`tableaux` for partial correctness

Let $C = C_1; C_2; \ldots; C_n$ and we want $\vdash_p \{\varphi\}C\{\psi\}$. We can consider several problems of the form $\vdash_p \{\varphi_i\}C_i\{\varphi_{i+1}\}$, with $\varphi = \varphi_0$ and $\psi = \varphi_n$. For that we annotate the commands that compose C with formulae φ_i and consider a proof `tableaux` :

$$\begin{array}{ll}
\{\varphi_0\} & \\
C_1; & \\
\{\varphi_1\} & \text{justification} \\
C_2; & \\
\vdots & \\
\{\varphi_{n-1}\} & \text{justification} \\
C_n & \\
\{\varphi_n\} &
\end{array}$$

Then we need to show

$$\vdash_p \{\varphi_i\}C_{i+1}\{\varphi_{i+1}\},$$

starting with φ_n. But how to obtain φ_i?

Weakest preconditions (wp)

For each command C and postcondition ψ a formula $wp(C,\psi)$ is the weakest precondition that being true in state s, ensures that in the state s' obtained after the execution of C and if C stops, the postcondition ψ holds.

- $\models_p \{wp(C,\psi)\}C\{\psi\}$
- $\models_p \{\varphi\}C\{\psi\}$ implies $\varphi \to wp(C,\psi)$ (called verification condition)

`tableaux` for partial correctness

- a formula φ_i obtained from C_{i+1} and φ_{i+1} is the *weakest precondition* of C_{i+1}
- given the postcondition φ_{i+1}, we can write

  $$wp(C_{i+1}, \varphi_{i+1}) = \varphi_i.$$

- From $wp()$ and using the consequence rule ($cons_p$) we can automatically generate the verification conditions,
- that can be proved automatically or assisted by a solver.
- In general if $\{\varphi\}C\{\psi\}$ the verification condition is:

  $$\varphi \to wp(C,\psi)$$

Weakest preconditions - ass_p

Assignment

$$\begin{array}{ll} \{\psi[E/x]\} & \\ x \leftarrow E & \\ \{\psi\} & \qquad ass_p \end{array}$$

A verification condition for $\{\varphi\}x \leftarrow E\{\psi\}$, is

$$\varphi \to \psi[E/x]$$

and $wp(x \leftarrow E, \psi) = \psi[E/x]$.

Exemp. 2.1. *Compute*

1. $wp(x \leftarrow 0, x = 0)$ *is* $0 = 0$.
2. $wp(x \leftarrow x + 1, x > 0)$ *is* $x + 1 > 0$.

Weakest preconditions - $cons_p$

Consequence

The rule $cons_p$ can be applied when $\varphi' \to \varphi$ and we have $\{\varphi\}\, C\, \{\psi\}$. In this case the *tableaux* can have two formulas in a row: φ' and below φ.

$$\begin{array}{ll} \{\varphi'\} & \\ \{\varphi\} & \qquad cons_p \end{array}$$

Exerc. 2.1. *Show with a* tableaux $\vdash_p \{y = 5\}x \leftarrow y + 1\{x = 6\}$. $\diamond$

Weakest preconditions if_p

Conditional

We want φ such that $wp(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi) = \varphi$.

$$\begin{array}{ll}
\{(B \to \varphi_1) \ \land \ (\neg B \to \varphi_2)\} & \\
\texttt{if}\, B\, \texttt{then} & \\
\quad \{\varphi_1\} & \\
\quad C_1 & \\
\quad \{\psi\} & \qquad if_p \\
\texttt{else} & \\
\quad \{\varphi_2\} & \\
\quad C_2 & \\
\quad \{\psi\} & \\
\{\psi\} & \qquad if_p
\end{array}$$

We can compute $\{\varphi_1\}C_1\{\psi\}$ e $\{\varphi_2\}C_2\{\psi\}$, and then $\varphi \equiv (B \to \varphi_1) \ \land \ (\neg B \to \varphi_2)$, i.e.,

$$wp(\texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2, \psi) = (B \to \varphi_1) \ \land \ (\neg B \to \varphi_2)$$

and the verification conditions are the ones generated by φ_1 and φ_2.

Exemp. 2.2. *Show with a* tableaux

$$\begin{array}{l}
\vdash_p \{\mathsf{true}\} \\
a \leftarrow x + 1; \\
\texttt{if}\, a - 1 = 0\, \texttt{then} \\
y \leftarrow 1 \\
\texttt{else} \\
y \leftarrow a \\
\{y = x + 1\}
\end{array}$$

$$\begin{array}{ll}
\{\mathsf{true}\} & \\
\{(x = 0 \to 1 = 1) \ \land \ (\neg(x = 0) \to x + 1 = x + 1)\} & cons_p \\
\{(x + 1 - 1 = 0 \to 1 = x + 1) \ \land \ (\neg(x + 1 - 1 = 0) \to x + 1 = x + 1)\} & cons_p \\
a \leftarrow x + 1 & \\
\{(a - 1 = 0 \to 1 = x + 1) \ \land \ (\neg(a - 1 = 0) \to a = x + 1)\} & ass_p \\
\texttt{if}\, a - 1 = 0\, \texttt{then} & \\
\{1 = x + 1\} \qquad\qquad if'_p & \\
y \leftarrow 1 & \\
\{y = x + 1\} \qquad\qquad ass_p & \\
\texttt{else} & \\
\{a = x + 1\} \qquad\qquad if'_p & \\
y \leftarrow a & \\
\{y = x + 1\} \qquad\qquad ass_p &
\end{array}$$

