7 Discrete models

Group 1
Author: Min Wu(8603148365, DIT025)
Email:minwuh081@gmail.com

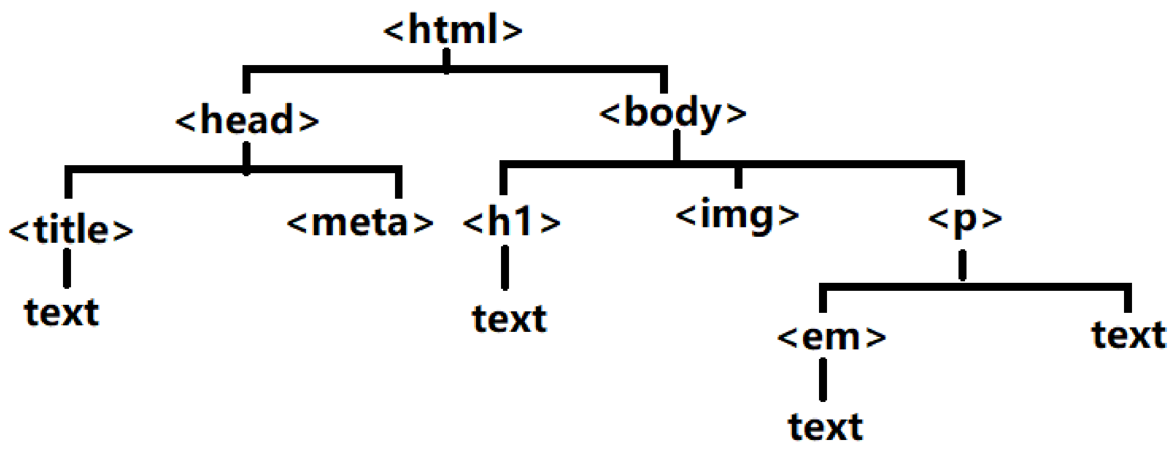
I hereby declare that all solutions are entirely my own work, without having taken part of other solutions.

The number of hours spent: 20hours (Min Wu)
The number of hours has been present in supervision for this module: 0h

(USING BASIC DISCRETE STRUCTURES)
Give applied examples of how you can represent or organize data (or procedures), in terms of each of the following basic mathematical concepts:
Set: unordered collection of items.
A set contains an unordered collection of objects which are called elements of the set.
For example:
Vowels in the Swedish alphabet:
Vowels={a,e,i,o,u,y,ä,å,ö}
The vowels are unordered listed.

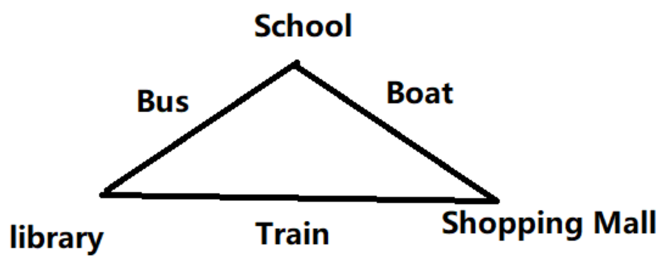
Sequence: sequentially ordered collection of items.
A sequence contains ordered collection of objects, for example, a sequence x1, x2, ..., xN is the ordered collection which means x1 as its first element, x2 as its second element, ..., and xN as its N-th element.
For example:
3D Cartesian coordinates:
(x,y,z)
The first value is for the x-axis, the second value is for the y-axis and the third value is for the z-axis which is ordered.

Tree: branching structure with a root.
A tree is an undirected graph containing branches and bound which means branches are connected by exactly one path.
For example:
HTML web page structure
HTML is the standard markup language for Web pages.



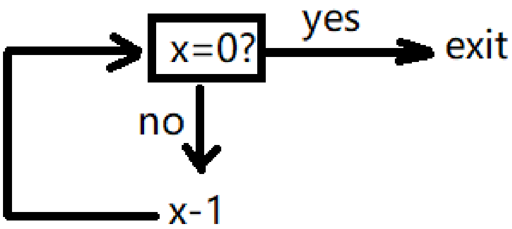
<html> is the root contains two branch <head> and <body>
<head> contains two branch <title> and <meta>
<body> contains three branch <h1>, <img> and <p>
the branches are unorderred collection.

Graph: Structure with vertices and edges
The graph contains a set of objects which are related to each other some pairs of the objects are in some sense "related". The objects are called vertices (also called nodes or points) and the relationships between vertices are called edges (also called link or line).
For example:



A person can take a bus to the library from school or from the school to the library.
A person can take the train from the library to shopping mall or from the shopping mall to the library.
The connection between places is linked without any direction specified.

