02141 Computer Science Modeling
Solutions to Selected Exercises from Formal Methods Appetizer, Chapter 4

Exercise 4.16 *Solution:* We first specify $\widehat{\mathcal{B}}\llbracket b \rrbracket$ as follows:

$$
\begin{array}{lcl}
\widehat{\mathcal{B}}\llbracket \texttt{true} \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2) & = & \{\mathsf{tt}\} \\
\widehat{\mathcal{B}}\llbracket \neg b \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2) & = & \{\widehat{\neg} s \mid s \in \widehat{\mathcal{B}}\llbracket b \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2)\} \\
\widehat{\mathcal{B}}\llbracket b_1 \wedge b_2 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2) & = & \{s_1 \mathbin{\widehat{\wedge}} s_2 \mid s_1 \in \widehat{\mathcal{B}}\llbracket b_1 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2), s_2 \in \widehat{\mathcal{B}}\llbracket b_2 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2)\} \\
\widehat{\mathcal{B}}\llbracket a_1 \ op \ a_2 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2) & = & \{s_3 \in s_1 \ \widehat{op} \ s_2 \mid s_1 \in \widehat{\mathcal{A}}\llbracket a_1 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2), s_2 \in \widehat{\mathcal{A}}\llbracket a_2 \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2)\}
\end{array}
$$

where $op \in \{=, >, \geq\}$ and

$\widehat{\neg}$	
tt	ff
ff	tt

$\widehat{\wedge}$	tt	ff
tt	tt	ff
ff	ff	ff

$\widehat{=}$	$-$	0	$+$
$-$	{tt, ff}	{ff}	{ff}
0	{ff}	{tt}	{ff}
$+$	{ff}	{ff}	{tt, ff}

$\widehat{>}$	$-$	0	$+$
$-$	{tt, ff}	{ff}	{ff}
0	{tt}	{ff}	{ff}
$+$	{tt}	{tt}	{tt, ff}

$\widehat{\geq}$	$-$	0	$+$
$-$	{tt, ff}	{ff}	{ff}
0	{tt}	{tt}	{ff}
$+$	{tt}	{tt}	{tt, ff}

Then we prove the statement $\mathcal{B}\llbracket b \rrbracket\sigma \in \widehat{\mathcal{B}}\llbracket b \rrbracket(\eta(\sigma))$ by structural induction on b:

- Case $\texttt{true}$: Then $\mathcal{B}\llbracket \texttt{true} \rrbracket\sigma = \mathsf{tt} \in \{\mathsf{tt}\} = \widehat{\mathcal{B}}\llbracket \texttt{true} \rrbracket(\eta(\sigma))$.

- Case $\neg b'$: We assume the induction hypothesis that $\mathcal{B}\llbracket b' \rrbracket\sigma \in \widehat{\mathcal{B}}\llbracket b' \rrbracket(\eta(\sigma))$. The conclusion then follows by a case analysis on $\mathcal{B}\llbracket b' \rrbracket\sigma$: If $\mathcal{B}\llbracket b' \rrbracket\sigma = \mathsf{tt}$ then $\mathcal{B}\llbracket \neg b' \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2) = \mathsf{ff} \in \{\widehat{\neg} s \mid s \in \widehat{\mathcal{B}}\llbracket b' \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2)\} = \widehat{\mathcal{B}}\llbracket \neg b' \rrbracket(\hat{\sigma}_1, \hat{\sigma}_2)$. We can make a similar argument in the case where $\mathcal{B}\llbracket b' \rrbracket\sigma = \mathsf{ff}$.

- Case $b_1 \wedge b_2$: We assume the induction hypothesis that $\mathcal{B}\llbracket b_1 \rrbracket\sigma \in \widehat{\mathcal{B}}\llbracket b_1 \rrbracket(\eta(\sigma))$ and $\mathcal{B}\llbracket b_2 \rrbracket\sigma \in \widehat{\mathcal{B}}\llbracket b_2 \rrbracket(\eta(\sigma))$. Again, the conclusion follows by a case analysis on $\mathcal{B}\llbracket b_1 \rrbracket\sigma$ and $\mathcal{B}\llbracket b_2 \rrbracket\sigma$.

- Case $a_1 \ op \ a_2$: For this case we first use the result of Exercise 4.14 to establish that $\mathsf{sign}(\mathcal{A}\llbracket a_1 \rrbracket\sigma) \in \widehat{\mathcal{A}}\llbracket a_1 \rrbracket(\eta(\sigma))$ and $\mathsf{sign}(\mathcal{A}\llbracket a_2 \rrbracket\sigma) \in \widehat{\mathcal{A}}\llbracket a_2 \rrbracket(\eta(\sigma))$. Finally, we conclude the proof by a case analysis on $\mathsf{sign}(\mathcal{A}\llbracket a_1 \rrbracket\sigma)$, $\mathsf{sign}(\mathcal{A}\llbracket a_2 \rrbracket\sigma)$, and op.