

# COMP3121

## Assignment 2

### A17S1N2

Evangelos Kohilas  
z5114986

By submitting this document you are confirming that all the answers are your work and are not take from any other sources unless clearly mentioned.

### Question 1

a)

$$\text{let } A^n = \begin{pmatrix} F(n+1) & F(n) \\ F(n) & F(n-1) \end{pmatrix} \quad (1)$$

When  $n = 1$

$$A^1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad (2)$$

Assume  $n = k$

$$A^k = \begin{pmatrix} F(k+1) & F(k) \\ F(k) & F(k-1) \end{pmatrix} \quad (3)$$

let  $n = k + 1$

$$A^{k+1} = AA^k \quad (4)$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F(k+1) & F(k) \\ F(k) & F(k-1) \end{pmatrix} \quad (5)$$

$$= \begin{pmatrix} F(k+1) + F(k) & F(k) + F(k-1) \\ F(k+1) & F(k) \end{pmatrix} \quad (6)$$

$$= \begin{pmatrix} F(k+2) & F(k+1) \\ F(k+1) & F(k) \end{pmatrix} \quad (7)$$

Therefore the formula is true by induction for all  $n > 0$ .

b)  $F(n)$  can be found in  $\log_2(n)$  matrix multiplications using a recursive algorithm

```
matrix = ((1, 1), (1,0))
func(n):
    if n == 1:
        return matrix
    if n is even:
        return func(n/2)^2
    if n is odd:
        return func(n-1) * matrix
```

## Question 2

a) First we calculate the Karastuba trick.

$$(a + b)(c + d) = ac + ad + bd + bc \quad (1)$$

$$ad + bd = (a + b)(c + d) - ac - bc \quad (2)$$

Then we substitute (2) into (4)

$$(a + ib)(c + id) = ac + adi + bdi + bc \quad (3)$$

$$= ac + i(ad + bd) + bc \quad (4)$$

$$= ac + i((a + b)(c + d) - ac - bc) + bc \quad (5)$$

Thus only requiring 3 real number multiplications.

b) First we calculate

$$a^2 - b^2 = (a + b)(a - b) \quad (1)$$

Then we substitute (1) into (2)

$$(a + ib)^2 = a^2 - b^2 + 2abi \quad (2)$$

$$= (a + b)(a - b) + 2abi \quad (3)$$

Thus only requiring 2 real number multiplications

c) By re-arranging by the laws of exponents:

$$(a + ib)^2(c + id)^2 = ((a + ib)(c + id))^2$$

Thus from above, we then calculate the middle multiplication using 3 real number multiplications, and then we find the square as above using 2 more real number multiplications.

## Question 3

Expand  $P(x)$  and  $Q(x)$  as follows.

$$P(x) = a_0 + x^{17}(a_{17} + a_{19}x^2 + a_{21}x^4 + a_{23}x^6)$$

$$Q(x) = b_0 + x^{17}(b_{17} + b_{19}x^2 + b_{21}x^4 + b_{23}x^6)$$

let  $y = x^2$  so that

$$R_a(y) = a_{17} + a_{19}y + a_{21}y^2 + a_{23}y^3$$

$$R_b(y) = b_{17} + b_{19}y + b_{21}y^2 + b_{23}y^3$$

then

$$P(x)Q(x) = a_0b_0 + x^{17}(a_0R_b(x^2) + b_0R_a(x^2)) + x^{34}R_a(x^2)R_b(x^2)$$

through brute force, we then calculate

$a_0b_0$  to require 1 multiplication

$a_0R_b(x^2)$  and  $b_0R_a(x^2)$  to require 4 multiplications each

then to multiply  $R_a(x^2)R_b(x^2)$  (of degree 3), we require  $2(3) + 1 = 7$  multiplications using the generalised Karatsuba method.

and so we get  $1 + 4 + 4 + 7 = 16$  multiplications of large numbers.

## Question 4

As  $P(x)$  has all 15 roots of unity, and  $x^{15} - 1$  and  $P(x)$  are both of the same degree and are both monic then it follows that

$$P(x) = x^{15} - 1$$

## Question 5

For any input  $(a_0, a_1, a_2, \dots, a_{2^n-1})$ , we can describe  $a_i$ 's new position by converting  $i$  to  $n$  binary places and finding the reversed sequence. e.g.  $6 \rightarrow 110 \rightarrow 011 \rightarrow 3$

## Question 6

let

$$f_m = \sum_{i+j=m} (j+1)q_jq_i \quad (1)$$

$$p_j = (j+1)q_j \quad (2)$$

then substitute (2) into (1)

$$\sum_{i+j=m} p_jq_i = \vec{p} * \vec{q} \quad (3)$$

as (3) is a linear convolution,  $f_m$  can be computed in  $O(n \log n)$  time by transforming  $\vec{p}$  and  $\vec{q}$  to a point value representation using FFT, calculating the linear multiplication, and then transforming back to coefficient form using inverse FFT.

## Question 7

- a) Starting at  $(0,0)$  any spiral arrangement such as the one below would require  $n^2$  queries to find the middle element as the local minimum.

<b>16</b>	<b>15</b>	<b>14</b>	<b>13</b>	<b>12</b>
17	18	19	20	<b>11</b>
<b>2</b>	<b>1</b>	<b>0</b>	21	<b>10</b>
<b>3</b>	24	23	22	<b>9</b>
<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>

- b) text b goes  
here

## Question 8

let  $A(k) = k^{th}$  smallest element of  $A$   
 let  $B(k) = k^{th}$  smallest element of  $B$   
 let  $i$  be the current iteration (starting from 1)  
 let  $s_f(i) = \lfloor \frac{n}{2^i} \rfloor, s_c(i) = \lceil \frac{n}{2^i} \rceil$   
 let  $a = s_f(1), b = s_c(1)$   
 let  $m_a = A(a+1), m_b = B(b+1)$   
 let  $N$  be the set of  $n$  elements such that  $\forall x \in N \cap A, x < m_a$  and  $\forall x \in N \cap B, x < m_b$

When all elements in  $N$  are smaller than  $m_a$  and  $m_b$ , the median will be the smallest of both  $m_a$  and  $m_b$ .

So we iterate.

if  $B(b) > m_a$  then there exist elements in  $N$  that are not smaller than  $m_a$ :

Therefore, we change  $m_a$  and  $m_b$  and increment  $i$ .

We increase  $a$  by  $s_c(i)$  to consider elements that may be smaller than the median.

We decrease  $b$  by  $s_f(i)$  to ignore elements that may be bigger than the median.

else if  $A(a) > m_b$  then there exist elements in  $N$  that are not smaller than  $m_b$ :

Therefore, we change  $m_a$  and  $m_b$  and increment  $i$ .

We decrease  $a$  by  $s_f(i)$  to ignore elements that may be bigger than the median.

We increase  $b$  by  $s_c(i)$  to consider elements that may be smaller than the median.

else:

We stop iterating, as all elements of  $N$  are smaller than both  $m_a$  and  $m_b$ , and we take the median to be smaller of the two

This algorithm will take at most  $O(\log n)$  queries, as every iteration we jump by a factor of 2, similar to that of a binary search.

Note: if  $a+1 > n$  assume  $m_b$  to be the median.