

Student ID Number:*(fill in your NUS Student ID here)*

Institute of Systems Science
National University of Singapore

**MASTER OF TECHNOLOGY IN
INTELLIGENT SYSTEMS**

Graduate Certificate Examination Semester II 2018/19

Subject: Intelligent Reasoning Systems

Sample Examination Questions

SECTION A

Question	Marks
1	/24
2	/16
TOTAL	/40

SECTION A

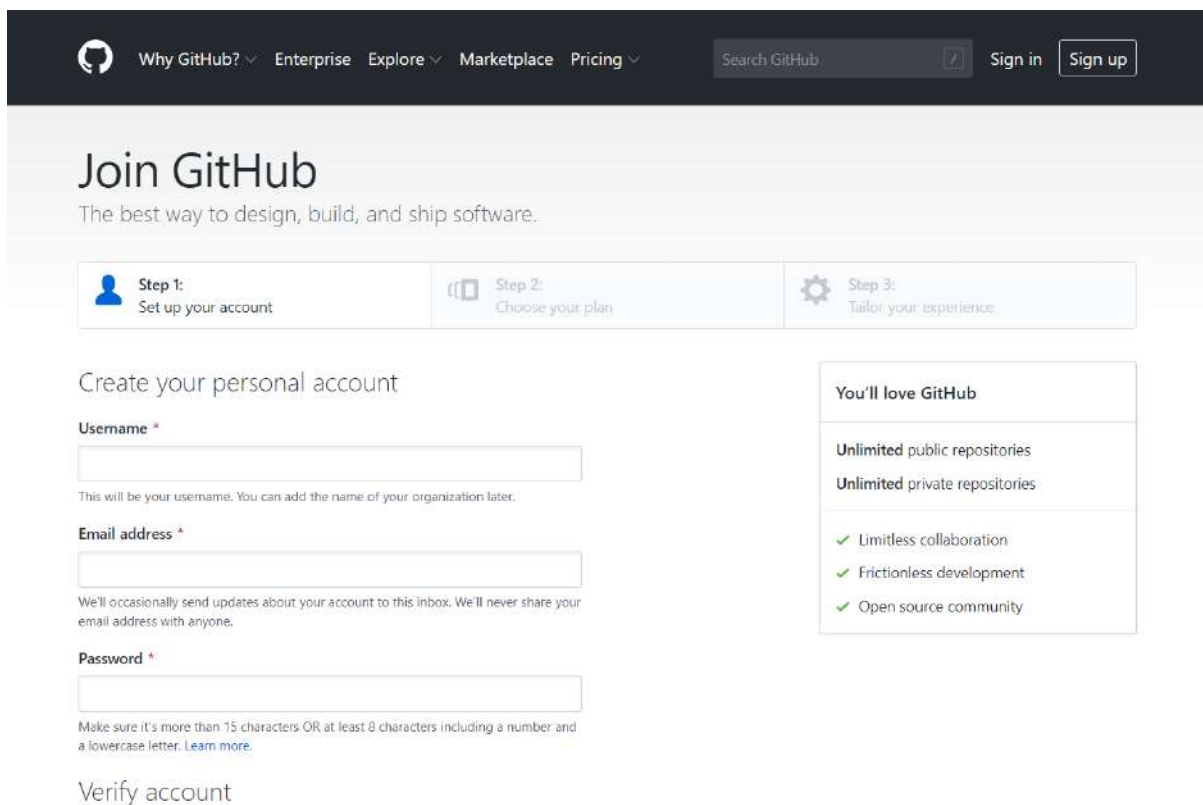
Question 1

(Total: 24 Marks)

Securing Online Account Registration for Microsoft's Github.com

You currently work in a top security firm, specialized in fighting against online bot attacks. Recently your firm is hired by a famous code collaboration and management giant, Github.com (owned by Microsoft), to evaluate the security of its automated online account creation, which enforces Real Human Verification, to prevent malware and robots from abusing automated account registration.

Below is the Sign up web page for Github account registration:



The screenshot shows the GitHub 'Join GitHub' registration page. The header includes navigation links like 'Why GitHub?', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing', along with a search bar and 'Sign in'/'Sign up' buttons. The main heading is 'Join GitHub' with the tagline 'The best way to design, build, and ship software.' Below this is a three-step progress bar: 'Step 1: Set up your account' (active), 'Step 2: Choose your plan', and 'Step 3: Tailor your experience'. The 'Create your personal account' section contains three required fields: 'Username', 'Email address', and 'Password', each with a brief explanation of the requirements. To the right, a box titled 'You'll love GitHub' lists benefits: 'Unlimited public repositories', 'Unlimited private repositories', 'Limitless collaboration', 'Frictionless development', and 'Open source community'. At the bottom, there is a 'Verify account' link.

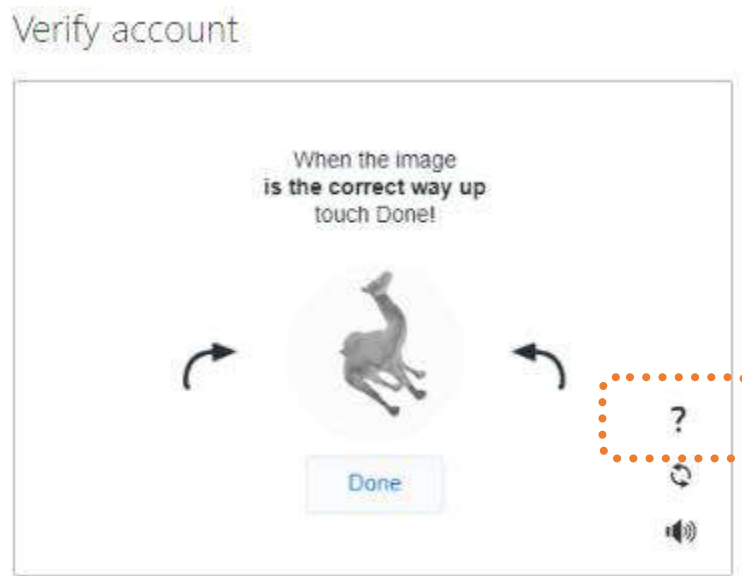
As a security expert, you are to conduct a penetration test against its online account creation. Thus you need to create an intelligent system/bot which is able to massively register new Github accounts through penetrating all of Github's online verifications during account creation.

In order to design/create the bot, you analyze the account registration procedures. Below is a typical flow:

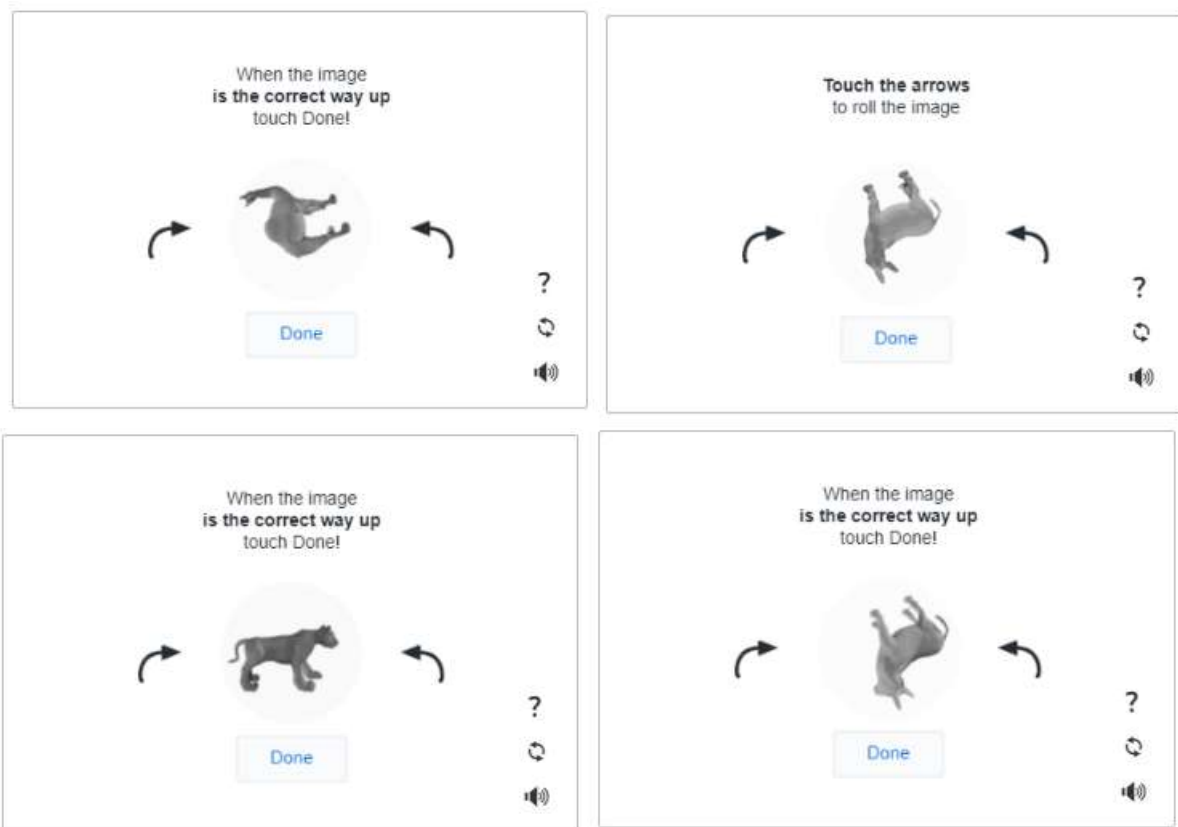
1. Go to web link <https://github.com/join?source=header-home> to click Sign up.
2. Fill in Username, Email address, and Password.

