# XIII. Number Theoretic Transform (NTT)

#### **● 13-A Definition**

Number Theoretic Transform and Its Inverse  $F(k) = \sum_{n=0}^{N-1} f(n) \alpha^{nk} \pmod{M}, k = 0, 1, 2 \cdots, N-1$ 

$$f(n) = N^{-1} \sum_{k=0}^{N-1} F(k) \alpha^{-nk} \pmod{M} \quad , n = 0, 1, 2 \cdots, N-1 \qquad f(n) \stackrel{NTT}{\Longleftrightarrow} F(k)$$

$$INTT$$

#### Note:

- (1) M is a prime number, (mod M): 是指除以 M 的餘數
- (2) N is a factor of M-1(Note: when  $N \neq 1$ , N must be prime to M)
- (3)  $N^{-1}$  is an integer that satisfies  $(N^{-1})N \mod M = 1$ (When N = M - 1,  $N^{-1} = M - 1$ )

(4)  $\alpha$  is a root of unity of order N

$$\alpha^{N} = 1 \pmod{M}$$

$$\alpha^{k} \neq 1 \pmod{M}, k = 1, 2, \dots, N-1$$

When  $\alpha$  satisfies the above equations and N = M - 1, we call  $\alpha$  the "primitive root".

$$\alpha^k \neq 1 \pmod{M}$$
 for  $k = 1, 2, \dots, M-2$  
$$\alpha^{M-1} = 1 \pmod{M}$$
 
$$\alpha^{-1}$$
 的求法與  $N^{-1}$  相似

 $\alpha^{-1}$  is an integer that satisfies  $(\alpha^{-1})\alpha \mod M = 1$ 

[Example 1]:

470

$$M = 5$$
  $\alpha = 2$   $\alpha^1 = 2 \pmod{5}$   $\alpha^2 = 4 \pmod{5}$   $\alpha^3 = 3 \pmod{5}$   $\alpha^4 = 1 \pmod{5}$ 

(1) When N = 4

When 
$$N = 4$$

$$\begin{bmatrix}
F[0] \\
F[1] \\
F[2] \\
F[3]
\end{bmatrix} = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 2 & 4 & 3 \\
1 & 4 & 1 & 4 \\
1 & 3 & 4 & 2
\end{bmatrix} \begin{bmatrix}
f[0] \\
f[1] \\
f[2] \\
f[3]
\end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\
1 & 2 & 4 & 3 \\
1 & 4 & 1 & 4 \\
1 & 3 & 4 & 2
\end{bmatrix} \begin{bmatrix}
f[0] \\
f[1] \\
f[2] \\
f[3]
\end{bmatrix}$$

(2) When N = 2

$$\begin{bmatrix} F[0] \\ F[1] \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} f[0] \\ f[1] \end{bmatrix}$$

#### [Example 2]:

M = 7, N = 6:  $\alpha$  cannot be 2 but can be 3.

$$\alpha = 2$$
:  $\alpha^1 = 2 \pmod{7}$   $\alpha^2 = 4 \pmod{7}$   $\alpha^3 = 1 \pmod{7}$ 

$$\alpha = 3$$
:  $\alpha^1 = 3 \pmod{7}$   $\alpha^2 = 2 \pmod{7}$   $\alpha^3 = 6 \pmod{7}$ 

$$\alpha^4 = 4 \pmod{7}$$
  $\alpha^5 = 5 \pmod{7}$   $\alpha^6 = 1 \pmod{7}$ 

Advantages of the NTT:

Disadvantages of the NTT:

## ● 13-B 餘數的計算

- $(1) x \pmod{M}$  的值,必定為  $0 \sim M 1$  之間
- (2)  $a + b \pmod{M} = \{a \pmod{M} + b \pmod{M}\} \pmod{M}$

例: 
$$78 + 123 \pmod{5} = 3 + 3 \pmod{5} = 1$$
(1,6)
$$= 3306 \times 225 \pmod{1}$$

(Proof): If 
$$a = a_1M + a_2$$
 and  $b = b_1M + b_2$ , then 
$$a + b = (a_1 + b_1)M + a_2 + b_2$$

 $(3) a \times b \pmod{M} = \{a \pmod{M} \times b \pmod{M}\} \pmod{M}$ 

例: 
$$78 \times 123 \pmod{5} = 3 \times 3 \pmod{5} = 4$$

(Proof): If 
$$a = a_1M + a_2$$
 and  $b = b_1M + b_2$ , then  $a \times b = (a_1 b_1M + a_1b_2 + a_2b_1)M + a_2b_2$ 

