Ve203 Discrete Mathematics

Sample Exercises for the Second Midterm Exam

The following exercises are sample exercises of a difficulty comparable to those found the actual second midterm exam. The exam will usually include of 4 to 5 such exercises to be completed in 100 minutes.

Exercise 1. The *selection sort* algorithm begins by finding the least element in a list. This element is moved to the front. Then the least element among the remaining elements is found and put into the second position. This procedure is repeated until the entire list has been sorted.

i) Give the pseudocode for an iterative implementation of selection sort. You may refer to the procedure min in Exercise **??**.

ii) Give a big-O estimate for the number of comparisons necessary to sort a list of n elements.

(4+2 Marks)

Solution.

i) The pseudocode is as follows:

```
Require: $selsort(a_1, a_2, \ldots, a_n\colon$ distinct integers$)$
  for $i = 1$ to $n - 1$ do
    $min := a_i$
    $k := 1$
    for $j = i + 1$ to $n$ do
      if $min > a_j$ then
        $min := a_j$
        $k := j$
      end if
    end for
    $c := a_i$
    $a_i := a_k$
    $a_k := c$
  end for
```

(4 Marks)

ii) We need $O(n)$ searches of lists of length $O(n)$ to find the smallest element, and each search has complexity $O(n)$. Thus, the entire algorithm needs $O(n)O(n) = O(n^2)$ steps. **(2 Marks)**

Exercise 2. A computer network consists of 6 computers. Each computer is directly connected to 0 or more of the other computers. Show that there are at least two computers in the network that are connected to the same number of other computers.
(2 Marks)

Solution. The network can not contain both one computer connected to every other computer and one computer connected to no other computer. Let C be the set of six computers and N the set of the number of network connections to other computers. Then either $N = \{0, \ldots, 4\}$ or $N = \{1, \ldots, 5\}$. **(1 Mark)** In any case, $|N| = 5$ and $|C| = 6$, so the map $C \to N$ is not injective by the pigeonhole principle. **(1 Mark)**

Exercise 3. Show that if seven integers are selected from the set $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, there must be at least two pairs of these integers with the sum 11.
(4 Marks)

Solution. There are five groups of pairs with sum 11:

$$A_1 = \{1, 10\}, \qquad A_2 = \{2, 9\}, \qquad A_3 = \{3, 8\}, \qquad A_4 = \{4, 7\}, \qquad \text{and} \qquad A_5 = \{5, 6\}$$

If we select seven integers from N, then by the pigeonhole principle at least two of them come from the same subset A_i. Once we have these two from the same group, there are five more integers and four groups. Again, the pigeonhole principle guarantees two integers in the same group. This gives us two pairs of integers, each pair from the same group. In each case these two integers have a sum of 11.

Exercise 4. Find all solutions of following the recurrence relations:

i) $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n$

ii) $a_n = 2a_{n-1} - 2a_{n-2}$, $a_0 = 1$, $a_1 = 2$.

(4+2 Marks)

Solution.

i) We first solve the homogeneous equation $a_n - 4a_{n-1} + 4a_{n-2} = 0$. Setting $a_n = r^n$, we obtain
$$r^2 - 4r + 4 = 0.$$
This equation has a single root $r = 2$, so the general homogeneous solution is given by
$$a_n^{\text{hom}} = c_1 \cdot 2^n + c_2 \cdot n2^n.$$
A particluar solution of the imhomogeneous equation is found through the ansatz
$$a_n^{\text{part}} = (b_0 + b_1 n)n^2 2^n.$$
This gives
$$(b_0 + b_1 n)n^2 2^n - (b_0 + b_1 n - b_1)(n-1)^2 2^{n+1} + (b_0 + b_1 n - 2b_1)(n-2)^2 2^n = (n+1)2^n$$

or

$$(b_0 + b_1 n)n^2 - (2b_0 + 2b_1 n - 2b_1)(n^2 - 2n + 1) + (b_0 + b_1 n - 2b_1)(n^2 - 4n + 4) = n + 1.$$

