ do } (z := z \times x; y := y - 1)\{z = x^{y_0}\}$, onde y_0 é o valor inicial de y.

3. Considera o comando $\texttt{repeat } C \texttt{ until } B$, cuja semântica natural é dada pelas seguintes regras:

$$\frac{\langle C, s\rangle \ \rightarrow \ s'}{\langle \texttt{repeat } C \texttt{ until } B, s\rangle \ \rightarrow \ s'} \text{ se } \mathcal{B}[\![B]\!]s' = \mathrm{V}$$

$$\frac{\langle C, s\rangle \ \rightarrow \ s', \ \langle \texttt{repeat } C \texttt{ until } B, s'\rangle \ \rightarrow \ s''}{\langle \texttt{repeat } C \texttt{ until } B, s\rangle \ \rightarrow \ s''} \text{ se } \mathcal{B}[\![B]\!]s' = \mathrm{F}$$

   (a) Escreve uma regra de Hoare para o comando `repeat`.

   (b) Considera a demonstração de integridade para a lógica de Hoare, apresentada na aula. Completa a demonstração para incluir a regra de Hoare definida na alínea anterior.

4. Deriva a seguinte regra alternativa para o comando `if` na lógica de Hoare:

$$\frac{\{\phi_t\}C_t\{\psi\}, \qquad \{\phi_f\}C_f\{\psi\}}{\{\phi\}\texttt{if } B \texttt{ then } C_t \texttt{ else } C_f\{\psi\}} \text{ se } \phi \rightarrow (B \rightarrow \phi_t) \wedge (\neg B \rightarrow \phi_f)$$