在 Number Theory 當中 只有  $M^2$  個可能的 m 因可能的 m 我

可事先將加法和乘法的結果存在記憶體當中 需要時再"LUT"

LUT : lookup table

# **13-C** Properties of Number Theoretic Transforms

#### P.1) Orthogonality Principle 跟FT很像

$$S_N = \sum_{n=0}^{N-1} \alpha^{nk} \alpha^{-n\ell} = \sum_{n=0}^{N-1} \alpha^{n(k-\ell)} = N \cdot \delta_{k.\ell}$$

proof : for 
$$k = \ell$$
,  $S_N = \sum_{n=0}^{N-1} \alpha^0 = N$ 

for 
$$k \neq 0$$
,  $(\alpha^{k-\ell l} - 1) S_N = (\alpha^{k-\ell} - 1) \sum_{n=0}^{N-1} \alpha^{n(k-\ell)} = \alpha^{N(k-\ell)} - 1 = 1 - 1 = 0$   
 $\therefore \alpha^{k-\ell} \neq 1$   $\therefore S_N = 0$ 

#### P.2) The NTT and INTT are exact inverse 跟FT很像

proof : 
$$g(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) \alpha^{-nk} = \frac{1}{N} \sum_{k=0}^{N-1} \left( \sum_{\ell=0}^{N-1} f(\ell) \alpha^{\ell k} \right) \alpha^{-nk}$$
$$= \frac{1}{N} \sum_{\ell=0}^{N-1} f(\ell) \sum_{k=0}^{N-1} \alpha^{(\ell-n)k} = \frac{1}{N} \sum_{\ell=0}^{N-1} f(\ell) \cdot N \delta_{\ell,n} = f(n)$$

#### P.3) Symmetry

$$f(n) = f(N-n)$$
  $\stackrel{\text{NTT}}{\Longleftrightarrow}$   $F(k) = F(N-k)$   
 $f(n) = -f(N-n)$   $\stackrel{\text{NTT}}{\Longleftrightarrow}$   $F(k) = -F(N-k)$ 

#### P.4) INNT from NTT

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) \alpha^{-nk} = \frac{1}{N} \sum_{(-k)=0}^{N-1} F(-k) \alpha^{nk} = NTT \text{ of } \frac{1}{N} F(-k)$$

Algorithm for calculating the INNT from the NTT

(1) F(-k): time reverse

$$F_0, F_1, F_2, ..., F_{N-1} \xrightarrow{\text{time}} F_0, F_{N-1}, ..., F_2, F_1$$

(2) NTT[ F(-k) ]

(3) 乘上 
$$\frac{1}{N} = M - 1$$

#### P.5) Shift Theorem

$$f(n+\ell) \leftrightarrow F(k) \alpha^{-\ell k}$$
$$f(n) \alpha^{n\ell} \leftrightarrow F(k+\ell)$$

#### P.6) Parseval's Theorem

$$N\sum_{n=0}^{N-1} f(n) f(-n) = \sum_{k=0}^{N-1} F^{2}(k)$$

$$N\sum_{n=0}^{N-1} f(n)^2 = \sum_{k=0}^{N-1} F(k)F(-k)$$

#### P.7) Linearity

$$a f(n) + b g(n) \leftrightarrow a F(k) + b G(k)$$

#### P.8) Reflection

If 
$$f(n) \leftrightarrow F(k)$$
 then  $f(-n) \leftrightarrow F(-k)$ 

# **Circular Convolution** (the same as that of the DFT)

If 
$$f(n) \leftrightarrow F(k)$$

$$g(n) \leftrightarrow G(k)$$
then  $f(n) \otimes g(n) \leftrightarrow F(k)G(k)$ 
i.e.,  $f(n) \otimes g(n) = INTT \{NTT[f(n)]NTT[g(n)]\}$ 

$$f(n) \cdot g(n) \leftrightarrow \frac{1}{N}F(k) \otimes G(k)$$
(Proof):  $INNT(NNT(f[n])NNT(g[n])) = N^{-1}\sum_{k=0}^{N-1}\alpha^{-nk}F(k)G(k)$ 

$$= N^{-1}\sum_{k=0}^{N-1}\alpha^{-nk}\sum_{m=0}^{N-1}f[m]\alpha^{mk}\sum_{q=0}^{N-1}g[q]\alpha^{qk}$$
We apply the fact that
$$= \sum_{m=0}^{N-1}\sum_{q=0}^{N-1}f[m]g[q]N^{-1}\sum_{k=0}^{N-1}\alpha^{-nk}\alpha^{mk}\alpha^{qk}$$

$$= \sum_{m=0}^{N-1}\sum_{q=0}^{N-1}f[m]g[q]\delta[((m+q-n))_N]$$

$$= \sum_{m=0}^{N-1}\sum_{q=0}^{N-1}f[m]g[((n-m))_N] = f[n] \otimes g[n]$$
When  $q = ((n-m))_N$ 

$$m+q-n \text{ is a multiple of } N$$

# **13-D** Efficient FFT-Like Structures for Calculating NTTs

• If *N* (transform length) is a power of 2, then the radix-2 FFT butterfly algorithm can be used for efficient calculation for NTT.