We use the following inference rule:

$[if'_p\ ]$

$$\frac{\{\varphi_1\}\, C_1\, \{\psi\} \qquad \{\varphi_2\}\, C_2\, \{\psi\}}{\{(B \to \varphi_1)\ \wedge\ (\neg B \to \varphi_2)\}\, \texttt{if}\, B\, \texttt{then}\, C_1\, \texttt{else}\, C_2\, \{\psi\}}$$

Exerc. 2.2. *Show that this rule can be deduced from the inference system* $\mathcal{H}$ $\diamond$

Weakest preconditions - $while_p$

We want $\vdash_p \{\varphi\}\texttt{while}\, B\, \texttt{do}\, C\, \{\psi\}$.
To use $while_p$ rule we need a formula η such that:

- $\varphi \to \eta$
- $\eta\ \wedge\ \neg B \to \psi$ e
- $\vdash_p \{\eta\}\texttt{while}\, B\, \texttt{do}\, C\{\eta\ \wedge\ \neg B\}$

Invariant

One invariant of the cycle $\texttt{while}\, B\, \texttt{do}\, C$ is a formula η such that

$$\models_p \{\eta\ \wedge\ B\}C\{\eta\}.$$

Weakest preconditions - $while_p$

$$\begin{array}{lll}
\{\varphi\} & & \\
\{\eta\} & & \\
\texttt{while}\, B\, \texttt{do} & & \\
\quad \{\eta\ \wedge\ B\} & & \\
\quad C & & \\
\quad \{\eta\} & & \\
\{\eta\ \wedge\ \neg B\} & & while_p \\
\{\psi\} & cons_p &
\end{array}$$

We have that $wp(\texttt{while}\, B\, \texttt{do}\, C, \psi) = \eta$, the verification conditions are $\varphi \to \eta$, $\eta\ \wedge\ \neg B \to \psi$ and the verification conditions of $\{\eta\ \wedge\ B\}C\{\eta\}$.

Exemp. 2.3. *Show that*

$$\vdash_p \{\textsf{true}\}y \leftarrow 1; z \leftarrow 0; \texttt{while}\ \neg z\ =\ x\ do\ (z \leftarrow z+1; y \leftarrow y \times z)\{y = x!\}$$

The invariant I is : $y = z!$ and verifies the conditions: Is implied by the precondition of `while` which is $y = 1 \wedge z = 0$:

$y \leftarrow 1$
$z \leftarrow 0$
$\{y = z!\}$?
$\texttt{while}\, \neg z = x\, \texttt{do}$
$\quad \{y = z! \wedge \neg z = x\}$
$\quad \{y \times (z+1) = (z+1)!\}$ $cons_p$
$\quad z = z + 1$
$\quad \{y \times z = z!\}$ ass_p
$\quad y = y \times z$
$\quad \{y = z!\}$ ass_p
$\{y = x!\}$?

because $(y = z! \wedge \neg z = x) \rightarrow y = z! \rightarrow y \times (z+1) = (z+1)!$.

$\{\mathsf{true}\}$
$\{1 = 0!\}$ $cons_p$
$y \leftarrow 1$
$\{y = 0!\}$ ass_p
$z \leftarrow 0$
$\{y = z!\}$ ass_p
$\texttt{while}\, \neg z = x\, \texttt{do}$
$\quad \{y = z! \wedge \neg z = x\}$
$\quad \{y \times (z+1) = (z+1)!\}$ $cons_p$
$\quad z \leftarrow z + 1$
$\quad \{y \times z = z!\}$ ass_p
$\quad y \leftarrow y \times z$
$\quad \{y = z!\}$ ass_p
$\{y = z! \wedge z = x\}$ $while_p$
$\{y = x!\}$ $cons_p$

Exerc. 2.3. *Show that*

$$
\begin{aligned}
&\vdash_p \{\mathsf{true}\} \\
&r \leftarrow x; q \leftarrow 0; \\
&\texttt{while}\, y \leq r\, \texttt{do} \\
&\quad r \leftarrow r - y; \\
&\quad q \leftarrow q + 1 \\
&\{r < y \ \wedge \ x = r + (y \times q)\}
\end{aligned}
$$

◇

The condition $x = r + (y \times q)$ is the invariant.

Exerc. 2.4. *Show that*

$\{x \geq 0\} z \leftarrow x; y \leftarrow 0;$ `while` $\neg z = 0$ `do` $(y \leftarrow y + 1; z \leftarrow z - 1)\{x = y\}$.

◇