Simplifying further,

$$\begin{aligned} -(2b_0 + 2b_1 n - 2b_1)(-2n + 1) + (b_0 + b_1 n - 2b_1)(-4n + 4) &= n + 1 \\ \Leftrightarrow 6b_1 n + 2b_0 - 10b_1 &= n + 1 \end{aligned}$$

so we have $b_1 = 1/6$ and $b_0 = 4/3$. The general solution is hence

$$a_n = c_1 \cdot 2^n + c_2 \cdot n2^n + \frac{1}{6}n^2 2^n + \frac{4}{3}n^3 2^n.$$

ii) Setting $a_n = r^n$, we obtain

$$r^2 - 2r + 2 = 0.$$

This equation has complex roots $r = 1 \pm i$. The general solution is

$$a_n = c_0(1 + i)^n + c_1(1 - i)^n.$$

The initial conditions give

$$c_0 + c_1 = 1, \qquad c_0 + c_1 + (c_0 - c_1)i = 2$$

or

$$c_0 + c_1 = 1, \qquad c_0 - c_1 = -i$$

Hence $c_0 = 1 - i/2$, $c_1 = 1 + i/2$ and we obtain

$$a_n = (1 - i/2)(1 + i)^n + (1 + i/2)(1 - i)^n.$$

Exercise 5.

i) Solve the simultaneous recurrence equations

$$a_n = 3a_{n-1} + 2b_{n-1}, \qquad b_n = a_{n-1} + 2b_{n-1}$$

with $a_0 = 1$, $b_0 = 2$.

ii) Let f be an increasing function. Find a big-O estimate for $f(n)$ if

$$f(n) = 5f(n/4) + 6n.$$

(4+4 Marks)

Solution.

i) Observe that

$$a_n + b_n = 4(a_{n-1} + b_{n-1}).$$

Set $c_n = a_n + b_n$. Then $c_n = 4c_{n-1}$ and $c_0 = 3$. It follows that $c_n = 3 \cdot 4^n = a_n + b_n$. Hence,

$$b_n = b_{n-1} + 3 \cdot 4^{n-1}.$$

A particular solution is $b_n = 4^n$, which satisfies $b_0 = 1$. The homogeneous system $b_n = b_{n-1}$, $b_0 = 2 - 1 = 1$ has solution $b_n = 1$. We obtain

$$b_n = 1 + 4^n$$

and from $3 \cdot 4^n = a_n + b_n$ we have $a_n = 2 \cdot 4^n - 1$.

ii) Suppose that $n = 4^k$ for some $k \in \mathbb{N}$. Then, assuming k is large enough, we have

$$\begin{aligned} f(n) &= 5f\left(\frac{n}{4}\right) + 6n \\ &= 5\left(5f\left(\frac{n}{4^2}\right) + 6\frac{5}{4}\right) + 6n \\ &\vdots \\ &= 5^k f(1) + 6n\left(1 + \frac{5}{4} + \cdots + \left(\frac{5}{4}\right)^{k-1}\right) \\ &= 5^k f(1) + 6 \cdot 4^k \frac{1 - (5/4)^k)}{1 - 5/4} \end{aligned}$$

This formula can be proved by induction: for $k = 1$ it is obviously true and assuming that it holds for k, we have

$$\begin{aligned} f(4^{k+1}) = 5f(4^k) + 6 \cdot 4^k &= 5^{k+1} f(1) + 5 \cdot 6 \cdot 4^k \frac{1 - (5/4)^k}{1 - 5/4} + 6 \cdot 4^k \\ &= 5^{k+1} f(1) + 6 \cdot 4^{k+1} \frac{5/4 - (5/4)^{k+1} + 1 - 5/4}{1 - 5/4} \\ &= 5^{k+1} f(1) + 6 \cdot 4^{k+1} \frac{1 - (5/4)^{k+1}}{1 - 5/4}. \end{aligned}$$

Hence,

$$f(4^k) = 5^k f(1) + 6 \cdot 4^k \frac{1 - (5/4)^k)}{1 - 5/4} = 5^k f(1) + 24(5^k - 4^k) = O(5^k)$$

as $k \to \infty$. This implies that $f(n) = O(5^{\log_4 n})$ as $n \to \infty$ when $n = 4^k$. Since f is increasing, we see that for arbitrary n there exists some k such that $f(4^k) \leq f(n) \leq f(4^{k+1})$, so $f(n) = O(5^{\log_4 n})$ as $n \to \infty$ without any restriction on n.