Decimation-in-time NTT

Decimation-in-frequency NTT

• The prime factor algorithm can also be applied for NTTs.

$$F(k) = \sum_{n=0}^{N-1} f(n) \alpha^{nk} = \sum_{r=0}^{\frac{N}{2}-1} f(2r) \alpha^{2rk} + \sum_{r=0}^{\frac{N}{2}-1} f(2r+1) \alpha^{(2r+1)k}$$

$$= \sum_{r=0}^{\frac{N}{2}-1} f(2r) (\alpha^2)^{rk} + \alpha^k \sum_{r=0}^{\frac{N}{2}-1} f(2r+1) (\alpha^2)^{rk}$$

$$= \begin{cases} G(k) + \alpha^k H(k) & , 0 \le k \le \frac{N}{2} - 1 \\ G(k - \frac{N}{2}) + \alpha^k H(k - \frac{N}{2}) & , \frac{N}{2} \le k \le N \end{cases}$$
where 
$$G(k) = \sum_{r=0}^{N/2-1} f(2r) (\alpha^2)^{rk} H(k) = \sum_{r=0}^{N/2-1} f(2r+1) (\alpha^2)^{rk}$$
One N-point NTT \to Two (N/2)-point NTTs plus twiddle factors

$$f(n) = (1, 2, 0, 0)$$

$$N = 4, M = 5$$

Permutation

(1, 0, 2, 0)

After the 1st stage

(1, 1, 2, 2)

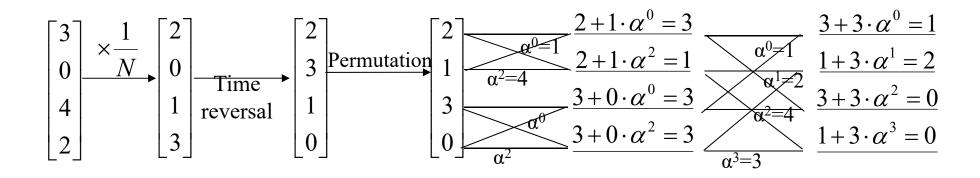
After the 2<sup>nd</sup> stage F(k) = (3, 0, 4, 2)

$$\begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix} \xrightarrow{\text{reversal}} \begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \end{bmatrix} \xrightarrow{\alpha^{2}=4} \begin{bmatrix} \frac{1+0\cdot\alpha^{0}=1}{1+0\cdot\alpha^{2}=1} & \frac{1+2\cdot\alpha^{0}=3}{1+2\cdot\alpha^{2}=2} & \frac{1+2\cdot\alpha^{0}=3}{1+2\cdot\alpha^{1}=5} & = \begin{bmatrix} 3 \\ 0 \\ 4 \\ 2 \end{bmatrix}$$

#### Inverse NTT by Forward NTT:

$$F(-k) \times \frac{1}{N}$$
  $(4^{-1} = 4)$ 

- 2) Time reversal
- 3) permutation
- 4) After first stage
- 5) After 2<sup>nd</sup> stage



# **13-E** Convolution by NTT

假設 x[n] = 0 for n < 0 and  $n \ge K$ , h[n] = 0 for n < 0 and  $n \ge H$  要計算 x[n] \* h[n] = z[n]

且 z[n] 的值可能的範圍是  $0 \le z[n] < A$  (more general,  $A_1 \le z[n] < A_1 + T$ )

- (1) 選擇 M (the prime number for the modulus operator), 滿足
  - (a) M is a prime number, (b)  $M \ge \max(H+K, A)$
- (2) 選擇 N (NTT 的點數), 滿足
  - (a) N is a factor of M-1, (b)  $N \ge H+K-1$

(4) 
$$X_1[m] = \text{NTT}_{N,M} \{x_1[n]\}, \quad H_1[m] = \text{NTT}_{N,M} \{h_1[n]\}$$
  
