LECTURE 17: LIBRARY CASE STUDY

Software Engineering

Mike Wooldridge

1 A Library Management System

- In this lecture, we specify a simple library system.
- Operations:
  - check out a book;
  - return a book;
  - add a book to library;
  - remove book from library;
  - get list of books by author or subject area;
  - get list of books checked out by particular borrower;

- All books must either be checked out or available for check out.
- No book may be simultaneously checked out and available.
- There is an upper limit to number of books that may be checked out.

1.1 Types

- We need sets for:
  - all possible books;
  - all possible copies of books;
  - all possible people;
  - all possible authors;
  - all possible subjects;
  - the various reports that may be produced.
- So parachute in:

$$[BOOK, COPY, PERSON, AUTHOR,\\ SUBJECT, REPORT]$$

1.2 State Space

- The state space is describes in several steps. First, a schema containing information relating to books in the library.

$$
\begin{array}{l}
\textit{ParaLibrary} \\
\hline
\textit{instance\_of} : \textit{COPY} \pfun \textit{BOOK} \\
\textit{written\_by} : \textit{BOOK} \pfun \mathbb{P}\,\textit{AUTHOR} \\
\textit{about} : \textit{BOOK} \pfun \mathbb{P}\,\textit{SUBJECT} \\
\hline
\operatorname{dom}\ \textit{written\_by} \subseteq \operatorname{ran}\ \textit{instance\_of} \\
\operatorname{dom}\ \textit{about} \subseteq \operatorname{ran}\ \textit{instance\_of}
\end{array}
$$

- *instance_of* tells us what book a copy is an instance of;
- the set

  $$\mathrm{ran}\ \mathit{instance\_of}$$

  is the set of all books in the library;
- *written_by* tells us who a book is written by; there may be more than one author, hence the powerset operation; there may be no authors;
- *about* tells us the subjects a book is about; there may be no subjects;
- first invariant tells us that we only know who wrote books in the library;
- second invariant tells us that we only know subjects of books in the library.

- The database part of the schema is as follows:

$$
\begin{array}{|l}
\multicolumn{1}{l}{\underline{\;LibraryDB\;}} \\
borrower, staff : \mathbb{P}\, PERSON \\
available, out : \mathbb{P}\, COPY \\
borrowed\_by : COPY \pfun PERSON \\
\hline
borrower \cap staff = \emptyset \\
available \cap out = \emptyset \\
\mathrm{dom}\ borrowed\_by = out \\
\mathrm{ran}\ borrowed\_by \subseteq borrower \\
\forall p : borrower \bullet \#borrowed\_by^{\sim}(\!|\{p\}|\!) \\
\quad \leq MaxCopies \\
\hline
\end{array}
$$

- *borrower* is the set of all borrowers known to the system;
- *staff* is the set of all staff known to the system;
- *available* is the set of all available books;
- *out* is the set of borrowed books (i.e., ones that have been checked out);
- *borrowed_by* tells us who borrowed the books out on loan.

- 1st invariant tells us that a person cannot be both a borrower and a staff;
- 2nd invariant tells us that books cannot be both available and checked out;
- 3rd invariant tells us that the only books appear have been borrowed by someone are those that are out;
- 4th invariant tells us that books can only be borrowed by borrowers;
- 5th invariant tells us that a borrower can only have out up to the maximum number of books.

- The library state space is then as follows:

$$
\begin{array}{|l}
\hline
\textit{Library} \\
\textit{ParaLibrary} \\
\textit{LibraryDB} \\
\hline
\operatorname{dom} \textit{instance\_of} = \textit{available} \cup \textit{out} \\
\hline
\end{array}
$$

- the only invariant in this schema tells us that the library does not know anything about books which are not in stock.

1.3 The Operations

- We assume initialisation operations; these are trivial.
- First we look at checking out books...
- Inputs: person name ($n?$) and copy ($c?$).

$$
\begin{array}{l}
\textit{CheckOut} \\
\hline
\Delta \textit{Library} \\
n? : \textit{PERSON} \\
c? : \textit{COPY} \\
\hline
n? \in \textit{borrower} \\
c? \in \textit{available} \\
\#\textit{borrowed\_by}^{\sim}(\!|\{n?\}|\!) \\
\quad < \textit{MaxCopies} \\
\textit{available}' = \textit{available} \setminus \{c?\} \\
\textit{out}' = \textit{out} \cup \{c?\} \\
\textit{borrowed\_by}' = \textit{borrowed\_by} \cup \\
\quad \{c? \mapsto n?\} \\
\hline
\end{array}
$$

- (Note that $f^{\sim}$ is the inverse of f.)
- 1st precondition is that the person trying to borrow must be a known borrower;
- 2nd precondition is that the book must be available;
- 3rd precondition is that the person trying to borrow must have out fewer than the maximum number of books available;
- the postconditions define the changes made to *available*, *out* and *borrowed_by*.

