

Z Example Taken from Some Homework

April 20, 2014

Introduction

The Class Manager's Assistant module must provide an interface for dealing with students enrolling in a class. Students enroll in a class. The result of the enrollment is specified by *EnrollResponse*. At some point in time, a student may be tested; it is assumed that a student will pass the test. When a student is tested, the Class Manager's Assistant must provide an appropriate *TestResponse*.

Given Set [Student]
| *size* : \mathbb{N}

EnrollResponse ::= *success* | *alreadyenrolled*
TestResponse ::= *success* | *alreadytested* | *notenrolled*

Abstract State Schema

For a *Class* in the Class Manager's Assistant, a student must enroll in a class to be considered enrolled. Once a student is enrolled, the student may be tested.

<i>Class</i>
<i>enrolled</i> : $\mathbb{P}Student$ <i>tested</i> : $\mathbb{P}Student$
<i>tested</i> \subseteq <i>enrolled</i> $\#enrolled \leq size$

Initialization of Abstract State

It is initially assumed that a class is empty, and therefore has no students enrolled.

[*Class'* | *enrolled'* = 0]

Operation - Enroll

When a student requests to be enrolled, that student is added to the Class.

$EnrollOK$
$\Delta Class$
$S? : Student$
$R! : EnrollResponse$
$S? \notin enrolled$
$enrolled' = enrolled \cup \{S?\}$
$R! = success$

If a student has already enrolled, then that student can not enroll in the Class again. Please note that this would be regardless of the student's test status since $tested \subseteq enrolled$.

$AlreadyEnrolled$
$\Xi Class$
$S? : Student$
$R! : EnrollResponse$
$S? \in enrolled$
$S? = alreadyenrolled$

Therefore, the enroll operation must be the disjunction of EnrollOK and AlreadyEnrolled.

$$Enroll \triangleq EnrollOK \vee AlreadyEnrolled$$

Operation - Test

When an enrolled student is tested, the student passes and is now part of the student population in the class marked as tested.

$TestOK$
$\Delta Class$
$S? : Student$
$R! : TestResponse$
$S? \in enrolled$
$S? \notin tested$
$tested' = tested \cup \{S?\}$
$enrolled' = enrolled$
$R! = success$

If a student has not enrolled, then the attempt to test the student must necessarily fail.

NotEnrolled
$\exists \text{Class}$ $S? : \text{Student}$ $R! : \text{TestResponse}$
$S? \notin \text{enrolled}$ $S? = \text{notenrolled}$

In addition, a student can not be tested twice.

AlreadyTested
$\exists \text{Class}$ $S? : \text{Student}$ $R! : \text{TestResponse}$
$S? = \text{tested}$ $R! = \text{alreadytested}$

Therefore, the test operation must be the disjunction of TestOK, NotEnrolled, and AlreadyTested.

$$\text{Test} \triangleq \text{TestOK} \vee \text{NotEnrolled} \vee \text{AlreadyTested}$$