NTT<sub>N,M</sub> 指 N-point 的 DFT (mod M)

(5) 
$$Z_1[m] = X_1[m]H_1[m], z_1[n] = INTT_{N,M} \{Z_1[m]\},$$

(6) 
$$z[n] = z_1[n]$$
 for  $n = 0, 1, ..., H+K-1$   
(移去  $n = H+K, H+K+1, ..., N-1$  的點)

(More general, if we have estimated the range of z[n] should be  $A_1 \le z[n] < A_1 + T$ , then

$$z[n] = ((z_1[n] - A_1))_M + A_1$$

適用於(1)x[n],h[n]皆為整數

(2) Max(z[n]) - min(z[n]) < M 的情形。

Consider the convolution of (1, 2, 3, 0) \* (1, 2, 3, 4)

Choose M = 17, N = 8,結果為:

## ● Max(z[n]) - min(z[n]) 的估測方法

假設 
$$x_1 \le x[n] \le x_2$$
,  $z[n] = x[n] * h[n] = \sum_{m=0}^{H-1} h[m] x[n-m]$ 

則  $Max(z[n]) - \min(z[n]) = (x_2 + x_1) \sum_{n=0}^{H-1} |h[n]|$ 

(Proof):  $Max(z[n]) = \sum_{m=0}^{H-1} h_1[m] x_2 + \sum_{m=0}^{H-1} h_2[m] x_1$ 

where  $h_1[m] = h[m]$  when  $h[m] > 0$ ,  $h_1[m] = 0$  otherwise  $h_2[m] = h[m]$  when  $h[m] < 0$ ,  $h_2[m] = 0$  otherwise  $\min(z[n]) = \sum_{m=0}^{H-1} h_1[m] x_1 + \sum_{m=0}^{H-1} h_2[m] x_2$ 
 $Max(z[n]) - \min(z[n]) = \sum_{m=0}^{H-1} h_1[m] (x_2 - x_1) + \sum_{m=0}^{H-1} h_2[m] (x_1 - x_2)$ 
 $= (x_2 - x_1) \left\{ \sum_{m=0}^{H-1} h_1[m] - \sum_{m=0}^{H-1} h_2[m] \right\} = (x_2 - x_1) \sum_{m=0}^{H-1} |h[m]|$ 

# **O** 13-F Special Prime Numbers

Fermat Number:  $M = 2^{2^p} + 1$  P = 0, 1, 2, 3, 4M = 3, 5, 17, 257, 65537

 $P \ge 5$  may not be prime.

Mersenne Number :  $M = 2^p - 1$  P = 1, 2, 3, 5, 7, 13, 17, 19, .....M = 1, 3, 7, 31, 127, 8191, 131071, 524287,.....

If  $M = 2^p - 1$  is a prime number, p must be a prime number.

However, if p is a prime number,  $M = 2^p - 1$  may not be a prime number.

The modulus operations for Mersenne and Fermat prime numbers are very easy for implementation.

$$2^{k} \pm 1$$

Example: 25 mod 7

$$\frac{11}{100a} 1001$$

$$\frac{100a}{1011}$$

$$\frac{100a}{12}$$

$$100$$

$$100$$

# **13-G** Complex Number Theoretic Transform (CNT)

The integer field  $Z_M$  can be extended to complex integer field

If the following equation does not have a sol. in  $Z_M$ 

This means (-1) does not have a square root

When M = 4k + 1, there is a solution for  $x^2 = -1 \pmod{M}$ .

When M = 4k + 3, there is no solution for  $x^2 = -1 \pmod{M}$ .

For example, when M = 13,  $8^2 = -1 \pmod{13}$ .

$$2^1 = 2$$
,  $2^2 = 4$ ,  $2^3 = 8$ ,  $2^4 = 3$ ,  $2^5 = 6$ ,  $2^6 = 12 = -1$ ,

$$2^7 = 11$$
,  $2^8 = 9$ ,  $2^9 = 5$ ,  $2^{10} = 10$ ,  $2^{11} = 7$ ,  $2^{12} = 1$ 

When M = 11, there is no solution for  $x^2 = -1 \pmod{M}$ .

