Report for assignment 1

Vasudha Todi (14EC10059)

January 10, 2016

Multiplication of long integers using FFT/IFFT technique

1. **Random generation of integers**

   The digits of the integers are generated randomly by taking the number of digits as a parameter.

2. **Obtaining polynomial from integers**

   Polynomials are obtained by taking the digits of the integers to be the coefficients of the polynomials

   E.g. : $5962 = A(x) = 2 + 6x + 9(x^2) + 5(x^3)$

3. **Fast Fourier Transform**

   Consider the above polynomial. Suppose it is to be evaluated at four points. The polynomial is broken into 2 parts, even and odd, and evaluated recursively.

   $A_{even}(x) = 2 + 9x$
   $A_{odd}(x) = 6 + 5x$
   $A(x) = A_{even}(x^2) + xA_{odd}(x^2)$

   If the four point are taken to be the 4th roots of unity(w), the time for evaluating the polynomial reduces to O(mlogm) using the FFT algorithm.

Algorithm 1 FFT

```
FFT(n, A, F)
if n = 1 then
    F[0] ← a_0
    return
end if
A_even = [a_0 a_2 ... a_{n-2}]
A_odd = [a_1 a_3 ... a_{n-1}]
FFT(n/2, A_even, EF)
FFT(n/2, A_odd, OF)
```

for $j \leftarrow 0; j \leq n/2; ++j$ **do**
  $F[j] = EF[j] + w^j * OF[j]$
  $F[j + n/2] = EF[j] - w^j * OF[j]$
end for

4. **Inverse Fast Fourier Transform**

   The IFFT is used to obtain the coefficients of a polynomial from its value at n points, i.e., the nth roots of unity.

Algorithm 2 IFFT

IFFT(n, A, F)
if $n = 1$ **then**
  $F[0] \leftarrow a_0$
  return
end if
$A_{even} = [a_0 a_2 ... a_{n-2}]$
$A_{odd} = [a_1 a_3 ... a_{n-1}]$
$IFFT(n/2, A_{even}, EF)$
$IFFT(n/2, A_{odd}, OF)$
for $j \leftarrow 0; j \leq n/2; ++j$ **do**
  $F[j] = EF[j] + w^{-j} * OF[j]$
  $F[j + n/2] = EF[j] - w^{-j} * OF[j]$
end for

   The final result is divided by n.

5. **Multiplication of two polynomials**

   Multiplication of 2 polynomials is achieved by multiplying their fast fourier transforms at sufficient number of points and then applying inverse FFT on the result.

Algorithm 3 Mutiplication

$FFT(m, A, F_A)$
$FFT(m, B, F_B)$
for $i = 1, m$ **do**
  $F_C[i] = F_A[i] * F_B[i]$
end for
$IFFT(m, F_C, C)$
$C \leftarrow \frac{1}{m} * C$

6. **Final Result**

   The final integer is obtained from the coefficients of the above polynomial.
   Example :

$12 * 26$
$A(x) = 2 + x$
$B(x) = 6 + 2x$
$C(x) = A(x) * B(x) = 12 + 10x + 2x^2$
$C \leftarrow 312$

END