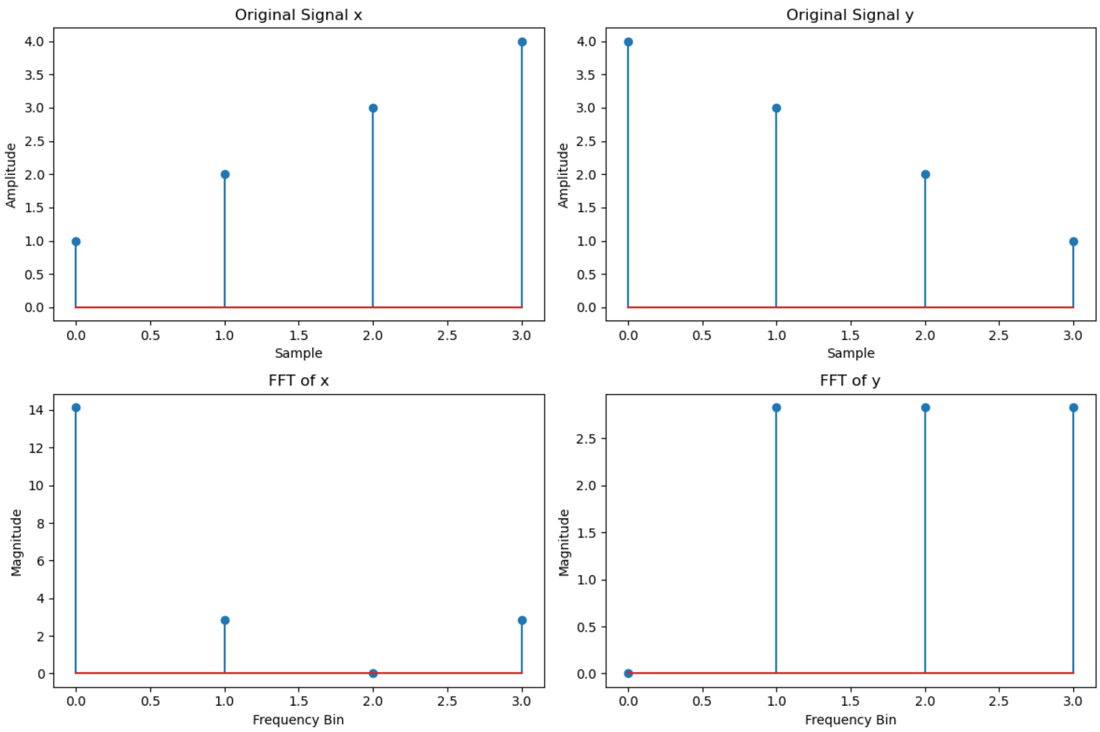
ADSP HW5 r12631055 林東甫

1.



2.

2. (a) 300

(i) non-sectioned convolution

(ii) 2048

(iii) 30596

Direct : $3 \cdot 1200 \cdot 300 = 1{,}080{,}000$

DFT : $N+M-1 = 1200+300-1 = 1499 < 2^{11} = 2048$

O: $2 \cdot 1200 \log 2048 \approx 1200 \cdot 11 = 13200$

$13200 + 2 \cdot 2048 + 13200 = 30596$

(b) 30

(i) sectioned convolution $L = 174$ $P \geq 174+30-1 = 203 \leq 256$

(ii) ~~256~~ $\cancel{1200+30-1 = 1229 \leq 2048}$ 256

$2 \cdot 211 \log 256 + 2 \cdot 256 + 211 \cdot 8 = 5876$

(iii) 5876

(c)

(i) sectioned convolution $L = 194+8-1 = 201 \leq 256$

(ii) ~~256~~ $\cancel{1200+8-1 = 1207 \leq 2048}$ 256

(iii) 5876

(d) 2

(i) direct $3 \cdot 1200 \cdot 2 = 7200$

(ii) none

(iii) 7200

3.

3. (a) Walsh transform

$1: 2^N \cancel{N = \sqrt{2^k}}$, $\frac{N(N+1)}{2}$ # $N = 2^k$, $k = 0, 1, 2, 3 \ldots$

$-1: 2^N \cancel{N = \sqrt{2^k}}$, $\frac{N(N-1)}{2}$ # $N = 2^k$, $k = 0, 1, 2, 3 \ldots$

(b) Harr transform

$1: 2^N \cancel{N = \sqrt{2^k}}$, $N + \frac{N}{2}\log_2 N$ $N = 2^k$, $k = 0, 1, 2, 3 \ldots$

$0: 2^N \cancel{N = \sqrt{2^k}}$, $N^2 - (N + \frac{N}{2}\log_2 N) - N(\log_4 N)$ $N = 2^k$

$-1: 2^N \cancel{N = \sqrt{2^k}}$, $N(\log_4 N)$ $N = 2^k$, $k = 0, 1, 2, 3 \ldots$

(c). Walsh transform

CDMA (code division multiple access)

Using the basis (rows) of the Walsh transform to perform modulation

∵ modulation : using some man-made waveform to represent a data.

(d.) Harr transform

Analysis of the local high frequency component (edges of different locations and scales) and extracting local features.

4(a).

4. (a)

1st row: [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]

[1, 0, 1] => [1, -1, 1]

[1, -1, 1] modulated by 1st row:

[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]

4th row: [1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1]

[1, 1, 0] => [1, 1, -1]

[1, 1, -1] modulated by 4th row:

[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]

10th row: [1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1

[0, 1, 1] => [-1, 1, 1]

[-1, 1, 1] modulated by 10th row:

[-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]

Addition [1, 3, 1, 3, -1, 1, -1, 1, 3, 1, 3, 1, 1, -1, 1, -1,
1, -1, 1, -1, -1, -3, -1, -3, -1, 1, -1, 1, -3, -1, -3, -1,
1, -1, 1, -1, 3, 1, 3, 1, -1, 1, -1, 1, 1, 3, 1, 3]

4(b).