If there is no solution for  $x^2 = -1 \pmod{M}$ , we can define an imaginary number i such that

$$i^2 = -1 \pmod{M}$$

Then, "i" will play a similar role over finite field  $Z_M$  such that plays over the complex field.

$$(a+ib)\pm(c+id) = (a\pm c)+i(b\pm d)$$
  
 $(a+ib)\cdot(c+id) = ac+i^2bd+ibc+iad$   
 $= (ac-bd)+i(bc+ad)$ 

# **13-H** Applications of the NTT

NTT 適合作 convolution

但是有不少的限制

新的應用: encryption (密碼學)

CDMA

#### References:

- (1) R. C. Agavard and C. S. Burrus, "Number theoretic transforms to implement fast digital convolution," *Proc. IEEE*, vol. 63, no. 4, pp. 550-560, Apr. 1975.
- (2) T. S. Reed & T. K. Truoay, "The use of finite field to compute convolution," *IEEE Trans. Info. Theory*, vol. IT-21, pp.208-213, March 1975
- (3) E. Vegh and L. M. Leibowitz, "Fast complex convolution in finite rings," *IEEE Trans ASSP*, vol. 24, no. 4, pp. 343-344, Aug. 1976.
- (4) J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*, Prentice-Hall, New Jersey, 1979.
- (5) 華羅庚,"數論導引,"凡異出版社,1997。

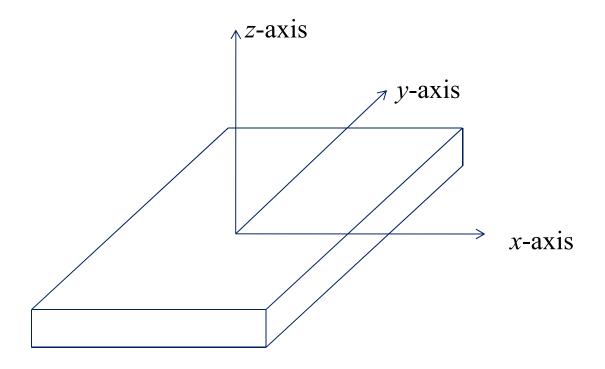
## 附錄十五 3-D Accelerometer 的簡介

3-D Accelerometer: 三軸加速器,或稱作加速規

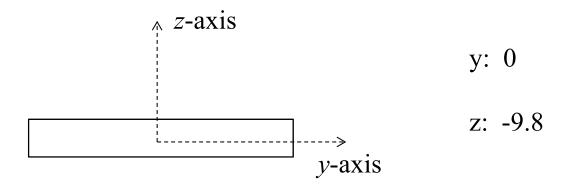
許多儀器(甚至包括智慧型手機)都有配置三軸加速器

可以用來判別一個人的姿勢和動作

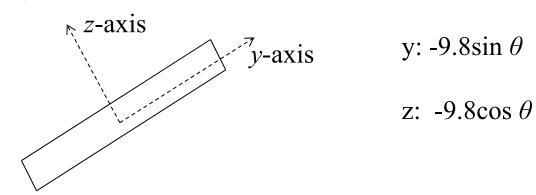
註: Gyrator (陀螺儀) 可以用來量測物體旋轉之方向,可補 3-D Accelerometer 之不足,許多儀器 (包括智慧型手機) 也內建陀螺儀之裝置, 3-D Accelerometer Signal Processing 和 gyrator signal processing 經常並用



根據x,y,z三個軸的加速度的變化,來判斷姿勢和動作 平放且靜止時,z-axis 的加速度為-g=-9.8



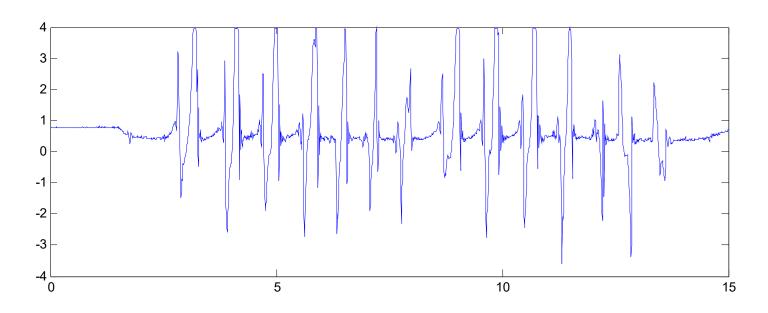
tilted by  $\theta$ 



可藉由加速規傾斜的角度,來判斷姿勢和動作

例子:若將加速規放在腳上.....

