

**FIT3013 Formal Specification in Software Engineering**  
**Semester 1 2008**  
**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  $\text{books\_on\_shelf}$  and  $\text{dom}(\text{books\_on\_loan})$  to *partition* the set  $\text{books\_in\_library}$ . 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.  
 (b) Would  $\text{dom}(\text{books\_on\_loan}) \cup \text{books\_on\_shelf} = \text{books\_in\_library}$  have been equally effective.
2. For the  $\text{Borrow}(\text{user}, \text{book})$  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.