The screenshot displays the GitHub 'Join GitHub' page. At the top, there is a navigation bar with links like 'Why GitHub?', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing'. A search bar and 'Sign in'/'Sign up' buttons are also present. The main heading is 'Join GitHub' with the tagline 'The best way to design, build, and ship software.' Below this, a progress bar shows three steps: 'Step 1: Set up your account', 'Step 2: Choose your plan', and 'Step 3: Tailor your experience'. The 'Create your personal account' section includes input fields for 'Username', 'Email address', and 'Password', each with a red asterisk indicating a required field. Below the 'Email address' field, there is a note: 'We'll occasionally send updates about your account to this inbox. We'll never share your email address with anyone.' Below the 'Password' field, there is a note: 'Make sure it's more than 15 characters OR at least 8 characters including a number and a lowercase letter. [Learn more.](#)' To the right of the form, a box titled 'You'll love GitHub' lists benefits: 'Unlimited public repositories', 'Unlimited private repositories', 'Limitless collaboration', 'Frictionless development', and 'Open source community'. Below the form, there is a 'Verify account' section with a visual puzzle. The puzzle shows a reindeer and a text prompt: 'When the image is the correct way up touch Done!'. There are arrows indicating the image should be rotated. Below the puzzle is a 'Done' button. At the bottom, there is a green 'Create an account' button. A disclaimer at the bottom of the form states: 'By clicking "Create an account" below, you agree to our [terms of service](#) and [privacy statement](#). We'll occasionally send you account related emails.'

3. You then proceed to Real Human Verification:



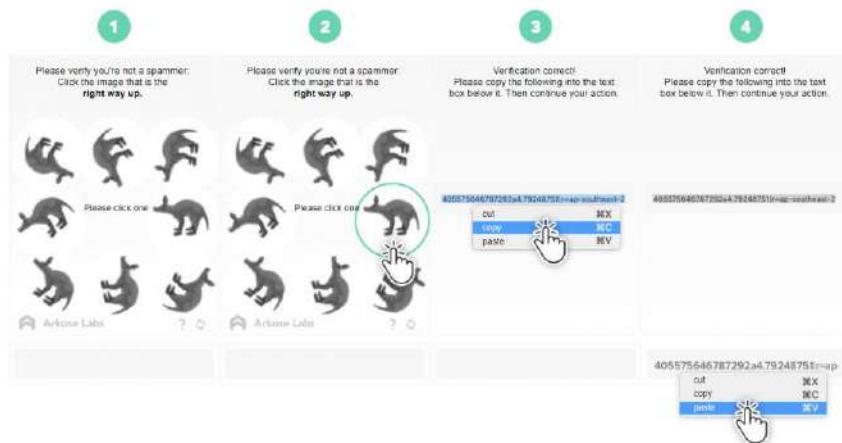
You also notice that there are many different animals that may appear:



4. You click '?' to understand how to verify the account correctly. Below is the Github [*How-to-Solve-Enforcement-Challenges.pdf*](#) guide:

How to Solve Enforcement Challenges

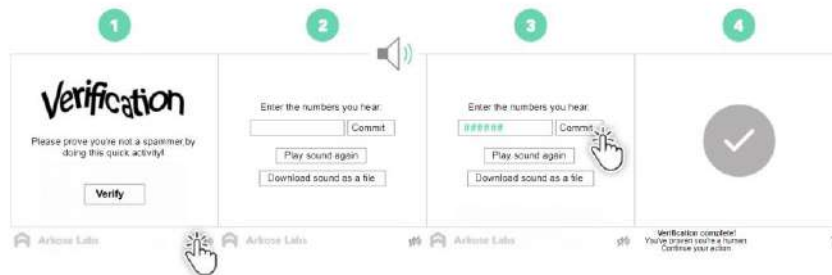
Roll the Ball (Simple)



Roll the Ball (Animated)



Audio Accessibility



Roll the Ball (Simple)

Roll the Ball (Simple) is an Enforcement Challenge that is compatible with older devices and verifies you're a real user.

To solve Roll the Ball (Simple) follow the steps below:

1. Click, or tap, the image that is oriented correctly relative to the points of up and down until no more images appear. E.g. an animal that appears to be standing upright on its feet.
2. Right click, or double tap, the code and select 'Copy'.
3. Click, or tap, the text box at the bottom of the game and select 'Paste'.
4. Continue your action.


Roll the Ball (Animated)

Roll the Ball (Animated) is an Enforcement Challenge that incorporates interactive elements to verify you're a real user.

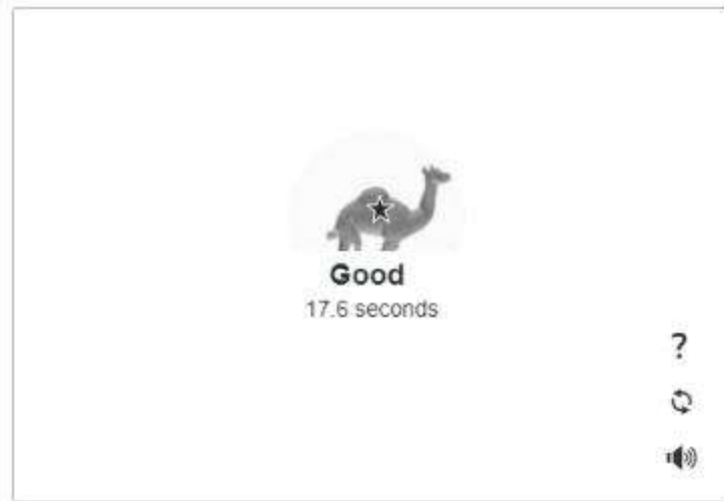
To solve Roll the Ball (Animated) follow the steps below:

1. Click, or tap, the 'Verify' button at the lower centre of the game.
2. Click, or tap, either of the arrows (←) (→) to rotate the ball until the image is oriented correctly relative to the points of up and down. E.g. until the subject appears to be standing upright.
3. Click, or tap, the 'Done' button at the lower centre of the game.
4. Continue your action.

Please note: Sometimes you may need to orient multiple images correctly before continuing your action.

5. By following the guide, you get through verification (the big check  shown below). You click '**Create an account**' button to obtain a new account successfully.

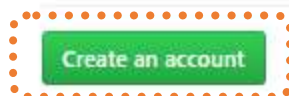
Verify account



Verify account




By clicking "Create an account" below, you agree to our [terms of service](#) and [privacy statement](#). We'll occasionally send you account related emails.



Now it's time to design/create your own intelligent bot system to massively create accounts (for a good reason).

After comprehensive analysis, you derive the key objective/mission for this AI system similar to the following:

Pass the critical **Verify account** step during account creation (solve the puzzle with variations of animal images, on demand: multiple-times), e.g. to reach that big check  stage shown on screen.

You recall that you currently own a working AI bot/system, with the capabilities as follows, you decide to re-use it by enhancing its ability for this new mission.

1. Able to see the computer screen, as in a form of image/pixels streaming, e.g. 60 frames/images per second.
2. Able to track and move the mouse cursor on screen based on screen coordination input: (X , Y)
3. Able to left click or right click the mouse button
4. Able to access, e.g. read in as pdf/txt/image format, the digitized document: ***How-to-Solve-Enforcement-Challenges.pdf***

Your further technical analysis revealed that:

1. By reusing your existing bot, there is no need to design the physical movement or hardware part of your AI bot/system, as it could operate the mouse the same as a human could, based on instructions from its own autonomous reasoning.
2. This AI will need to autonomously determine (the number of) clockwise/anti-clockwise clicks before clicking 'Done' on the Verify account screen.
3. This bot system should autonomously decide to use either clockwise or anti-clockwise (direction) button for clicking, based on minimum clicks (less effort) needed.
4. You will focus on the smartness/reasoning enhancement of this AI bot/system.