[Quoting the Master Theorem is also sufficient, but do not award marks if a student gets the answer wrong in this case.]

Exercise 6. Find the percentage of 7-digit numbers (i.e., numbers between 1,000,000 and 9,999,999) that have seven distinct digits.
(4 Marks)

Solution. There are 9,000,000 distinct seven-digit integers. **(1 Mark)** The number of such integers that have all digits distinct can be computed as follows: The first digit can be selected in nine ways (since 0 is not allowed). The subsequent six digits, if no digits are to repeat, can be selected in $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 9!/3!$ ways. **(1 Mark)** Altogether the proportion of all seven-digit integers with all digits distinct is

$$p = \frac{9 \cdot 9!/3!}{9 \cdot 10^6} = \frac{9 \cdot 6720}{10^6} = 0.06048,$$

so 6.048% of all 7-digit numbers have distinct digits. **(2 Marks)**

Exercise 7. Consider an alphabet A,B,C,D. When we transmit a letter it is sometimes corrupted by noise. Assume that there is a probability $p = 0.1$ of error. To protect the communicagtion from errors, instead of transmitting once, we transmit the same letter three times in a row (e.g. to send C we send CCC). The receiver will decode the message by deciding the letter that occurs the most often. If there is no single letter that is most frequent, then the message is not decoded. For example, CBC will be decoded as a "C".

The letter A is transmitted in this way. What is the probability that the receiver correctly decodes a transmission?
(3 Marks)

Solution. The transmission will be decoded as "A" if either of the following signals is received:

$$AAA,\ AAX,\ AXA,\ XAA,$$

where X stands for either B, C or D. We have

$$P[AAA] = 0.9^3, \qquad P[AAX] = P[AXA] = P[XAA] = 0.9^2 \cdot 0.1$$

so the probability that an "A" is decoded is

$$p = 0.9^3 + 3 \cdot 0.9^2 \cdot 0.1 = 0.9^2 \cdot 1.2 = 0.81 \cdot 1.2 = 0.972.$$

Exercise 8. The letters I, I, I, I, M, P, P, S, S, S, S are arranged at random. What is the probability that the arrangement will spell MISSISSIPPI?
(3 Marks)

Solution. We can solve this problem treating the choices of consecutive letters as "operations." The first operation must give the letter M; hence there is only one way of choosing it. The next letter (out of the remaining 10) must be an I, and it can be selected in 4 ways. Proceeding in this way, the sequence of consecutive 11 choices leading to the word MISSISSIPPI can be performed in $1 \times 4 \times 4 \times 3 \times 3 \times 2 \times 1 \times 2 \times 2 \times 1 \times 1$ ways, which equals 4!4!2!1!. On the other hand, the total number of ways one can perform the operations of consecutively choosing letters from the set is 11!. Consequently, the required probability is

$$p = \frac{4!4!2!1!}{11!}.$$

Exercise 9. The RSA cryptosystem is based on encrypting plaintext M to ciphertext C by setting

$$C = M^e \bmod n,$$

where e is the exponent of encryption and n is taken to be the product of two (large) prime numbers. Explain why the cipher would not be secure, i.e., M could be obtained from C without excessive calculational effort, if n were a large prime number and not the product of two primes.
(3 Marks)

Solution. Suppose that we use a prime for n. To find a private decryption key from the corresponding public encryption key e, one would need to find a number d that is an inverse to e modulo $n-1$. Then

$$de = 1 + k(n-1)$$

for some $k \in \mathbb{Z}$ and

$$C^d \equiv M^{ed} \bmod n \equiv M^{1+k(n-1)} \bmod n \equiv M \cdot (M^{n-1})^k \bmod n.$$

Since $M^{n-1} \equiv 1 \bmod n$ by Fermat's Little Theorem, $C^d = M$ and the plaintext is regained. **(2 Marks)**
But finding such a d is easy because $n-1$ is known. **(1 Mark)** For example, the Euclidean algorithm can be used.