(2) Suppose that length($x[n]$) = 1200. What is the best way to implement the convolution of $x[n]$ and $y[n]$ if

(a) length($y[n]$) = 300, (b) length($y[n]$) = 30,

(c) length($y[n]$) = 8, and (d) length($y[n]$) = 2?

Please show (i) the calculation method (direct, non-sectioned convolution, or sectioned convolution), (ii) the number of points of the FFT, (iii) and the number of real multiplications for the best implementation method. Also, consider the general case where $x[n]$ and $y[n]$ are complex sequences and the FFT of $y[n]$ can be computed in prior. (25 scores)

direct : $3N \cdot M$, non-sec : $2MUL_P + 3P$, sec : $2S \cdot MUL_P + 3SP$

(a) $N = 1200$ $M = 300$

direct : $3 \times 1200 \times 300 = 1080000$

non-sec : $P \geq N + M - 1 = 1499$

choose $P \geq 1499 \Rightarrow P = 1680 \Rightarrow mul = 2 \times 10420 + 3 \times 1680$

$= 25880$

sec : $L_0 = 600$, $P_0 = 600 + 300 - 1 = 899$

$\Rightarrow P = 504$, $MUL_P = 2300$, $L = 1198$, $S = \left\lceil \frac{1200}{1198} \right\rceil = 2 \Rightarrow 2 \times (2 \times 2300 + 3 \times 504)$

$\Rightarrow \underline{12224}$

(b) $N = 1200$, $M = 30$

direct : $3 \times 1200 \times 30 = 108000$

non-sec : $P_0 = 1200 + 30 - 1 = 1229 \Rightarrow P = 1344$, $MUL = 8352$, $\Rightarrow 20536$

sec : $L_0 = 174$, $P_0 = L_0 + M - 1 = 203$

$P = 144$, $MUL = 936$, $L = 115$, $S = 11$ $\Rightarrow \underline{14364}$

(c)

direct : $3 \times 1200 \times 8 = 28800$

non-sec : $p = 1200 + 8 - 1 = 1207 \Rightarrow p = 1260$, $MUL = 7640$

$\Rightarrow 2 \times 7640 + 3 \times 1260 = 19060$

sec : $L_0 = 30$, $P_0 = L_0 + M - 1 = 37 \Rightarrow p = 36$, $MUL = 64$

$L = 36 - 8 + 1 = 29$

$S = \lceil \frac{1200}{29} \rceil = 42$

$\Rightarrow 42 \times (2 \times MUL + 3 \times 30) = \underline{9912}$

(d)

direct : $3 \times 1200 \times 2 = \underline{7200}$

non-sec : $p = 1260$, $MUL = 7640$

$\Rightarrow 2 \times 7640 + 3 \times 1260 = 19000$

sec : $L_0 = 2$, $P_0 = L_0 + M - 1 = 3$

$p = 4$, $L = 4 - 2 + 1 = 3$, $S = \lceil \frac{1200}{3} \rceil = 400$

$\Rightarrow 400 \times (2 \times 3 + 3 \times 4) = \underline{7200}$

or

0 12

rc

LA

(3) (a) What are the number of entries equal to 1 and -1 for the 2^k-point Walsh transform? (b) What are the number of entries equal to 1, 0, and -1 for the 2^k-point Haar transform? (c) What is the most important application of the Walsh transform nowadays? (d) What is the most important advantage of the Haar transform nowadays? (20 scores)

(a) 除了第一個 row =1，其他 1, -1 各半

$1 = \frac{2^k - k}{2} + k$, $-1 = \frac{2^k - k}{2}$

(b) 2^k-point ⇒ $k+1$ group ⇒

group 1 $(1, -1, 0) : (k, 0, 0)$

group 2 $(1, -1, 0) : (\frac{k}{2}, \frac{k}{2}, 0)$

⋮

group $k+1$ $(\frac{k}{2}, \frac{k}{2}, (2^{k-1}-1) \cdot k)$

⇒ $1 : (\frac{k}{2}) \cdot (k+2)$, $-1 : \frac{k}{2} \cdot k$, $0 : 2^k - k(k+1)$

(c) CDMA

(d)

1. 分析 local high frequecy component
2. 抽 local feature

(4) (a) What is the results of CDMA if there are three data [1 0 1], [1 1 0], [0 1 1] and these three data are modulated by the 1^{st}, 4^{th}, and 10^{th} rows of the 16-point Walsh transform? (The beginning row is the 1^{st} row). (10 scores)

