$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\, C \,\}\ \texttt{B}\ \{\, sp(B,C) \,\}}\ \text{sp}}{\{\, H_{B,P} \wedge C \,\}\ \texttt{B}\ \{\, sp(B,C) \wedge H_{B,P} \,\}}\ \text{constancy}}{\{\, H_{B,P} \wedge C \,\}\ \texttt{B}\ \{\, H_{B,P} \,\}}\ \text{conseq}}{\{\, H_{B,P} \,\}\ \texttt{while C do B}\ \{\, H_{B,P} \wedge \neg C \,\}}\ \text{while}$$
$$\dfrac{\{\, H_{B,P} \,\}\ \texttt{while C do B}\ \{\, H_{B,P} \wedge \neg C \,\}}{\{\, P \,\}\ \texttt{while C do B}\ \{\, H_{B,P} \wedge \neg C \,\}}\ \text{conseq}$$

Fig. 1: Hoare-style proof for the havoc abstraction

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\{\, C \,\}\ \texttt{B}\ \{\, sp(B,C) \,\}}\ \text{sp}}{\{\, H_{B,P} \wedge C \,\}\ \texttt{B}\ \{\, sp(B,C) \wedge H_{B,P} \,\}}\ \text{constancy}}{(\{\, (sp(B,C) \vee P) \wedge H_{B,P} \wedge C \,\}\ \texttt{B}\ \{\, sp(B,C) \wedge H_{B,P} \,\}}\ \text{conseq}}{(\{\, (sp(B,C) \wedge H_{B,P}) \vee P \wedge C \,\}\ \texttt{B}\ \{\, sp(B,C) \wedge H_{B,P} \,\}}\ \text{equiv}}{(\{\, sp(B, C \wedge H_{B,P}) \vee P \wedge C \,\}\ \texttt{B}\ \{\, sp(B, C \wedge H_{B,P}) \,\}}\ \text{constancy(of sp)}}{(\{\, sp(B, C \wedge H_{B,P}) \vee P \wedge C \,\}\ \texttt{B}\ \{\, sp(B, C \wedge H_{B,P}) \vee P \,\}}\ \text{conseq}}{\{\, sp(B, C \wedge H_{B,P}) \vee P \,\}\ \texttt{while C do B}\ \{\, (sp(B, C \wedge H_{B,P}) \vee P) \wedge \neg C \,\}}\ \text{while}$$
$$\dfrac{\{\, sp(B, C \wedge H_{B,P}) \vee P \,\}\ \texttt{while C do B}\ \{\, (sp(B, C \wedge H_{B,P}) \vee P) \wedge \neg C \,\}}{\{\, P \,\}\ \texttt{while C do B}\ \{\, (sp(B, C \wedge H_{B,P}) \vee P) \wedge \neg C \,\}}\ \text{conseq}$$

Fig. 2: Hoare-style proof for naive loop abstraction

The Hoare-style proof for the havoc abstraction is shown in Fig. 1. Formally $H_{B,P}$ is derived from P by existential quantification over all variables from the set $mod(\texttt{B})$ that contains all variables that are modified in the loop body B. This allows us to use it with the rule of constancy in the second step because $free(H_{B,P}) \cap mod(\texttt{B}) = \emptyset$. [1] Since $H_{B,P}$ implies P, we can use the rule of consequence in the last step.

The proof for naive abstraction is shown in Fig. 2.

[1] Since we use the rule of constancy, we need to require that there is no aliasing (e.g. via pointers) in loop body. In the presence of aliasing, we would need to generalize the proof e.g. by using separation logic and the frame rule instead.