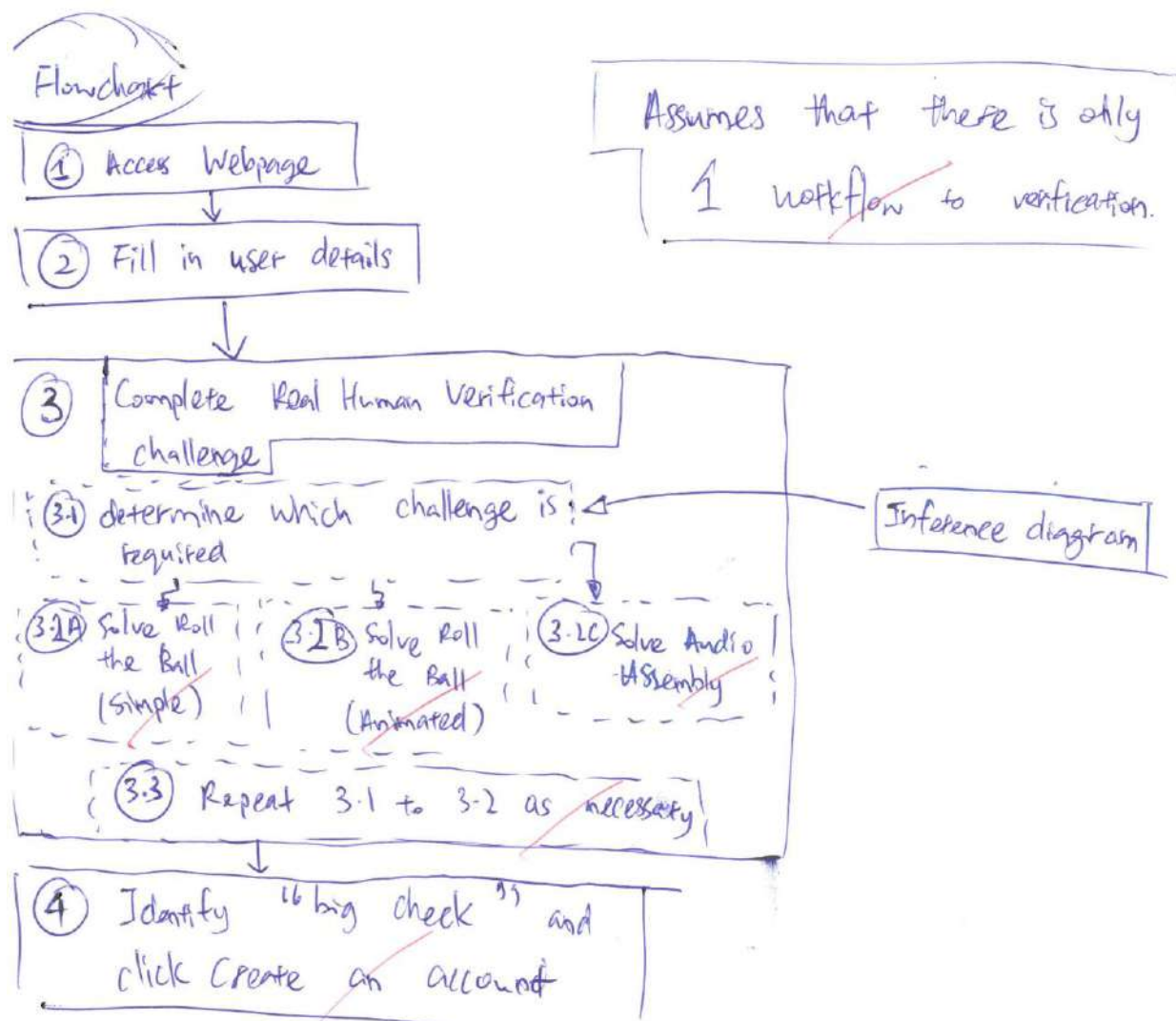
You are now ready to start your job (exam question and answer)...

Answer the following questions

- a. Assuming you were the intelligent system/AI bot, you read through that ***How-to-Solve-Enforcement-Challenges.pdf***, then you generalize/generate the knowledge/strategy to successfully handle numerous possible variations of this account verification, e.g. changed animal image. **Decompose** this problem to sub-problems. For each sub-problem, **write** down the useful knowledge, references, and/or reasoning strategies for solving the verification under possible variations, using concise natural language (English). **Annotate** different reasoning types used where applicable.

Hint: One key reasoning task is for the AI bot/system to determine whether/when the verification image's subject is in the correct right way up position: animal standing upright. Another one is the decision to use either clockwise or anti-clockwise button for clicking, based on minimum clicks (less effort) needed. How to achieve these universally?

(5 Marks)

Write Your Answer Here

Continue Your Answer Here

= I would use an interactive package such as Selenium together with the mouse.

↳ As selenium can detect the html/css elements such as a button box as needed. (The X,Y position of the mouse is not that accurate for different sized webpages)

For STEP ①, I would need a table of all the sign-up links if there are multiple

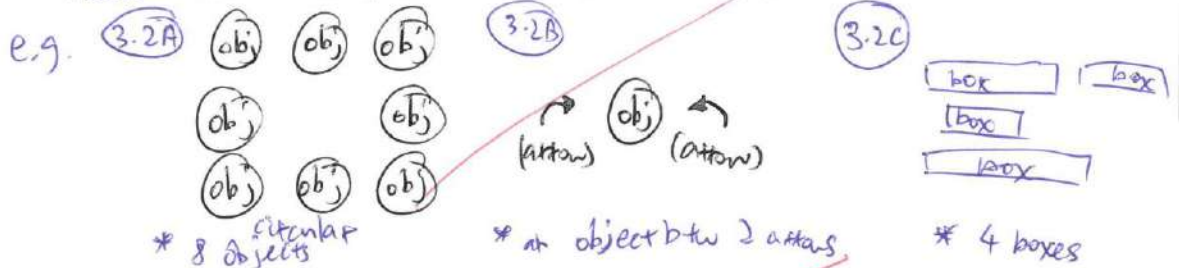
Attribute Worksheet

For STEP ②, I would need a table of randomly generated username / email / password, I could generate it via using a dictionary of known words so it will not be so suspicious, (e.g. blue ~~mamma~~ @gmail.com us

Attribute Worksheet
OR a pre made manual list

by Rules Decision Table

For STEP ③.① I would need to know which type of challenge is required. We can use the position of the items and semantic web to do this.



For STEPS ③.2A & ③.2B I would need to know the angle of the object with respect to the top, (θ)

③.2A Which object has the smallest θ or ③.2B I would need to know how much change in angle (Δ) is given by one click. If $\theta \geq 180^\circ$, turn anticlockwise

Other guidelines to answer:

1. Determine upright position of animal image

Decompose animal image into body parts, then annotate name of body parts, e.g. head, neck, ear, horns, nose, forelimb, hind leg, main body, tail, etc.

Example techniques include:

Use common sense reasoning framework, e.g. semantic web, frames, thematic roles.

Use image processing, object detection, object masking, e.g. pre-trained deep learning models.

Other reasonable techniques

2. Determine clockwise or anticlockwise click button

Identify head, body and legs, then determine the facing direction of animal in image

Calculate the angle between animal's facing horizontal vector/line and screen web page horizontal line.

If angle degree smaller or equal to 180 degree, click clockwise button, else, click anticlockwise.

Example candidate techniques include:

Use spatial relationship reasoning of head, body, and leg's relative positions to determine facing direction.

Other reasonable techniques

3. Heuristic reasoning strategy to handle exception scenarios, e.g. repeated image verification prompted; three different means of verification, network error, etc.

b. **Indicate** any additional knowledge sources/bases useful for this problem solving.