(b) In (a), if the 7^{th} and the 19^{th} entries of the CDMA results are missed, can we recover the original data? Why? (5 scores)

$$V_{16} = \left[\begin{array}{cccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&-1&-1&-1&-1&1&1&1&1&-1&-1&-1&-1\\
1&1&-1&-1&-1&-1&1&1&1&1&-1&-1&-1&-1&1&1\\
1&1&-1&-1&1&1&-1&-1&1&1&-1&-1&1&1&-1&-1\\
\hline
1&-1&-1&1&1&-1&-1&1&1&-1&-1&1&1&-1&-1&1\\
1&-1&-1&1&-1&1&1&-1&1&-1&-1&1&-1&1&1&-1\\
1&-1&1&-1&-1&1&-1&1&1&-1&1&-1&-1&1&-1&1\\
1&-1&1&-1&1&-1&1&-1&1&-1&1&-1&1&-1&1&-1\\
\hline
1&1&1&1&1&1&1&1&-1&-1&-1&-1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1&-1&-1&-1&-1&1&1&1&1\\
1&1&-1&-1&-1&-1&1&1&-1&-1&1&1&1&1&-1&-1\\
1&1&-1&-1&1&1&-1&-1&-1&-1&1&1&-1&-1&1&1\\
\hline
1&-1&-1&1&1&-1&-1&1&-1&1&1&-1&-1&1&1&-1\\
1&-1&-1&1&-1&1&1&-1&-1&1&1&-1&1&-1&-1&1\\
1&-1&1&-1&-1&1&-1&1&-1&1&-1&1&1&-1&1&-1\\
1&-1&1&-1&1&-1&1&-1&-1&1&-1&1&-1&1&-1&1
\end{array}\right]
\begin{array}{c}
0\\3\\4\\7\\8\\11\\12\\15\\1\\2\\5\\6\\9\\10\\13\\14
\end{array}$$

(a)

$m_0 + m_3 + m_9$ $\overline{M}$

$[1331, -111-1, 3113, 1-1-11][1-1-11, 1-1-11, -111-1, -111-1]$

$[1-1-1, 3113, -111-1, 1331]$

(b)

$\overline{M} \cdot m_0 \Rightarrow [>0][<0][>0] \Rightarrow [1, 0, 1]$

$\overline{M} \cdot m_3 \Rightarrow [>0][>0][<0] \Rightarrow [1, 1, 0]$

$\overline{M} \cdot m_9 \Rightarrow [<0][>0][>0] \Rightarrow [0, 1, 1]$

還原

(5) Ramanujan's Sum in NTT

Given $M = 11$, $\alpha = 8+6i$, and $N = 12$. Please determine the complex number theoretic transform (CNT) of $\mathbf{x}$ if

$$\mathbf{x} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Hint: fft(x) is as follows, which is Ramanujan's Sum

$$fft(\mathbf{x}) = \begin{bmatrix} 4 & 0 & 2 & 0 & -2 & 0 & -4 & 0 & -2 & 0 & 2 & 0 \end{bmatrix}$$ (8 scores)

(6) (a) Please determine

$$3^{2049} \bmod 103 \qquad \text{(Hint: 費馬小定理)}$$

(b) Suppose that $x \bmod 43 = 2$ *and* $x \bmod 67 = 13$

Please Determine

$$x \bmod 2881. \qquad \text{(Hint: Chinese Remainder Theorem)}$$

(c) $n! = n(n-1)(n-2) \ldots. 1$. Please determine $39! \bmod 43$

(Hint: Wilson's Theorem) (12 scores)

(a) $(3, 103) = 1 \Rightarrow 3^{102} \equiv 1$

$$\Rightarrow 3^{2049} = (3^{102})^{9} \cdot 3^{9} \equiv 10 \#$$

(b)

(c) $(p-1)! \equiv -1 \mod p$

$\Rightarrow 42! \equiv -1 \mod 43$

$42! = 42 \cdot 41 \cdot 40 \cdot 39!$

$\equiv (-1)(-2)(-3)\, 39! \equiv -6 \cdot 39!$

$43 = 7 \cdot 6 + 1$

$1 = 43 + (-6) \cdot 7 \Rightarrow$ inverse$(-6) = 7$ mod 43 $\Rightarrow 39! \equiv -1 \cdot 7$

$\equiv -7$

$\equiv 36 \mod 43$