走路時,沿著其中一個軸的加速度變化



應用: 動作辨別

運動(訓練,計步器)

醫療復健,如 Parkinson 患者照顧,傷患復原情形

3-D Accelerometer Signal Processing 是訊號處理的重要課題之一

其他(如動物的動作,機器的運轉情形的偵測)

一方面固然是因為應用多,另一方面, 3-D Accelerometer Signal 容易受 noise 之干擾,要如何藉由 3-D Accelerometer Signal 來還原動作以及移動速度,仍是個挑戰

# XIV. Walsh Transform (Hadamard Transform)

## **14-A Ideas of Walsh Transforms**

• 8-point Walsh transform

- Advantages of the Walsh transform:
  - (1) Real
  - (2) No multiplication is required
  - (3) Some properties are similar to those of the DFT

• Forward and inverse Walsh transforms are similar.

forward: 
$$F[m] = \sum_{n=0}^{N-1} f[n]W[m,n]$$
, inverse:  $f[m] = \frac{1}{N} \sum_{n=0}^{N-1} W[m,n]F[n]$ 

• Alternative names of the Walsh transform:

#### Hadamard transform, Walsh-Hadamard transform

- Orthogonal Property  $\sum_{n=0}^{N-1} W[m_0, n]W[m_1, n] = 0 \qquad \sum_{n=0}^{N-1} W[m, n]W[m, n] = N$ if  $m_0 \neq m_1$
- Zero-Crossing Property
- Even / Odd Property
- Fast Algorithm

Useful for spectrum analysis

Sometimes also useful for implementing the convolution

#### Walsh transform 和 DFT, DCT 有許多相似處

$$\mathbf{DCT} = \begin{bmatrix} 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.3870 & 1.1759 & 0.7857 & 0.2759 & -0.2759 & -0.7857 & -1.1759 & -1.3870 \\ 1.3066 & 0.5412 & -0.5412 & -1.3066 & -1.3066 & -0.5412 & 0.5412 & 1.3066 \\ 1.1759 & -0.2759 & -1.3870 & -0.7857 & 0.7857 & 1.3870 & 0.2759 & -1.1759 \\ 1.0000 & -1.0000 & -1.0000 & 1.0000 & 1.0000 & -1.0000 & -1.0000 & 1.0000 \\ 0.7857 & -1.3870 & 0.2759 & 1.1759 & -1.1759 & -0.2759 & 1.3870 & -0.7857 \\ 0.5412 & -1.3066 & 1.3066 & -0.5412 & -0.5412 & 1.3066 & -1.3066 & 0.5412 \\ 0.2759 & -0.7857 & 1.1759 & -1.3870 & 1.3870 & -1.1759 & 0.7857 & -0.2759 \end{bmatrix}$$

#### **References for Walsh Transforms**

- [1] K. G. Beanchamp, Walsh Functions and Their Applications, Academic Press, New York, 1975.
- [2] B. I. Golubov, A. Efimov, and V. Skvortsov, *Walsh Series and Transforms: Theory and Applications*, Kluwer Academic Publishers, Boston, 1991.
- [3] H. F. Harmuth, "Applications of Walsh functions in communications," *IEEE Spectrum*, vol. 6, no. 11, pp. 82-91, Nov. 1969.
- [4] H. F. Harmuth, *Transmission of Information by Orthogonal Functions*, Springer-Verlag, New York, 1972.

## **14-B** Generate the Walsh Transform

2-point Walsh transform

$$V=2$$

$$V_{2}=\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$V_{3}=\begin{bmatrix} -1 \end{bmatrix}$$

$$V_{4}=\begin{bmatrix} -1 \end{bmatrix}$$

$$V_{4}=\begin{bmatrix} -1 \end{bmatrix}$$

$$V_{5}=\begin{bmatrix} -1 \end{bmatrix}$$

$$V_{5}=\begin{bmatrix} -1 \end{bmatrix}$$

4-point Walsh transform

$$W_{4} \neq F_{4}$$

$$F_{4} = \begin{bmatrix} ? \end{bmatrix}$$

How do we obtain the  $2^{k+1}$ -point Walsh transform from the  $2^k$ -point Walsh transform?

Step 1 
$$\mathbf{V}_{2^{k+1}} = \begin{bmatrix} \mathbf{W}_{2^k} & \mathbf{W}_{2^k} \\ \mathbf{W}_{2^k} & -\mathbf{W}_{2^k} \end{bmatrix}$$

Step 2 根據 sign changes 將 rows 的順序重新排列

$$\mathbf{V}_{\mathbf{2}^{k+1}} \xrightarrow{permutation} \mathbf{W}_{\mathbf{2}^{k+1}}$$

已知  $\mathbf{W}_{2^k}$  每個 row 的 sign change 數,由上到下分別為  $0,1,2,3,.....,2^{k-1}$ 

則  $V_{2^{k+1}}$  每個 row 的 sign change 數,由上到下分別為  $0, 3, 4, 7, \ldots, 2^{k+1}-1, 1, 2, 5, 6, \ldots, 2^{k+1}-2,$ 