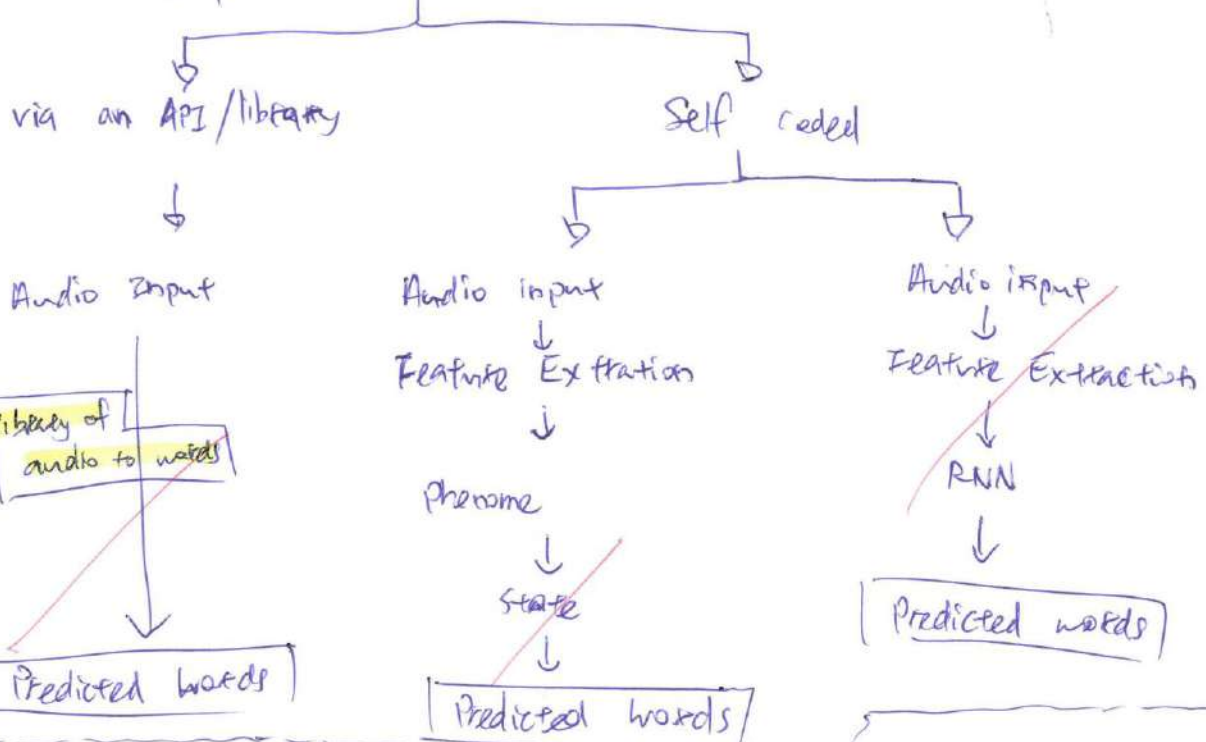
(3 Marks)

Write Your Answer Here

Knowledge source/base

(1)

3.2C The ability to convert speech to text.



(2)

3.2A & 3.2B A repository of animal photos and their angle to the vertical. This can be used to do matching.

(3)

3.2B To detect the feet/head position of the animals to detect the likely angle to the vertical e.g. the head should be above the feet

Library of possible looking feet/head/hands of animals

(head)
feet

gtr and gtr

Other guidelines to answer:

Common sense knowledge base like animal ontology and semantic web in animal classification.

Defined thematic roles system for animal parts and relationships.

Spatial relationship of animal parts, using first order logic or frames.

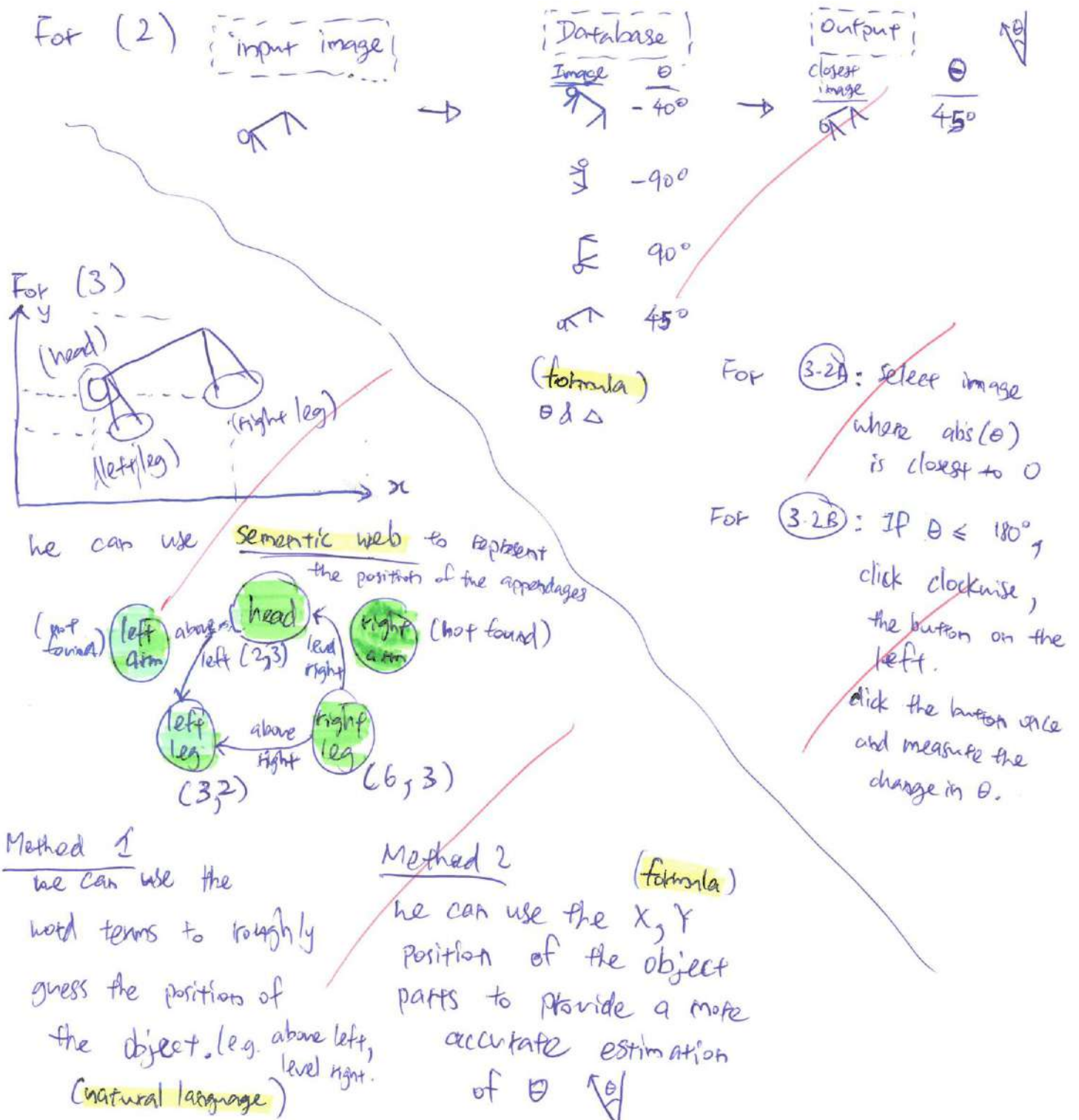
Image records after post edge detection processing to extract animal outline figures in mono color.

Contextual/Animal image data base for re-training and optimizing deep learning models for animal parts annotation/tagging.

- c. Give example knowledge representations in the animal context, e.g. using a lion image, to respective knowledge bases, based on your answer to question 1.b.

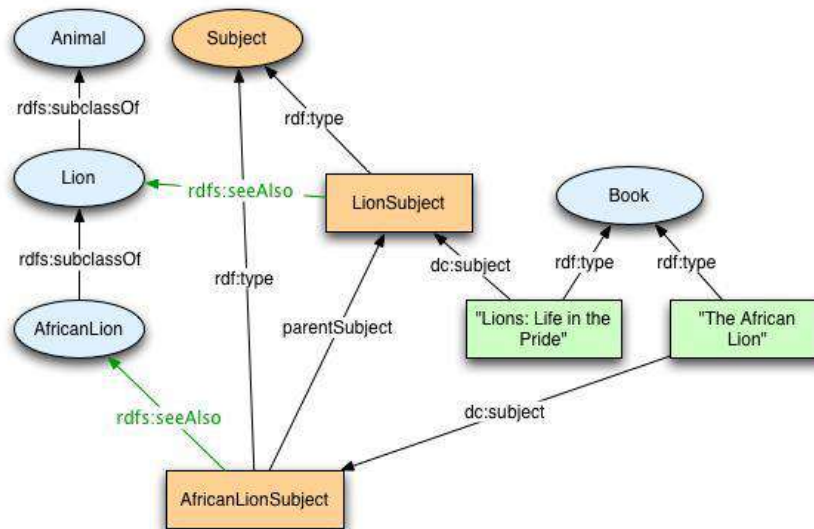
(3 Marks)

Write Your Answer Here



Other guidelines to answer:

Common sense knowledge base like animal ontology and semantic web in animal classification. An example ontology/semantic web structure:



Key: "S:" = Show Synset (semantic) relations, "W:" = Show Word (lexical) relations
 Display options for sense: (gloss) "an example sentence"

Noun: Lion

S: (n) lion, king of beasts, Panthera leo (large gregarious predatory feline of Africa and India having a tawny coat with a shaggy mane in the male)

S: (n) lion, social lion (a celebrity who is lionized (much sought after))

S: (n) Leo, Lion ((astrology) a person who is born while the sun is in Leo)

S: (n) Leo, Leo the Lion, Lion (the fifth sign of the zodiac; the sun is in this sign from about July 23 to August 22)

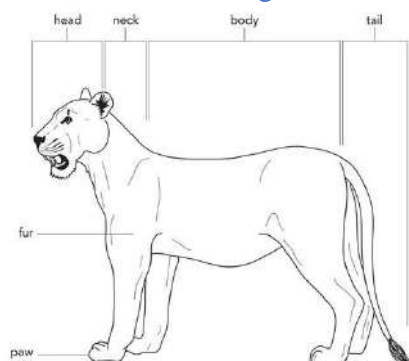
Noun: Leo

S: (n) Leo, Lion ((astrology) a person who is born while the sun is in Leo)

S: (n) Leo (a zodiacal constellation in northern hemisphere between Cancer and Virgo)

S: (n) Leo, Leo the Lion, Lion (the fifth sign of the zodiac; the sun is in this sign from about July 23 to August 22)

Contextual/Animal image data base of body parts annotation.



- d. Make appropriate assumptions, e.g. sub tasks, function modules, as well as legitimate bot actions provided in the earlier section of 'Existing capability of AI bot/system', then **design (architect)** the AI bot/system using appropriate knowledge models, e.g. inference diagram, block diagram, process flowchart, rulesets, loops, branches, and/or other relevant representation assets.

(5 Marks)

Write Your Answer Here

flowchart

Step 1 Access webpage

Call actions will either use Selenium or the bot to click)

↳ use table of weblinks + selenium to open webpage

Step 2 Fill in user details

↳ extract user details from table

username = ...

email_address = ...

password = ...

(using selenium)

↳ detect box item for

(using selenium)

↳ fill in box item for

{username, email_address, password}

{username, email_address, password}

Step 3-1 Determine which challenge is required

verify which of the following fits the image in the box under (to verify account)

3-2A ○ ○ ○

3-2B ○

3-2C

others

if not detected, exit & send prompt

(branches)

IF 3-2A: solve challenge

IF 3-2B: solve challenge

- separate the 8 objects

- identify θ of each object to vertical (see 1c)

- click on object with $\min(\text{abs}(\theta))$

- detect textbox, copy text, paste text (either by Selenium or by left and right clicking by the bot)

- identify θ of object to vertical (see 1c)

- identify Δ of change in θ per click

- initiate the # of clicks in clockwise or anti-clockwise based on θ and Δ . (see 1c)

- when complete, repeat identify of θ , click done if $\theta \leq \text{threshold}$.

Continue Your Answer Here

IP (3.20) : solve challenge →

- click on "download save as a file"
- do speech to text conversion (see 16)
- paste text into empty textbox
- click on "commit" button

(3.3) : check if there are other challenges (loop) →

- repeat detection of (3.1)
- repeat steps (3.2A), (3.2B), (3.2C) as needed

Step (4) : Identify "big check" and create account →

- identify "big check" ✓
- click on "create an account"
- save details + timestamp + status into some database/table for future use.

Exit conditions : - in (3.1), unable to detect challenge
 - total time greater than xxx seconds
 - link broken/errors.

Other guidelines to answer:

Webpage object detector: identify objects of interest useful to account verification and creation, e.g. animal image, click buttons

Animal body parts detector

Animal facing vector line detector

Angle calculator for clockwise and anticlockwise

Upright position detector

Confirmation and success detector

Other reasonable system modules, user interfaces

System scalability, concurrency

Reasonable pseudo code with below elements:

Start and end

Loop logic

Inputs list

User interface

Success and failure notification

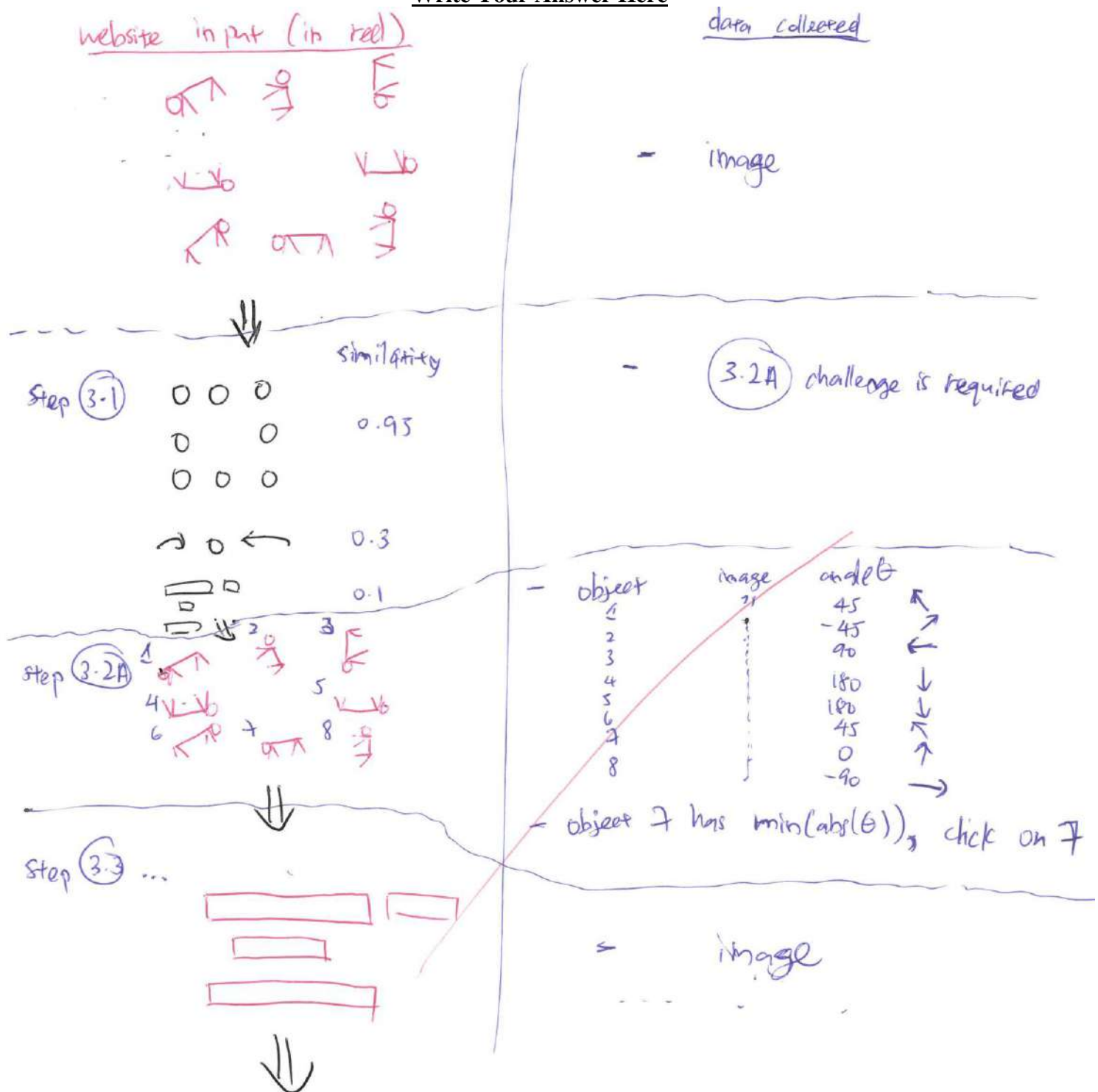
Exception handling

- e. Based on your design in question 1.d, use **one** sample animal image, e.g. a lion, to **instantiate** the reasoning process from data flow perceptive.

Hint: Make use of knowledge representations and/or data structures you have designed in question 1.c.

(3 Marks)

Write Your Answer Here



Continue Your Answer Here

Step 3.1

000	
0 0	0.05
000	
30 ←	0.1
↓	
↓	
↓	0.98
↓	

- 320 challenge is required

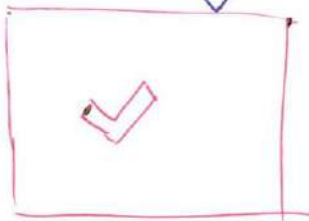
Step 3.2

- download audio file
(----- .mp4)
- call package/API
(54372)
- paste text representation

- audio file

- text representation of
audio file

Step 3.3
⋮



- (big check)
is seen

Step 4

Complete create
account.