4(b) Yes, by (a): Using inner product $= \dfrac{\text{inner product}}{N}$ $>0 \Rightarrow 1$, $<0 \Rightarrow -1$

1, 3, 1, 3, -1, 1, -1, 1, 3, 1, 3, 1, 1, -1, 1, -1

		inner product	
1st	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	16	$\Rightarrow \frac{16}{16} = 1$
4th	1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1	16	$\frac{16}{16} = 1$
10th	1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1	-16	$\frac{-16}{16} = -1$

1, -1, 1, -1, -1, -3, -1, -3, -1, 1, -1, 1, -3, -1, -3, -1

1st	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	$\frac{-16}{16} = -1$
4th	1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1	$\frac{16}{16} = 1$
10th	1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1	$\frac{16}{16} = 1$

1, -1, 1, -1, 3, 1, 3, 1, -1, 1, -1, 1, 1, 3, 1, 3

1st	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	$\frac{16}{16} = 1$
4th	1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1	$\frac{-16}{16} = -1$
10th	1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1	$\frac{16}{16} = 1$

1st: [1, -1, 1] => [1, 0, 1], 4th: [1, 1, -1] => [1, 1, 0]

10th: [-1, 1, 1] => [0, 1, 1]

If 7th and 19th entries ~~is~~ are missed:

1, 3, 1, 3, -1, 1, 0 (7th), 1, 3, 1, 3, 1, 1, -1, 1, -1

1, -1, 0 (19th), -1, -1, -3, -1, -3, -1, 1, -1, 1, -3, -1, -3, -1

1st inner product $\frac{17}{16} = 1.0625$

4th: $\frac{15}{16} = 0.9375$

10th $\frac{-15}{16} = -0.9375$

1st $\frac{-17}{16} = -1.0625$

4th $\frac{15}{16} = 0.9375$

10th $\frac{15}{16} = 0.9375$

7th $0 \Rightarrow -1$

19th $0 \Rightarrow 1$

Fi

5.

5. Given $M=11$, $\alpha=8+6i$, $N=12$

$x=[0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1]$

$\alpha^k \bmod M$ where $\alpha=8+6i$, $k=0,1,\dots,11$

$\alpha^0\equiv 1$, $\alpha^1\equiv 8+6i$, $\alpha^2\equiv 6+8i$, $\alpha^3\equiv 4+i \cdots \alpha^{11}\equiv -1$

$$CNT_k=\sum_{j=0}^{N-1} x_j\cdot(\alpha^k)^j \bmod M$$

$$CNT_0 = x_0\cdot\alpha^0+x_1\cdot\alpha^0+x_2\cdot\alpha^0+\dots+x_{11}\cdot\alpha^0 \bmod 11$$
$$= 4 \bmod 11 = 4$$

$$CNT_1 = x_0\alpha^1+x_1\alpha^1+x_2\cdot\alpha^1+\dots+x_{11}\cdot\alpha^1 \bmod 11$$
$$=(8+6i)+(8+6i)+(8+6i)+(8+6i) \bmod 11$$

$\vdots$

$CNT=[4,0,2,0,-2,0,-4,0,-2,0,2,0]$

6.

6.

(a) Fermat's little theorem : if p is a prime number, then $\forall a$, $a^p - a$ is an integer multiple of p :

$a^p \equiv a \pmod{p}$ $\therefore$ $a^{p-1} \equiv 1 \bmod p$

consider $2049 = 102 \times 20 + 9$, $3^{102} \equiv 1 \bmod 103$

$3^{102 \times 20 + 9} = (3^{102})^{20} \times 3^9$ where $(3^{102})^{20} \equiv 1^{20} \equiv 1 \bmod 103$

$3^{2049} \equiv 3^9 \bmod 103$, $3^9 \bmod 103 = \underline{10}$ #

(b)

$\begin{cases} x \equiv 2 \bmod 43 \\ x \equiv 13 \bmod 67 \end{cases}$ $43b \equiv 1 \pmod{67}$

$b = \cancel{4}53$

$67a \equiv 1 \pmod{43} \Rightarrow \cancel{24}a \equiv 1 \pmod{43}$

$a = \cancel{53}9$, $43 \times 13 \times 53 = 29627$, $67 \times 9 \bmod 43 =$

$\therefore \cancel{b}$ $67 \times 2 \times 9 = 1206$, $29627 + 1206 = 30833$

$67 \times 43 = 2881$, $30833 - (2881 \times 10) = 2023$

Ans: $2023 + 2881k$, $k = 0, 1, 2, \ldots$

(c)

Wilson's Theorem : If p is a prime number, then $(p-1)! \equiv -1 \bmod p$

Let $p = 43$ $\therefore$ $42! \equiv -1 \bmod 43 \Rightarrow (42 \cdot 41 \cdot 40 \cdot 39!) \equiv -1 \bmod 43$

$42 \equiv -1 \pmod{43}$, $41 \equiv -2$, $40 \equiv -3$, $-1 \cdot -2 \cdot -3 \cdot 39! \equiv -1 \bmod 43$

$\because -6 \cdot 39! \equiv -1 \bmod 43$ $\therefore$ $39! \bmod 43 = -7$ $\therefore$ $\underline{39! \bmod 43 = 36}$ #

No Extra (學號末碼 5)