1.4 Returning a Book

- One input: the copy to be returned.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Return}} \\
\hline
\Delta Library \\
c? : COPY \\
\hline
c? \in out \\
available' = available \cup \{c?\} \\
out' = out \setminus \{c?\} \\
borrowed\_by = \{c?\} \lhd borrowed\_by \\
\hline
\end{array}
$$

- precondition states that the book can only be returned if it is out;
- 1st post-condition says that the book is available after the operation;
- 2nd post-condition says that the book is no longer out;
- 3rd post-condition uses domain subtraction to remove the correct record from the *borrowed_by* function.
- For example,

$$borrowed\_by = \{b01 \mapsto mjw, b02 \mapsto en,\ b03 \mapsto mjw\}$$

$$\{b01\} \lhd borrowed\_by = \{b02 \mapsto en,\ b03 \mapsto mjw\}$$

1.5 Adding Books to the Library

- There are two cases to consider:
  - where the book is completely new to the library;
  - where the book is another copy of a book that is already in the library.
- We have two schemas to capture these two situations:
  - *AddNewBook*;
  - *AddAnotherCopy*.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\_\ AddNewBook\ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Delta Library \\
c? : COPY \\
b? : BOOK \\
a? : \mathbb{P}\, AUTHOR \\
s? : \mathbb{P}\, SUBJECT \\
\hline
b? \notin \operatorname{ran}\ instance\_of \\
c? \notin available \cup out \\
available' = available \cup \{c?\} \\
instance\_of' = instance\_of \cup \{c? \mapsto b?\} \\
written\_by' = written\_by \cup \{b? \mapsto a?\} \\
about' = about \cup \{b? \mapsto s?\} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{AddAnotherCopy} \\
\Delta \textit{Library} \\
c? : \textit{COPY} \\
b? : \textit{BOOK} \\
\hline
c? \notin \textit{available} \cup \textit{out} \\
b? \in \operatorname{ran} \textit{instance\_of} \\
\textit{available}' = \textit{available} \cup \{c?\} \\
\textit{instance\_of}' = \textit{instance\_of} \cup \{c? \mapsto b?\} \\
\hline
\end{array}
$$

1.6 Removing Books

- Removing a books from the library is similarly complicated; once again there are 2 possibilities to consider…
  - removing a book that is the only copy;
  - removing one copy of a book leaving several other copies behind.
- Two schemas:
  - *RemoveOther* to remove one of several copies;
  - *RemoveLast* to remove the last copy.

$$
\begin{array}{|l}
\hline
\textit{RemoveOther} \\
\Delta \textit{Library} \\
c? : \textit{COPY} \\
\hline
c? \in \textit{available} \\
\#(\textit{instance\_of}^{\sim}(\!|\{\textit{instance\_of}(c?)\}|\!)) > 1 \\
\textit{available}' = \textit{available} \setminus \{c?\} \\
\hline
\end{array}
$$

- Note that there is no need to alter any variables in *ParaLibrary*; we only change *available*, to indicate that the book is no longer available.

$$
\begin{array}{|l}
\textit{RemoveLast} \\
\hline
\Delta \textit{Library} \\
c? : \textit{COPY} \\
\hline
c? \in \textit{available} \\
\#(\textit{instance\_of}^{\sim}(\!|\{\textit{instance\_of}(c?)\}|\!)) = 1 \\
\textit{available}' = \textit{available} \setminus \{c?\} \\
\textit{instance\_of}' = \{c?\} \lhd \textit{instance\_of} \\
\textit{written\_by}' = \{\textit{instance\_of}(c?)\} \lhd \\
\quad \textit{instance\_of} \\
\textit{about}' = \{\textit{instance\_of}(c?)\} \lhd \textit{about} \\
\hline
\end{array}
$$

1.7 Interrogating the Database

- Two options:
  - search by author;
  - search by subject;
  - find out what copies someone has borrowed.

- *ByAuthor* takes an author name and produces the set of all books that the author appeared in the 'author' list of.

$$\begin{array}{|l}
\hline
\textit{ByAuthor} \\
\Xi \textit{Library} \\
a? : \textit{AUTHOR} \\
out! : \mathbb{P}\, \textit{BOOK} \\
\hline
out! = \{b : \textit{BOOK} \mid a? \in \textit{written_by}(x)\} \\
\hline
\end{array}$$

- *BySubject* takes a set of subjects and produces a list of all the books which have these subjects in their 'about' list.

$$\begin{array}{|l}
\hline
\textit{BySubject} \\
\Xi \textit{Library} \\
s? : \mathbb{P}\, \textit{SUBJECT} \\
out! : \mathbb{P}\, \textit{BOOK} \\
\hline
out! = \{b : \textit{BOOK} \mid s? \subseteq \textit{about}(b)\} \\
\hline
\end{array}$$

- Finally, finding out who has borrowed what...

$$
\begin{array}{|l}
\multicolumn{1}{l}{\underline{\quad \textit{BooksBorrowedBy} \qquad\qquad\qquad\qquad\qquad}} \\
\Xi Library \\
n? : PERSON \\
out! : \mathbb{P}\, COPY \\
\hline
n? \in borrower \\
out! = borrowed\_by^{\sim}(\!|\{n?\}|\!) \\
\hline
\end{array}
$$