↑)

- Repeat from 1
- Save into database

for username, email address, password
Completed on ...
YYYYMMDD HH:MM:SS

Other guidelines to answer:

Click sign up to load account verification web page

Locate and extract current image using parsing

Detected as lion using knowledge models and representations

Feed into animal parts detector to annotate lions various body parts using instantiations

Other reasonable reasoning steps

- f. The ultimate goal for Github is to prevent possible AI bots' attack like the one you have designed above. One possible way is to creatively optimize the image repository being used in the verification process. The optimization objective is to maximize the chance that humans will be able to solve it while minimizing the likelihood of successful automated attacks by AI bots, e.g. create imaginative animals which don't exist in nature. You need to **generate** new idea(s) for anti-attack methods. Then **suggest** some possible intelligent optimization techniques to implement your idea(s). Lastly, **describe** the technical mechanisms in detail, e.g. domain models, representations, etc.

(5 Marks)

Write Your Answer Here

Anti-attack methods

1) keep changing the verification methods/rules/challenges

Implementation

database of all challengers

Match exposed

randomly selected per match

April exposed

2) For (3.2A), Specify the nearest to right side up instead of exactly right side up

(none are right side up.)

↑ ↑ ↑ (closest)

3) For (3.2A), - use animals without legs/appendages.
- use only a face.
- random position of appendages

use a database of faces & perturbate the angle yourself.

each 0 B A
can be an item,
randomly generate them with specific faces

4) For (3.2B), each button changes the angle by an increasing or decreasing value than is not constant

rule-based

(original) $\Delta = 0$ (1 click) $\Delta = 30$ (2 click) $\Delta = 80$

0 +30
30 +50
80 +70

5) For (3.2C), - add background noise.
- have 2 speakers and as for the word in one of the accents (e.g. English & American)

English: man 45000

American: man 45657

English (input): 45000

American (audio): 45657

Combine 2 clips of speaking

Other guidelines to answer:

Different optimization techniques such as genetic algorithm, hill climbing and simulated annealing can be used, to per mutate animal parts to generate new animal image, in order to extend animal repository.

When genetic algorithm is used for optimization, chromosome representation and fitness function need to be designed. The chromosome can represent the set of parameters used in generating the animal images, e.g. background pattern, blurring, contrast adjustment, distortion amount, etc.

Fitness function can be defined as follows:

$$F = H - \alpha \cdot A$$

Where F is the fitness value; H is the likelihood of human success; A is the likelihood of a successful automated attack; α is the importance assigned for the two different objectives.

H can be modelled and evaluated using some indirect simulation tools. A can be evaluated through the interaction with the AI bots.

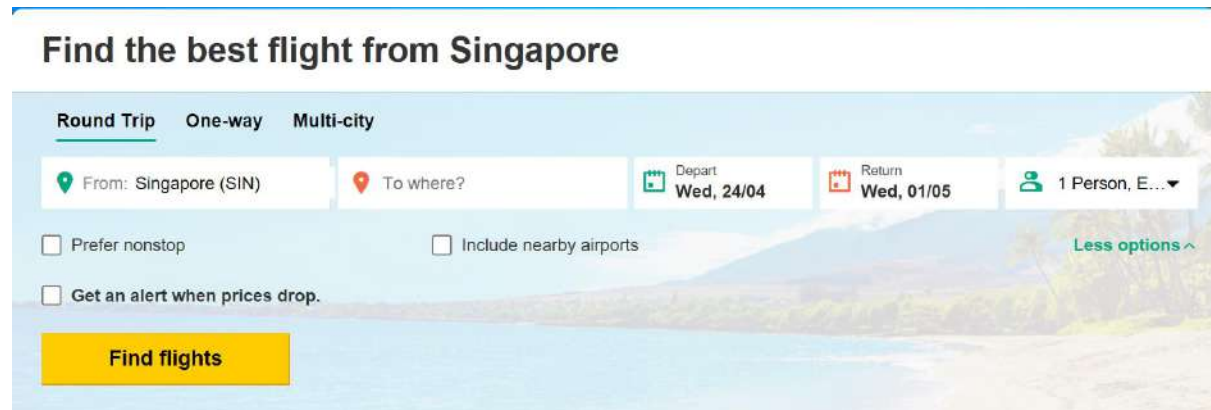
Other normal genetic algorithms operations such as selection, crossover, and mutation should also be included.

Question 2

(Total: 16 Marks)

Adventure Booking and Recommendation Application

Modern travel agencies have developed travel websites, with detailed information and online booking capabilities. By filling in request forms, users can book airline tickets, car rentals, hotels, and other travel related services.



A sample flight booking request form

With the development of AI technologies, it is time to on board intelligent technologies to deal with user's booking requests in the form of natural languages instead of request forms.

Your team is employed to design and build an intelligent system to interact with users through natural conversations (in English) in order to handle flight booking requests, as well as to make recommendation on hotels based on the booking requests and other related information potentially to be collected through the conversation.

Answer the following questions**For the sub-task of flights booking:**

- a. **Provide** several training utterances to detect the intent of **flightbooking** and explain the necessary labels to tag on the keywords or entities. Try to vary the utterances for a good coverage of phrase patterns.

(3 marks)

Write Your Answer Here

- ① I want to book a flight from @sys.geo-city to @sys.geo-city departing @sys.date returning @sys.date for @sys.integer persons.
- ② I want to fly from @sys.geo-city on @sys.date for @sys.integer people.
- ③ What are the flights on @sys.date from @sys.geo-city to @sys.geo-city.

Explanation.

Slots for flight-booking intent.

from/to city \Rightarrow @sys.geo-city.from/to date \Rightarrow @sys.date
@sys-integer.number of passengers \Rightarrow ~~sys-integer~~

- utterances catered for round-trip & single trip.

Other guidelines to answer:

"get a flight for {Date}"

"book a flight on {Date}"

"book {return} flights from {Location} to {Location} on {Date} and {Date}"

"book a {direct} flight for {Date} from {Location} to {Location}"

"May I book a flight from {Location} to {Location} for {Date}"

"book flight from {Location} to {Location} on {Date} for {Number} persons"

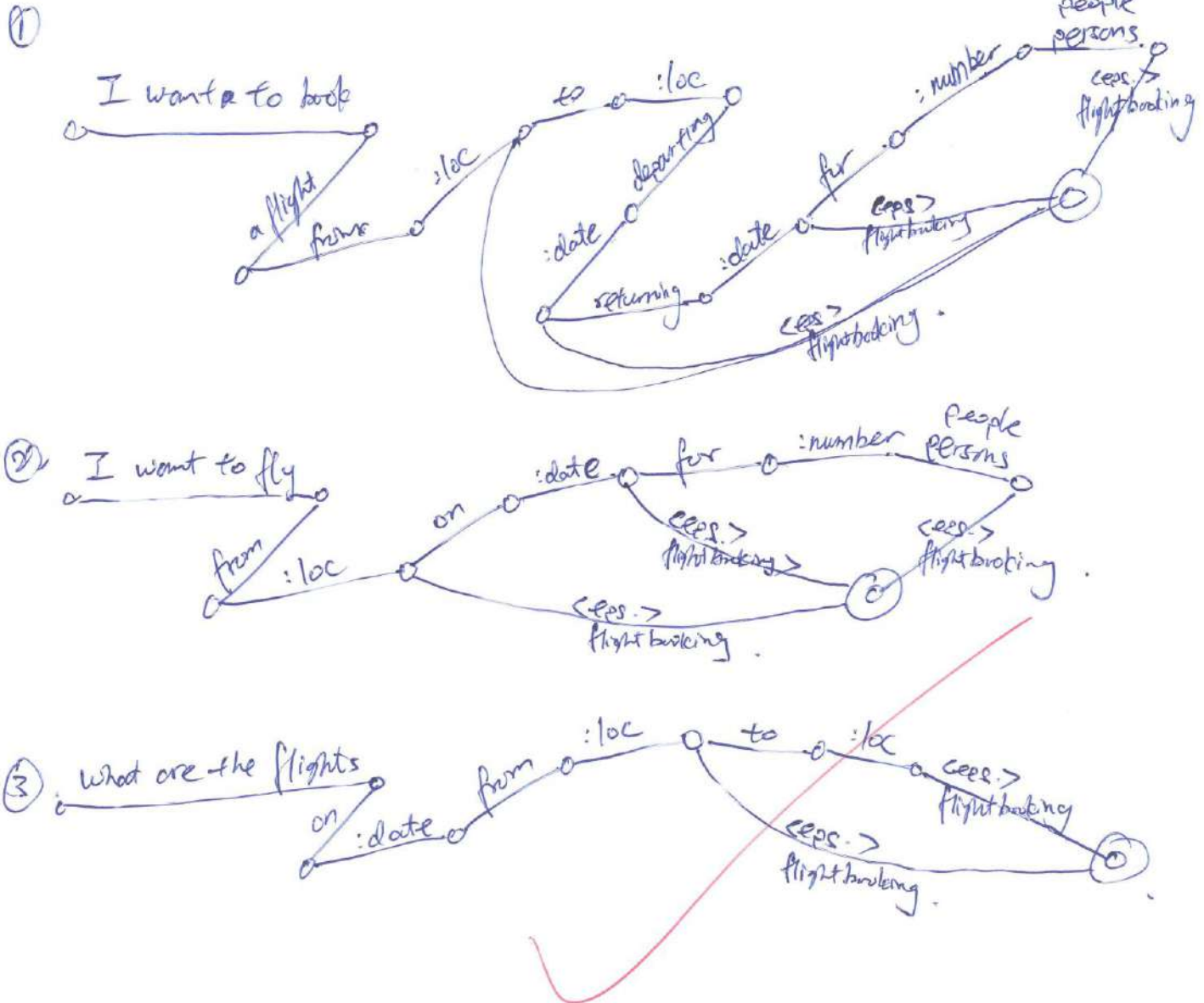
The mandatory labels should be given to “date”, “location” and the keywords “return”