Directed graph: graph where links are directed (usually represented with arrows)
Weighted graph: graph with a single number for each edge (can be undirected or directed)
A directed graph is a graph with oriented edges. A directed graph is similar to a tree except that the nodes may point to upstreaming nodes. Thus a node can have more than one node pointing to it. This is a loop.
For example:

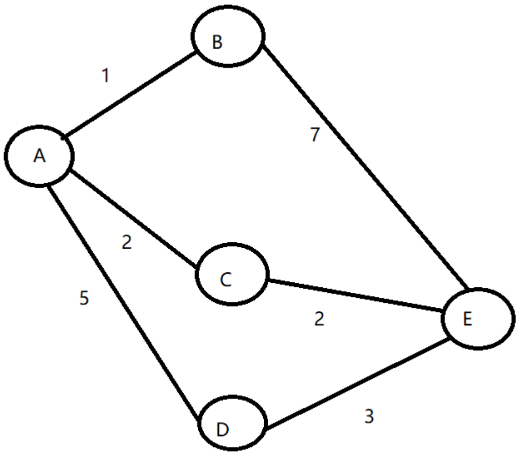


```
while (x !=0)
{x-1}
```

Weighted graph: graph with a single number for each edge (can be undirected or directed)

In a weighted graph, a single number is assigned to each edge, the number can represent distance, time or other properties. A weighted graph is used to find out the minimal results, for example, the shortest problem.

For exampel:



A site to E site through B, C and D. The time spent is illustrated in the graph. Try all the pathways and to find out the shortest path.

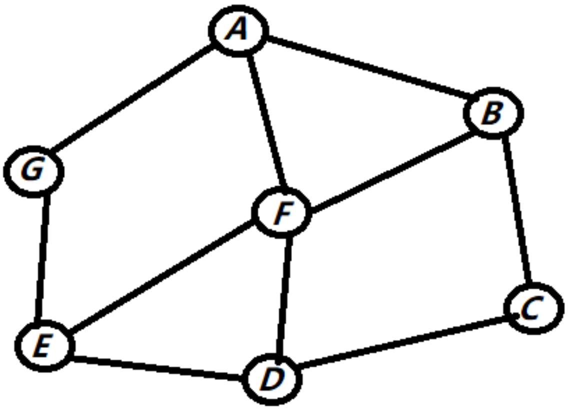
(MATHEMATICS VERSUS DATA STRUCTURES)
What are your thoughts about the relationship between discrete mathematical concepts as these mentioned above, and data structures in programming.

Boolean algebra and logic play critical roles in programming as well as discrete math. Discrete mathematical concepts is used to design proof which is used in programming algorithms. Arrays and data structures are all about sets, trees and matices. Recursion is used in loops. All the discrete mathematical concepts are represented in programming.

(MAP COLOURING)

This problem is about how many colours you may need to colour a map so that neighbouring countries have different colours.

a) Suggest how to model this problem as a graph problem (i.e. as a problem on a graph).



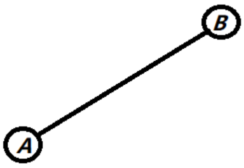
The graph:

The nodes are countries.

The lines represent two countries are neighbouring.

b) Try to figure out how many colours you may need to colour any map (a finite number or possibly infinitely many)? Create examples as you need to try out.

Countries: 3

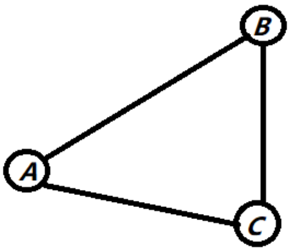


lines: 3

The maximal neighbouring countries of a country:1

color: 2

Countries: 3



lines: 3

The maximal neighbouring countries of a country:2

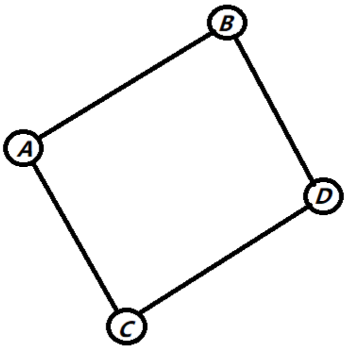
color: 3

Countries: 4

lines: 4

The maximal neighbouring countries of a country:2

color: 3

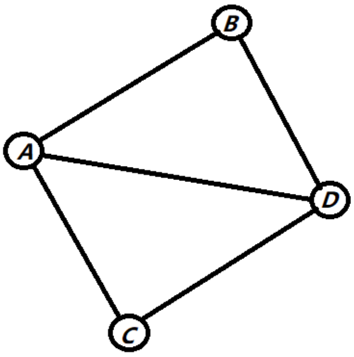


Countries: 4

lines: 5

The maximal neighbouring countries of a country:3

color: 4



It is a finity number and the number of colors needed depends on the maximal number of neighbouring countries +1 (the maximal lines drawn from a country + 1)