若 row 的index 由0 開始

則  $V_{2^{k+1}}$ 第 n 個 row (n is even and n < N/2) 的 sign change 為 2n (n is odd and n < N/2) 的 sign change 為 2n + 1 (n is even and  $n \ge N/2$ ) 的 sign change 為 2n+1-N (n is odd and  $n \ge N/2$ ) 的 sign change 為 2n-N

要根據 sign change 的數目將  $V_{2^{k+1}}$  的 row 重新排列

$$\mathbf{V}_{\mathbf{2}^{k+1}} \xrightarrow{permutation} \mathbf{W}_{\mathbf{2}^{k+1}}$$

#### sign changes

504

$$\mathbf{W}_{2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \mathbf{V}_{4} = \begin{bmatrix} \mathbf{W}_{2} & \mathbf{W}_{2} \\ \mathbf{W}_{2} & -\mathbf{W}_{2} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 \times -1 \times 1 \times -1 & -1 & 3 \\ 1 & 1 \times -1 & -1 \times 1 \end{bmatrix} \qquad \frac{3}{1}$$

#### sign changes

Constraint for the number of points of the Walsh transform:

N must be a power of  $2(2, 4, 8, 16, 32, \dots)$ 

Although in Matlab it is possible to define the  $12 \cdot 2^k$  point or the  $20 \cdot 2^k$  point Walsh transform, the inverse transform require the floating-point operation.

hadamard (N)

### **14-C** Alternative Forms of the Walsh Transform

#### 標準定義

from zero-crossing

- Sequency ordering (i.e., Walsh ordering) ...... using for signal processing
- Dyadic ordering (i.e., Paley ordering) ..... using for control
- Natural ordering (i.e., Hadamard ordering) .....using for mathematics

Sequency ordering	Dyadic ordering	Natural ordering	W[m, n]
•	→(Gray Code) ←	→(Bit Reversal)	
row 0 =	row 0 =	row 0 =	[1, 1, 1, 1, 1, 1, 1]
row 1 =	row 1 =	row 4 =	[1, 1, 1, 1, -1, -1, -1, -1]
row 2 =	row 3 =	row 6 =	[1, 1, -1, -1, -1, 1, 1]
row 3 =	row 2 =	row 2 =	[1, 1, -1, -1, 1, 1, -1, -1]
row 4 =	row 6 =	row 3 =	[1,-1,-1, 1, 1,-1,-1, 1]
row 5 =	row 7 =	row 7 =	[1,-1,-1, 1,-1, 1, 1,-1]
row 6 =	row 5 =	row 5 =	[1,-1, 1,-1,-1, 1,-1, 1]
row 7 =	row 4 =	row 1 =	[1,-1, 1,-1, 1,-1, 1,-1]

• Dyadic ordering Walsh transform

• Natural ordering Walsh transform

• binary code 
$$n = \sum_{p=1}^{k} b_p 2^{p-1}$$
 to gray code  
When  $N = 2^k$ 

$$g_k = b_k$$
,  $g_q = XOR(b_{q+1}, b_q)$  for  $q = k-1, k-2, ...., 1$   $m = \sum_{q=1}^k g_q 2^{q-1}$ 

• gray code to binary code

When 
$$N = 2^k$$

$$b_k = g_k$$
,  $b_q = XOR(b_{q+1}, g_q)$  for  $q = k-1, k-2, ...., 1$ 

# **14-D** Properties

- (1) Orthogonal Property
- (2) Zero-Crossing Property
- (3) Even / Odd Property
- (4) Linear Property

If 
$$f[n] \Rightarrow F[m]$$
,  $g[n] \Rightarrow G[m]$ , ( $\Rightarrow$  means the Walsh transform)

then 
$$a f[n] + b g[n] \Rightarrow a F[m] + b G[m]$$

#### (5) Addition Property

$$W[m,n] \cdot W[l,n] = W[m \oplus l,n]$$

註: Addition modulo 2 (denoted by ⊕)

$$0 \oplus 0 = 1 \oplus 1 = 0$$
,  $0 \oplus 1 = 1 \oplus 0 = 1$ ,

$$(\sum_{p=0}^{k} a_k 2^p) \oplus (\sum_{p=0}^{k} b_k 2^p) = \sum_{p=0}^{k} (a_k \oplus b_k) 2^p$$

Example:

 $\oplus \frac{7}{4} \qquad \frac{1}{1} \quad \frac{1}{0} \quad \frac{1}{0}$ 

, therefore  $3 \oplus 7 = 4$ 

⊕: logic addition (similar to XOR)