The utterances can be provided with real date values and location values

- b. **Draw** a Finite State Transducers to detect the intents and slots based on the utterances provided in question a.

(3 marks)

Write Your Answer Here

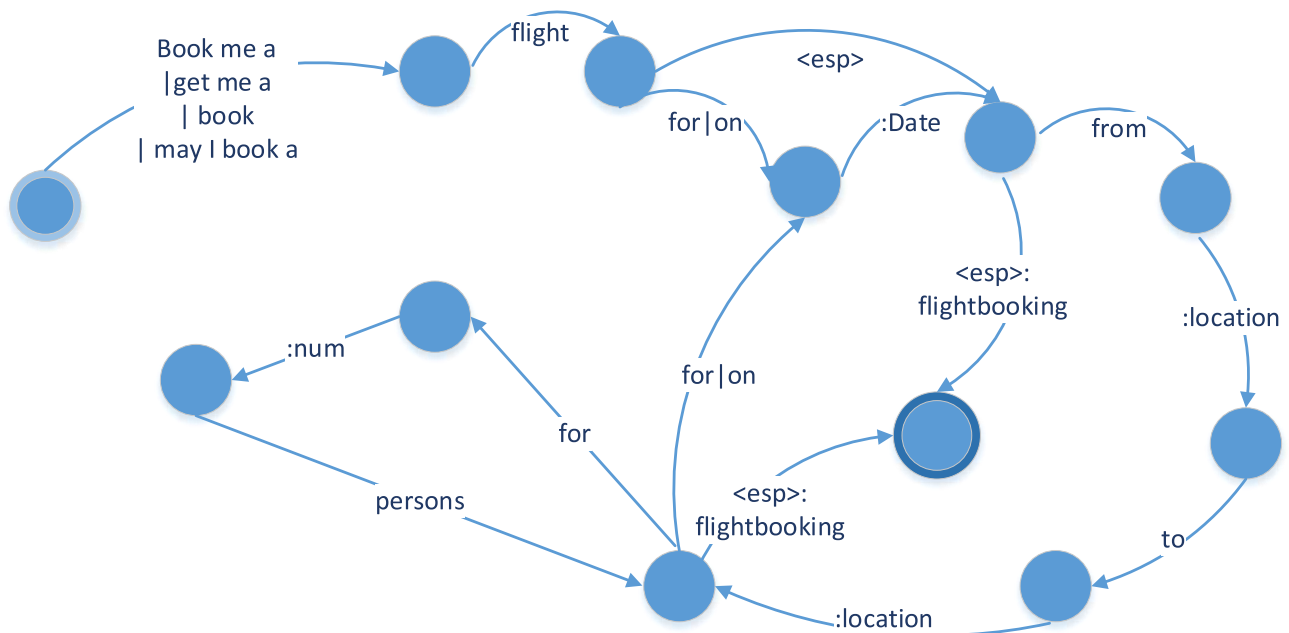


Assumptions

- ① Can accept 1 location and/or 1 date only.
- ② must provide at least 1 location.

Other guidelines to answer:

A sample FST structure would be as follow:



For the sub-task of hotel recommendation:

- c. The recommendation sub-module will initiate a conversation with users to collect the information defined by the request form below. Propose a few technical methods to validate user's responses.

Hint: e.g., to detect an invalid city, date, etc. using which resources or techniques

The form is titled 'Search' and has a yellow background. It contains the following fields:

- Destination/Property Name:** A text input field with 'Dali' entered.
- Check-in Date:** A date picker with a calendar icon and a dropdown arrow.
- Check-out Date:** A date picker with a calendar icon and a dropdown arrow.
- 2 adults:** A dropdown menu showing '2 adults'.
- No children:** A dropdown menu showing 'No children'.
- 1 room:** A dropdown menu showing '1 room'.
- I'm traveling for work:** A checkbox with a question mark icon.
- Search:** A blue button with white text.

A sample hotel booking request form

(3 marks)

Write Your Answer Here

- ① Validation 1 : Destination/Property Name (slot detection)
 - Have custom ^{slot detection} entry listing only valid destinations available for booking.
 - Ask for same field again if invalid/unclear voice.
- ② Validation 2 : Check-in / check-out Date
 - Slot detection → check for valid date transcription.
 - Add rule : WHEN check-out-date < check-in-date THEN Retry.
- ③ Validation 3 : Number of persons and rooms.
 - Assume max. 2 persons + 1 child per room.
 - Add rules: ~~WITHIN num_adults <= 2 AND~~ one room cannot have more than 2 adults and 1 child.

Other guidelines to answer:

The information to be collected (non-exhaustive list):

Date

City

The number of travelers

The number of children

The number of rooms needed

Trip purpose: business or sightseeing

Template/rule-based question-response can be used to shape the conversation with users.

The information provide in the user's response can be checked through regular expression (e.g., for date and numbers related slots) and validated against the knowledge base in specific domain (e.g., dictionary of City names).

d. A set of concepts have been identified as below:

- **Travel:** It represents the information collected for flight booking.
- **Stay:** It represents the intention and slots of the “stay action”
- **City:** It holds the City details
- **Area:** It defines a particular area of a City
- **Hotel:** It holds the hotel details
- **Room:** It holds the room details

Design knowledge bases using Frames/Thematic Role systems for those concepts.

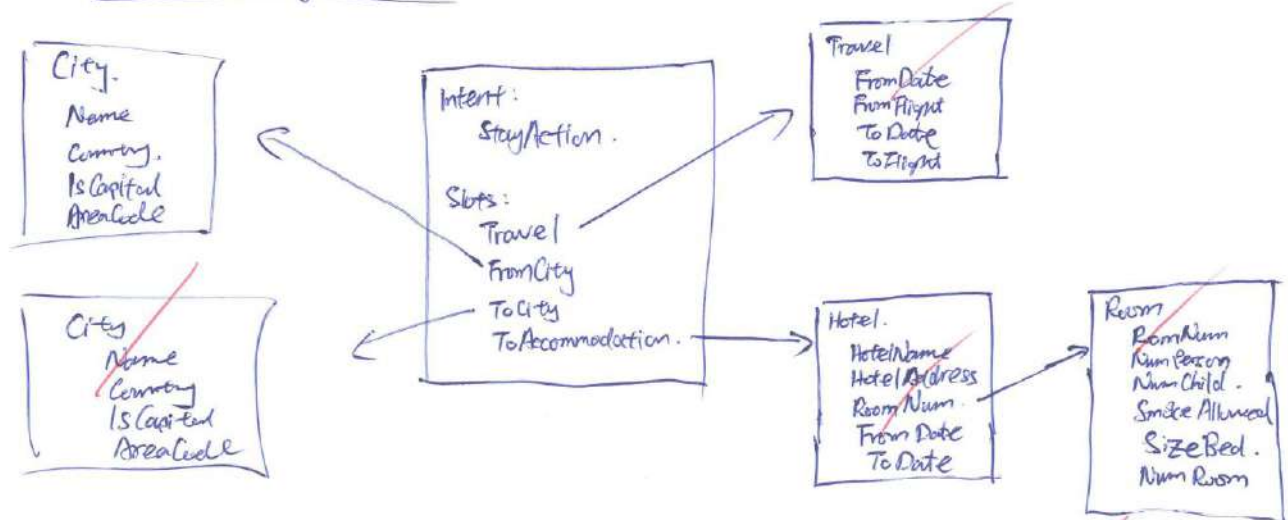
Illustrate the graph-based structure to organize the knowledge with example data.