(SORTING COMPLEXITY)

Many common sorting algorithms are based on the idea of pairwise comparisons (insertsort, mergesort, quicksort etc.). The time complexity of such algorithms are often O(n^2) or O(n log n) (better), which means that the number of steps such an algorithm may need in the worst case is proportional to n log n, where n is the number of items to be sorted. This is often written using the shorthand notation

O(n log n) where O means “order of”, sometimes called big O notation. We will here consider a slightly more abstract result, namely that any comparison-based algorithm will need at least n log n comparisons in the worst case. Read and understand the theorem and the proof. Explain the main ideas.

One version of the proof

Comparison sort in general Please search as you like if you need more links about this - include any references you have used.

Big O notation provides a way to describe how the times takes to run a function growth as the size of input.

For exampel:

One array it contains 9 elements A=[1,2,3,4,5,6,7,8,9],

First, to calculate sum of then defined using python:

```
def sumArray(A):
        total=0;
        for a in A:
                total=total+a;
        return total;
```

Second, to make a function which is independent on this array.

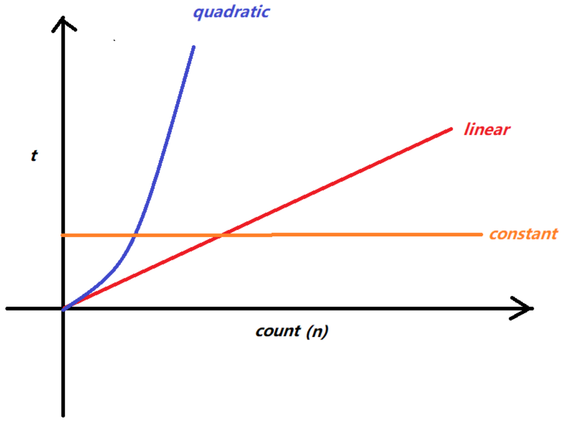
```
def constantArray(A):
        total=1;
        return total;
```

How long will it take to run this function? It might depend on:

1. Performance of the computer.
2. The running environments.
3. The input data.

The big O notation is used to evaluate the third factor.

The number of elements vs the running time vs are plotted as below:



- The relationship between the number of elements and the running time is linked to a linear function for 1d sum function.
- The relationship between the number of elements and the running time is linked to a constant for the function which is independent of the input.

Now there is a 2d array A = [[1,2,3], [4,5,6], [7,8,9]] to calculate the sum of this array.

```
def sum2dArray(A):
        total=0;
        for a in A:
                for b in a:
                        total=total+a;
        return total;
```

- The relationship between the number of elements and the running time is linked to quadratic function for this 2d-sum function.

The relationship between the number of elements and the running time is linked to a constant for the function which is independent of the input.

constant relationship: time = O(1) -> time = constant

linear relationship: time= an+b if n is very large time ≃ an ≃ n, so time ≃ O(n)

quadratic relationship: time= an^2 + bn +c, if n is very large, then an^2 is much bigger than bn, so an is the biggest growing term. time ≃ n^2 ≃ O(n^2)

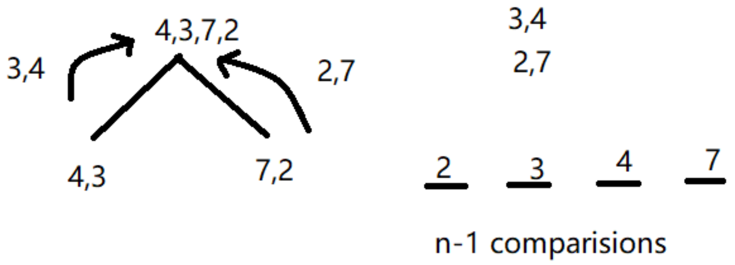
Big O notation definiation:

- using the biggest growing term
- taking out the coefficient.

Furthermore, the relationships between time and the number of input is independent of the operating environment and computer language.

For a sorting problem:

For example: mergesort



1. Split the list into two list and then to four and ... until it only contains one or two elements in the list
2. sort the list which has two elements and return the list which contains only one element.
3. Using the merge sort method to sort two list and return to the upstream.

By using the merge sort, the comparison is n-1 times, where is the n elements in the list.

