

FIT3013 Formal Specification in Software Engineering
Semester 1 2009
Event-B Exercises 2
Machines

1. In the **SimpleLibrary** machine, we have three variables

$$\begin{aligned} \text{books_in_library} &\subseteq \text{BOOK} \\ \text{books_on_shelf} &\subseteq \text{books_in_library} \\ \text{books_on_loan} &\in \text{books_in_library} \leftrightarrow \text{users} \end{aligned}$$

We want books_on_shelf and $\text{dom}(\text{books_on_loan})$ to *partition* the set books_in_library . Normally, we would specify this by:

$$\begin{aligned} \text{dom}(\text{books_on_loan}) \cup \text{books_on_shelf} &= \text{books_in_library} \wedge \\ \text{dom}(\text{books_on_loan}) \cap \text{books_on_shelf} &= \{\} \end{aligned}$$

but it was specified by

$$\text{dom}(\text{books_on_loan}) = \text{books_in_library} - \text{books_on_shelf}$$

- (a) Show that the former follows from the latter.

Answer: By forming the union with books_on_shelf on both sides of the above equation, we get:

$$\text{dom}(\text{books_on_loan}) \cup \text{books_on_shelf} = (\text{books_in_library} - \text{books_on_shelf}) \cup \text{books_on_shelf}$$

Since $(A - B) \cup B = A$, QED.

- (b) Would $\text{dom}(\text{books_on_loan}) \cup \text{books_on_shelf} = \text{books_in_library}$ have been equally effective.

Ans: No, because it doesn't require that a book on loan cannot be on a shelf as well.

2. For the **Borrow**(user,book) operation of the **SimpleLibrary** machine we get a proof obligation to show that

$$\text{dom}(\text{books_on_loan} \cup \{\text{book} \mapsto \text{user}\}) = \text{books_in_library} - (\text{books_on_shelf} - \{\text{book}\})$$

Reason why this is true.

Answer: We have, from 1a,

$$\text{dom}(\text{books_on_loan}) = \text{books_in_library} - \text{books_on_shelf}$$

So

$$\begin{aligned} \text{dom}(\text{books_on_loan} \cup \{\text{book} \mapsto \text{user}\}) &= \text{dom}(\text{books_on_loan}) \cup \{\text{book}\} \\ &= (\text{books_in_library} - \text{books_on_shelf}) \cup \{\text{book}\} \end{aligned}$$

But $\text{book} \in \text{books_on_shelf}$, so:

$$= (\text{books_in_library} - (\text{books_on_shelf} - \{\text{book}\})) \cup \{\text{book}\}$$

But now, since $\text{book} \in \text{books_in_library}$, the trailing union can be elided (we know it is in books_in_library , and not in the thing being subtracted), so it remains in the final set:

$$= \text{books_in_library} - (\text{books_on_shelf} - \{\text{book}\})$$

QED