INTERNATIONAL UNIVERSITY OF EAST AFRICA
'Learning to Succeed'

FACULTY OF SCIENCE AND TECHNOLOGY

END OF SEMESTER EXAMINATIONS - DECEMBER 2025

PROGRAMME: BSSE
YEAR/SEM: YEAR 3/SEMESTER 1
COURSE CODE: SWE3100
NAME: FORMAL METHODS OF SOFTWARE ENGINEERING

DATE:
TIME:

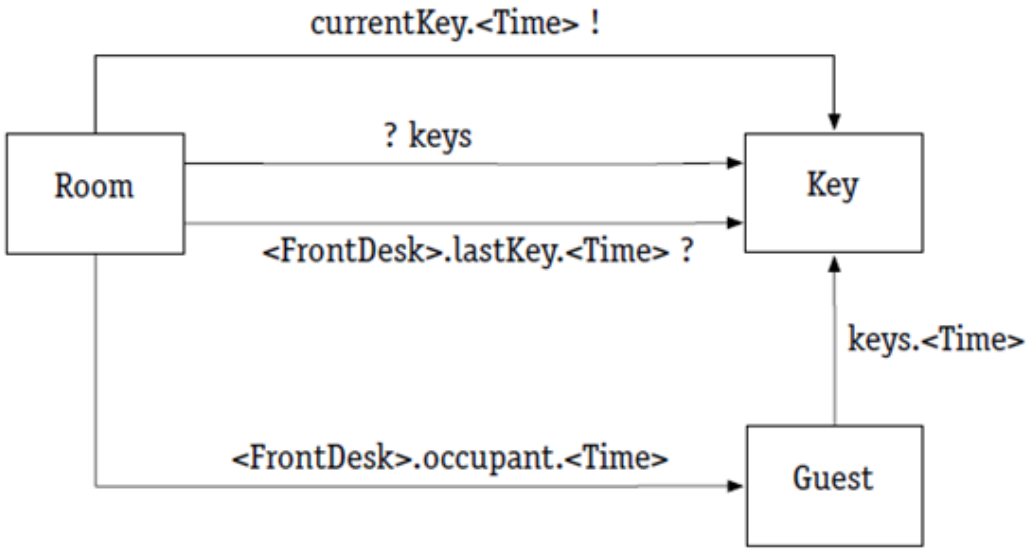
INSTRUCTIONS TO CANDIDATES:

SECTION A

Attempt all Questions in Section A

Question 1:

Most hotels now issue disposable room keys; when you check out, you can take your key with you. How, then, can the hotel prevent you from re-entering your room after it has been assigned to someone else? The trick is recordable locks, which have been in use in hotels since the 1980's, initially in mechanical form, but now almost always electronic. The idea is that the hotel issues a new key to the next occupant, which recodes the lock, so that previous keys will no longer work. The lock is a simple, stand-alone unit (usually battery-powered), with a memory holding the current key combination. A hardware device, such as a feedback shift register, generates a sequence of pseudorandom numbers. The lock is opened either by the current key combination, or by its successor; if a key with the successor is inserted, the successor is made to be the current combination, so that the old combination will no longer be accepted. This scheme requires no communication between the front desk and the door locks. By synchronizing the front desk and the door locks initially, and by using the same pseudorandom generator, the front desk can keep its records of the current combinations in step with the doors themselves.



Model and Analyse this scheme using the alloy tool knowledge and Formal Methods in Software engineering (40 Marks)

Question 2:

For organizing a large collection of media files, such as photos, movies, or soundtracks, the built-in facilities of a file system are usually not good enough. Applications for "media asset management" allow you to view large collections in thumbnail form; to move, rename, copy and backup files; to attach labels and captions; to generate webpages; and so on. The main

advantages over the standard file system's interface is that you can form catalogues that crosscut the directory structure, and apply batch operations to collections of files at once. This example is a model of a few of the essential functions of one of the popular applications, iView Media Pro. I developed it to illustrate how modelling can give you insight into very basic functions: the kind that seem obvious at first glance, but are subtler when examined carefully. This kind of modelling is ideally performed in the early stages of developing a program such as Media Pro, but is also useful later, when new functionality threatens to compromise the clarity of the key abstractions. Although I'd used (and been impressed by) Media Pro for several years, when I constructed this model, I hadn't understood the details of the basic functions. I was motivated by occasional unpleasant surprises that made me wonder whether they might have been designed differently. From the modeling experience, I came to the conclusion that the design was eminently sensible, and that aside from the addition of an undo facility, I found no opportunity for an improvement in the underlying abstractions. Constructing and analyzing the model gave me a number of insights. It would belabor them to show the model in its intermediate forms, and to attempt to explain how they arose. Instead, I'll present the final version of the model, with a separate summary of the insights gained.