O(n)=O(n/2)(left)+O(n/2)(right)+(n-1)

for n is 4

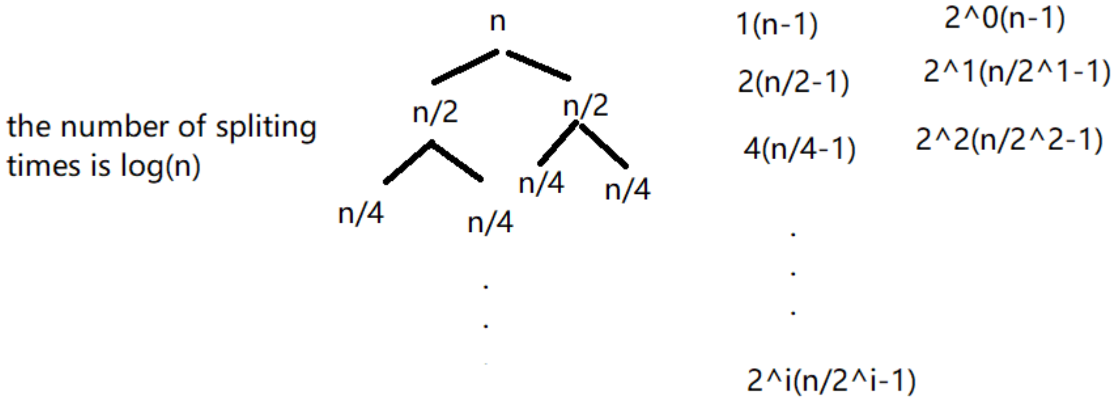
O(4)=O(2)+O(2)+4-1, where O(2)=O(1)+1

Assume O(1)=0

O(2)=1

O(4)=2+3=5

For n



The i is the level. The number of spliting times is log(n)

The sum of 2^i(n/2^i-1) will be the O(n)

$$\sum_{i=0}^{log(n)-1} 2^{i}(n/2^{i}-1)$$

$$= \sum_{i=0}^{log(n)-1} n-2^{\hat{\imath}}$$

=nlog(n)

(investigating the world)

(BALANCING CHEMICAL REACTIONS)

We will here consider a common type of problem where a reaction is known in terms of which compounds are involved, but where the actual number of molecules is not. For example, consider the reaction for burning propane (e.g. in a propane cooker): C3H8 + O2 —> CO2 + H2O

a) Model the problem as a system of diophantine equations, i.e. equations where the variables must be integers.

Assume x C3H8 and y O2, x and y are integers
so C=3x, H=8x and O=2y
C is only in CO2 and H is only in H2O
so
CO2 is 3x
H2O is 4x
then
6x*O+4x*O=2y*O
so

$10x=2y$
$5x=y$
$5x-y=0$
b) Solve with the Mathematica function FindInstance. (Another similar problem is when you know the weight percentage of the atomic elements in a compound, and you want to determine the molecular formula for the compound)

I tried my best but I couldn’t solve it because missing the other diophantine equations, will correct it after follow-up lecture

(designing)

(PROJECT PLANNING PROBLEM)

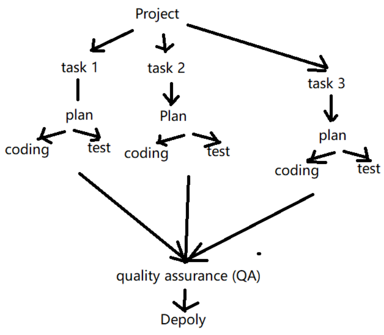
Industrial projects where many people are involved are usually split into smaller tasks that are scheduled with their own starting time, duration and deadline. Several tasks can be ongoing in parallel, but if a task is dependent on other tasks it cannot begin until these tasks are completed. In this problem we will consider how a directed network can be used for planning and management of such projects.

a) Explain how a directed graph can be used to model a number of tasks in a project. Each task is assumed to have a given duration and may be dependent on the completion of other tasks.

The directed graph can be used to design the workflow. The project is cut into many small tasks. Through the directed graph, people can know which tasks can be done parallelled what task needed to be finished before the project can go further. The directed graph can be useful to set the priority of each task.

b) An important question is the minimum possible time to complete the project. For this purpose, determine how a shortest path algorithm can be used to find the critical path = the sequence of tasks that determines the minimum total length of the project. Hint: 1) make up a simple example and you will understand what we are asking for. 2) make sure you understand what problem it is that you want to solve, 3) only thereafter think about how to model your problem as a shortest path problem. Also make sure you did a) before you begin with b).

An example in a project of software deploy.