*Hint: You may only keep the attributes related to the **travel** topic and omit other irrelevant information. Frames should be linked properly*

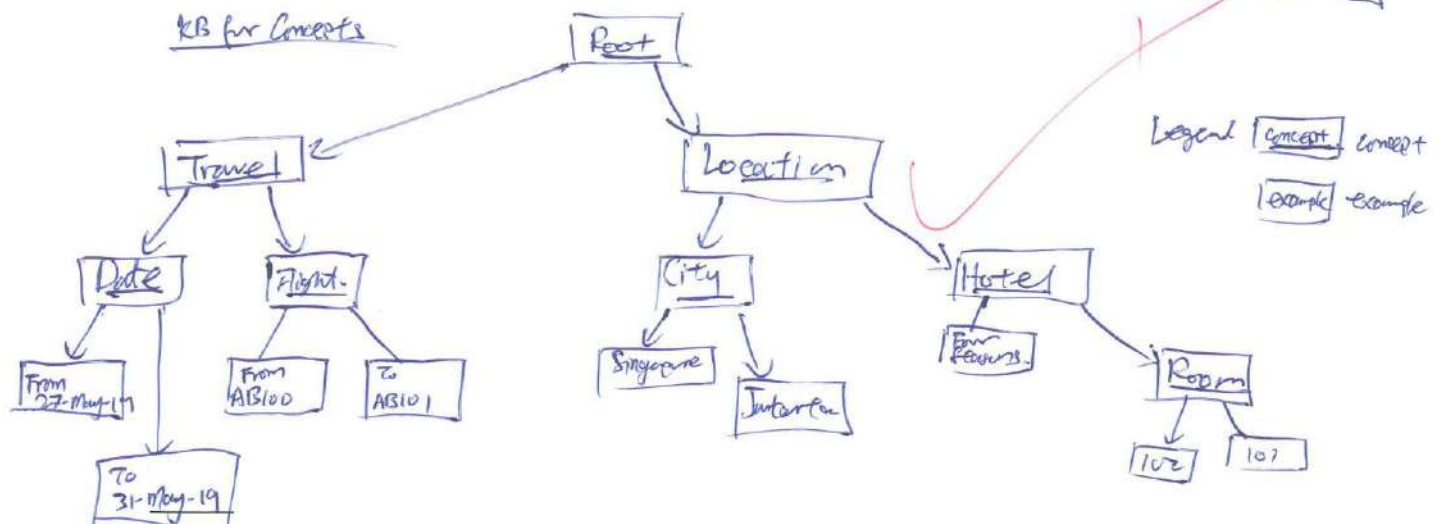
(4 marks)

Write Your Answer Here

Thematic Role System

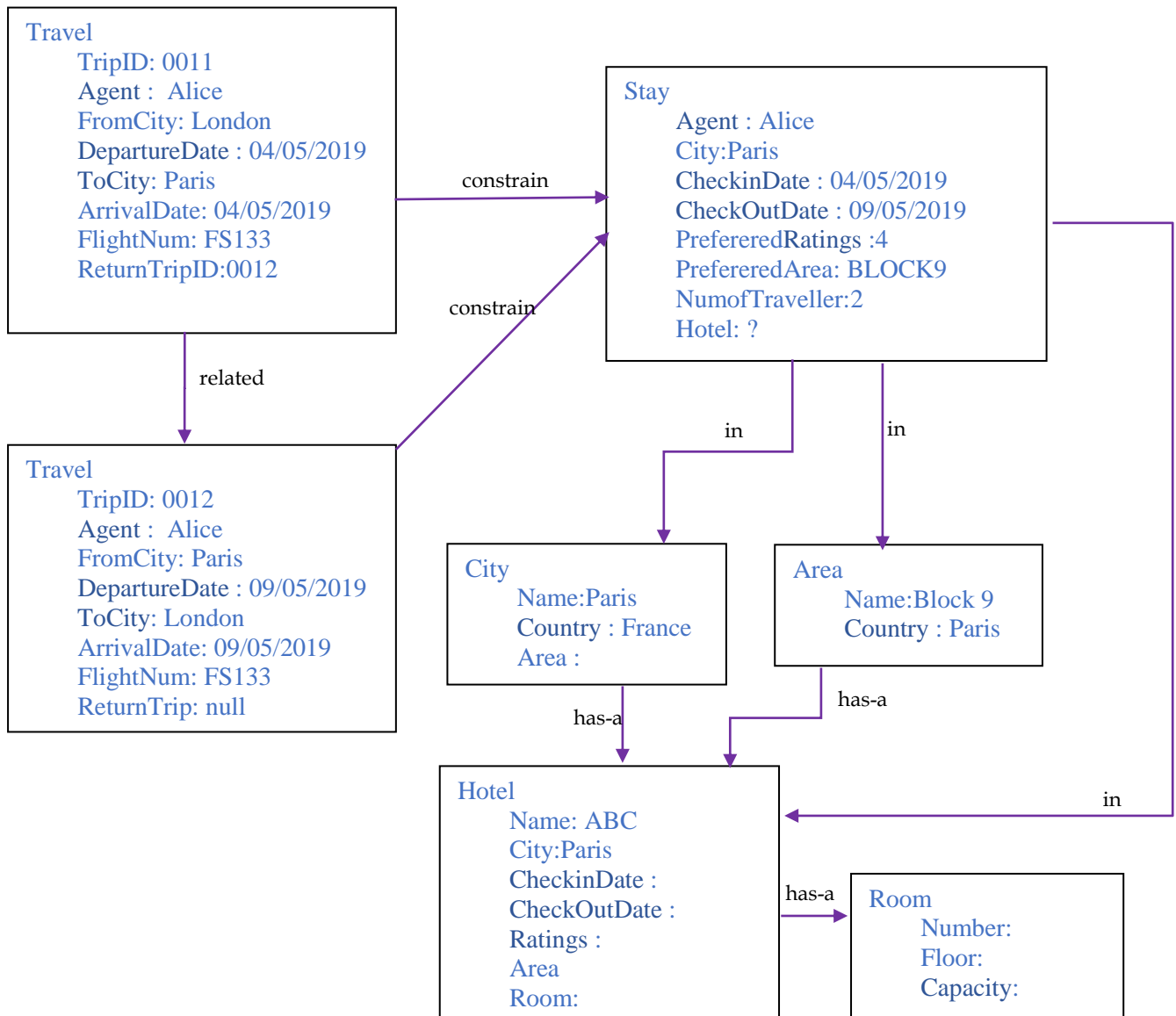


KB for Concepts



Other guidelines to answer:

Frames and thematic roles systems can be used here to represent the knowledge. And the frames should be organized with graph structure. There could be other reasonable tags defined to represent a relationship.



- e. The goal for this task/system is to make flight booking and hotel recommendation through conversational interface, to better sell tickets and/or increase customer loyalty. Based on the design above, **identify one major** technical limitation or business concern of the system, then **propose** your approaches to address this limitation.

(3 marks)

Write Your Answer Here

- One major limitation of this system is the validation of identity of the person booking & subsequently billing this person. Business concern is that there is no way to bill or confirm if it is ~~not~~ a malicious attempt / security breach.
- Approaches to mitigate this issue include:
 - ① Only allow this function post account login.
 - ② Only allow this function for accounts with validated credit card account number.
 - ③ Send confirmation to validated email or mobile so that real customer ~~knows~~ is informed.

Other guidelines to answer:

Students may raise the following limitations as well as other reasonable points

The designed FST may not be able to detect the unseen utterances.

This problem could be solved better with machine learning/NLP method for intent detection and entity recognition. The HMM/CRF/RNN based models can be employed to address the labeling problem.

The information collected for hotel booking may not be enough.

Such as hotel types, hotel ratings and user specific preference etc. could be collected further through conversations.

Some rules and strategies can be designed to improve the efficiency of the system:

Define the compulsory slots to be included by users' response

Deal with the missing data for slots

Design follow up questions when answers are not expected

Design the priorities to rank the hotel based on the intents/slots and knowledge base.

While this system could benefit additional customer with visual impairment, there are customers who have speech impairment or other disability might not be able to operate through the system's conversational interfaces. Possible suggestions include: enable the customer to switch between conversation and web browsing, or remember the customer preferences, and other reasonable mitigations.

END OF EXAM PAPER