Formal Methods

Name: Aoun-Haider

ID: FA21-BSE-133

Section: A

Assignment no. 3

Date: 05-06-2023

Question no. 01

The software concerns recording the collection of books and works as software to manage the personal library. The software needs a database to manage the collection of books. The personal collection of books may contain so many books that it tends to buy duplicate books. There is an estimate that a flat is big enough to store the MAX number of books only.

The types involved here are the set of all possible books, called [BOOK].
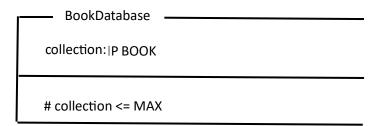
```
[BOOK]

MAX: ℕ

Response ::= alreadyOwned | noSpace
───────────────────────────────────
MAX = 1000
```

a) Write a system state schema BookDatabase containing the only state variable which is collection: P BOOK. Further, the only invariant is that the number of books in the set collection can't exceed the MAX number.

```
┌─── BookDatabase ───────────────────
│
│  collection: P BOOK
│
├────────────────────────────────────
│
│  # collection <= MAX
│
└────────────────────────────────────
```

b) Write an operation schema BuyBook to add the book. Further, the new book should not already exist in the book database.

```
┌─── BuyBook ──────────────────────────
│  Δ BookDatabase
│
│  newBook? : BOOK
├──────────────────────────────────────
│  # collection <  MAX
│
│  newBook? ∉ collection
│
│  collection' = collection U {newBook?}
└──────────────────────────────────────
```

c) Write an operation schema AlreadyOwned which returns the output that the book to be added is already existed in the book database.

```
┌─── AlreadyOwned ─────────────────────
│  Ξ BookDatabase
│
│  newBook? : BOOK
│
│  r!: Response
├──────────────────────────────────────
│  newBook? ∈ collection
│
│  r! = alreadyOwned
└──────────────────────────────────────
```

d) Write an operation schema NoSpace which returns the message that there is no space to add a new book in the book database.

```
┌─── NoSpace ──────────────────────────
│  Ξ BookDatabase
│
│  r! : Response
├──────────────────────────────────────
│  #collection = MAX
│
│  r! = noSpace
└──────────────────────────────────────
```