If the time is limited, the shortest pathway to deploy a program should be to code it and deploy it directly without testing anything, but risks, of course, are increased which might increase the time in solving bugs in the future. If the time is limited, the risk requirement needed to be evaluated and the tasks of testing need to be planned to those blocks which could cause big problems instead of testing everything before deploy. The bug reports can be used instead to mark the defects or bugs and solve them later, for example, in the next version.

d) In practice it may be the case that the exact duration of the tasks is not known. Suggest how the model could be extended to handle this. What useful things could be done with such an extended model and how? How easy would such a model be to use?

If the duration of the tasks become more clear, I could add extra branches if the extra tasks can run parallelled or extend the branch and estimate the time needed for the extension and the correlations to the upstream/downstream works. It is easy to use this model because it is easy to show the needs and the priorities for each task.

(RSA CRYPTOSYSTEM)

Explain in your own words the RSA cryptosystem and the main ideas behind. Try to do it to provide easy understanding of the main ideas, and also in sufficient detail so that someone who understands your explanation should be able to implement it. Feel free to search and use any sources - just list the references you have used. This is a nice more complete explanation. For modulo arithmetic in general, see the mathematical knowledge section below.

RSA cryptosystem is a method used to encrypt and decrypt messages.

Two key generated (private key and public key) using RSA cryptosystem

public-key -> encrypt message

private key -> decrypt message

Generate two keys

1. need two prime numbers pq for example (7,11)
2. calculate n which equals n=pq for example 91= 7*13
3. calculate qn which equals (p-1)(q-1) for example 72=(7-1)(13-1)
4. choose an integer k which is between 1 and qn, and k does not share any factor with qn, for example, k= 5 (1-72)
5. calculate d which equals d*k=1+xqn (where x is an integer) for example x=2 d*k=1+144 d=29 when k=5 so (d,k)=(29,5)

The public key is (n,k) for example (91,5). The public key can be kept well-known.

The private key is (n,d) in which d is kept in secret for example (91,29).

To encrypt a message:

For example:

Using public key (n,k) for example (91,5) here, I want to send a message with only one character “B”

1. Character B convert to numeric number for example 2.
2. Calculate c equals 2^k mod n = 2^5 mod 91 c=32
3. The other person will get the message c =32

To decrypt a message:

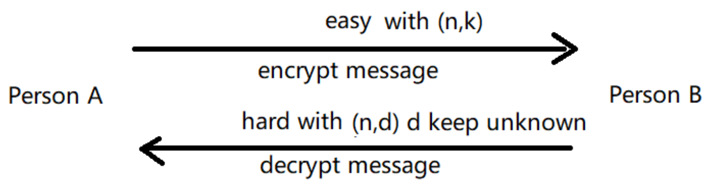
Using private key (n,d) for example (91,29) here, If I get the number 32

1. calculate 2^d mod n using (n,d)=(91,29), which is 32^29 (mod) 91 = 2.
2. convert 2 to the message B

If I don’t know the d (29 here), it will be very hard to reach 2.

Main Idea.

The way to encrypt message using public key is easy to do. but the decrypt message by the public key is very hard if the d is not known.



(thinking)

(GOOD EXPLANATIONS)

a) Have a look at some solutions to the problems in the course, explained in a simple but reasonably good way. Note the flow of the explanations and compare with your 3 own explanations. You are here encouraged to not mainly focus on the answer itself but rather on how it is explained. What are your observations?

For the problems map coloring problem.
I showed the explanation by first give some initial simple examples, and then find out the potential relationship between the number of different colors and the neighboring countries.
Give same simple examples -> guess the possible relationships-> draw a conclusion
For big O notation problem.
I showed the explanation:
First, explain what is big O notation, what is used for and how it can be used.
Second, explain in sorting problems.
Third relating the big O notation with the sorting problem to get the results O(n log (n))

Explain the mathematical method -> applied the method to solve a problem -> draw a conclusion

For the problem (MEDICAL TEST) in module 6
First, transfer the information using a table
Second, Apply the mathematical method to the information
Third, present a conclusion to the results.

analyze the information -> transfer the information to the data in a table -> draw a conclusion
b) Can you relate the flow of an argument or explanation to some mathematical concepts in this module?

DISCRETE STRUCTURES explanation

explain the different discrete structures
differences between those discrete structures
give an example for each discrete structure (relate the discrete structure to the programming methods)

c) How would you say that reasoning and explaining is related?

The explaining is based on answering the questions related to “what”, “why” and “how” so the reasoning- explaining (why - because) is one of the ways of explaining an object.

(SELF-CHECK)

passed