Answer the following questions (40 Marks)

i. Show the model diagram for the catalog state declarations
ii. Model the operations associated with hiding and showing assets

SECTION B

Attempt any 3 Questions in Section B

Question 1:

Using examples of Alloy code explain the following terms in formal specification (*05 marks@*)

a) Signatures and Fields

b) Predicates and Functions

c) Facts

d) Assertions

Question 2:

a) Define the intersection of two sets A and B in set theory. (*05 marks*)

b) Explain the difference between a relation and a function in the context of Alloy. (*05 marks*)

c) Provide an example of a valid Alloy signature named "Person" with attributes "name" and "age." (*05 marks*)

d) Describe the meaning of the reflexive property of a relation in formal terms (*05 marks*)

Question 3:

The Alloy Analyzer will generate instances of models so that we can see if they match our intentions. Write down and briefly explain at least three instances of our model below (20 marks)

```
abstract sig Person {}

sig Man extends Person {}

sig Woman extends Person {}

sig Married in Person {}
```

Question 4:

a) Express the following logic properties on set without using the #operator (15 marks)

i. Set has at least one element

ii. Set has no elements

iii. Set has exactly one element

iv. Set has at least two elements

v. Set has exactly two elements

b) What is formal specification and state some advantages for using them (05 marks)

Question 5:

a) Provide examples of real-world applications where formal methods have been successfully employed. (06 marks)

b) Discuss how the use of formal methods in software engineering has evolved over time. (04 marks)

c) Evaluate the impact of formal methods on software development practices, considering both benefits and challenges. (06 marks)

d) Consider future trends and potential advancements in the field of formal methods. (04 marks)

Question 6:

a) What do you understand by predicates and propositions in relation to formal methods (04 marks)

b) For each of the following English statements provide the most accurate translation in propositional logic. (02 marks@)

i. If Bill met Jane yesterday, they went to the movies or to the park.

ii. The alarm goes off if and only if there is smoke.

iii. I get sad when it rains.

iv. I'll call you unless I get your message first.

v. I'll call you if I'm not done; otherwise, I'll see you there.

vi. Hurry up, otherwise you will miss the train.

vii. No pain, no gain.

viii. Jane wants a black and white cat.

Question 7:

a) Using examples, write short notes on the following in relation to formal methods (10 Marks)

i. Statement

ii. Proposition

iii. Predicate

iv. Formal methods

b) Specify using comprehension notation (06 marks)

i. Odd positive integers

ii. The squares of integers, i.e. {1, 4, 9, 16, 25, ...}

c) Describe the principles of formal specification (04 marks)

Question 8:

a) A farmer is carrying a fox, a chicken, and a sack of grain. He must cross a river using a boat that can only hold the farmer and at most one other thing. If the farmer leaves the fox alone with the chicken, the fox will eat the chicken; and if he leaves the chicken alone with the grain, the chicken will eat the grain. How can the farmer bring everything to the far side of the river intact? Use formal methods and states to illustrate and model this solution. (20 marks)

Question 9:

a) Given the following alloy code show the model and graphical representation of the code below (05 marks)

```
abstract sig Person {}

sig Man extends Person {}

sig Woman extends Person {}

sig Married in Person {}
```

b) The Alloy Analyzer will generate instances of models so that we can see if they match our intentions. Which of the following are instances of our current model in (a) above and explain your answers (15marks)

A

Person={(P0), (P1), (P2}

Man={(P1), (P2)}

Married = {}

B

Person = {(P0), (P1)}

Man = {(P0)}

Married = {(P1), (P0)}

C

Person={(P0), (P1), (P2)

Man={(P1), (P2)}

Married = {}

D

Person = {(P0), (P1)}

Man = {(P0)}

Married = {(P1), (P0)}

E

Person={(P0), (P1), (P2), (P3)}

Man={(P0), (P1), (P2), (P3)}

Married={(P2), (P3)}

Question 10:

a) What types of systems have been modeled with Alloy? (4 marks)

b) What types of questions can Alloy Analyzer answer? (4 marks)

c) What is the purpose of each of the sections in an Alloy specification? (4 marks)

d) Using examples write short notes on the following? (8 marks)

i. Atom

ii. Relations

iii. Signatures and Fields

iv. Predicates and Functions

Question 11:

a) Using the example of a family structure:

i. How would you use multiplicities to define the children relation? (5 marks)

ii. How would you use multiplicities to define the spouse relation? (5 marks)

b) Explain the expected output of this code. Does it look correct? What, if anything, would you change about it? (10 marks)

```
---------- Signatures ----------

abstract sig Person {
        children: set Person,
        siblings: set Person
}

sig Man, Woman extends Person {}

sig Married in Person {
```

spouse: one Married

}

/* create an instance with at most three atoms in every top-level signature

* (in this case just Person). 3 is the SCOPE.

*/

run {} for 3

Question 12:

a) Given the sets: A = {1,2,3,4,5} B = {3,4,5,6,7} C = {5,6,7,8,9}. Compute the following: (08 Marks)

i. A∪B

ii. A∩B

iii. B−C

iv. Power set of A

b) Given the set S = {a, b, c, d, e}, find: (04 Marks)

i. The cardinality of S, i.e., |S|

ii. The number of subsets of S Given the sets: X = {1,2} and Y = {a, b, c}, compute the Cartesian product X×Y

c) Consider the relation R = {(1,2), (2,3), (3, 4)} on the set S = {1,2,3,4}

Determine: (08 Marks)

i. The domain of R.

ii. The range of R.

iii. Is R a function? Justify your answer.