(6) Special functions

$$\delta[n] = 1$$
 when  $n = 0$ ,  $\delta[n] = 0$  when  $n \neq 0$   
 $\delta[n] \Rightarrow 1$ ,  $1 \Rightarrow N \cdot \delta[n]$ 

(7) Shifting property

If 
$$f[n] \Rightarrow F[m]$$
, then  $f[n \oplus k] \Rightarrow W(k, m) \cdot F[m]$ 

(8) Modulation property

If 
$$f[n] \Rightarrow F[m]$$
, then  $W(k, n) \cdot f[n] \Rightarrow F[m \oplus k]$ 

(9) Parseval's Theorem

If 
$$f[n] \Rightarrow F[m]$$
, If  $f[n] \Rightarrow F[m]$ ,  $g[n] \Rightarrow G[m]$ ,
$$\sum_{n=0}^{N-1} |f[n]|^2 = \frac{1}{N} \sum_{n=0}^{N-1} |F[m]|^2 , \sum_{n=0}^{N-1} f[n]g[n] = \frac{1}{N} \sum_{n=0}^{N-1} F[m]G[m]$$

If 
$$f[n] \Rightarrow F[m]$$
,  $g[n] \Rightarrow G[m]$ ,  
then  $h[n] = f[n] \star g[n] \Rightarrow F[m] G[m]$ 

$$f[n] \star g[n] = W^{-1}(W(f[n])W(g[n]))$$

W: Walsh transform

W<sup>-1</sup>: inverse Walsh transform

★ means the "logical convolution"

\* means the "logical convolution"
$$h[n] = f[n] * g[n] = \sum_{l=0}^{N-1} f[l]g[n \oplus l] = \sum_{l=0}^{N-1} f[n \oplus l]g[l]$$

For example, when N = 8,

$$h[3] = f[0]g[3] + f[1]g[2] + f[2]g[1] + f[3]g[0] + f[4]g[7] + f[5]g[6] + f[6]g[5] + f[7]g[4]$$

$$h[2] = f[0]g[2] + f[1]g[3] + f[2]g[0] + f[3]g[1] + f[4]g[6] + f[5]g[7] + f[6]g[4]$$
 $+ f[7]g[5]$ 

Comparison: In digital signal processing, we often use

linear convolution (standard form of convolution)

$$\sum_{l=0}^{N-1} f[l]g[n-l]$$

#### circular convolution

H[h]: 
$$\sum_{l=0}^{N-1} f[l]g[((n-l))_{N}]$$

$$IDFT_{N} \{DFT_{N}[f[n]]DFT_{N}[g[n]]\} = \sum_{l=0}^{N-1} f[l]g[((n-l))_{N}]$$

For example, when N = 8,

$$H[3] = f[0]g[3] + f[1]g[2] + f[2]g[1] + f[3]g[0] + f[4]g[7] + f[5]g[6] + f[6]g[5] + f[7]g[4]$$

$$H[2] = f[0]g[2] + f[1]g[1] + f[2]g[0] + f[3]g[7] + f[4]g[6] + f[5]g[5] + f[6]g[4]$$

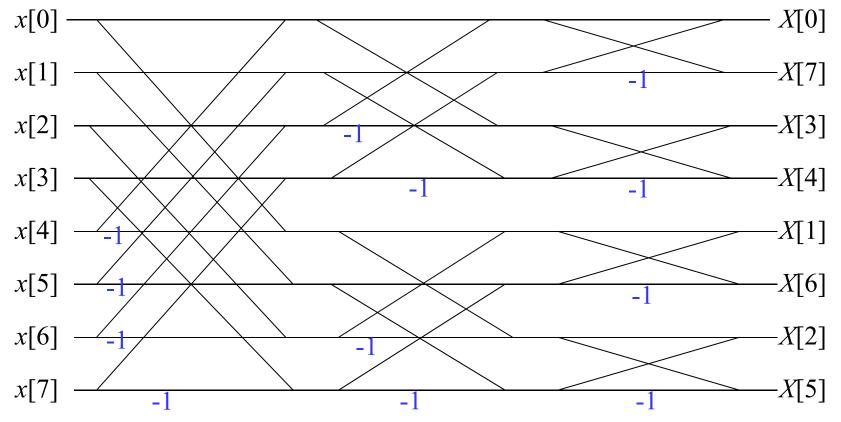
$$h = 2 + f[7]g[3]$$

# **14-E Butterfly Fast Algorithm**

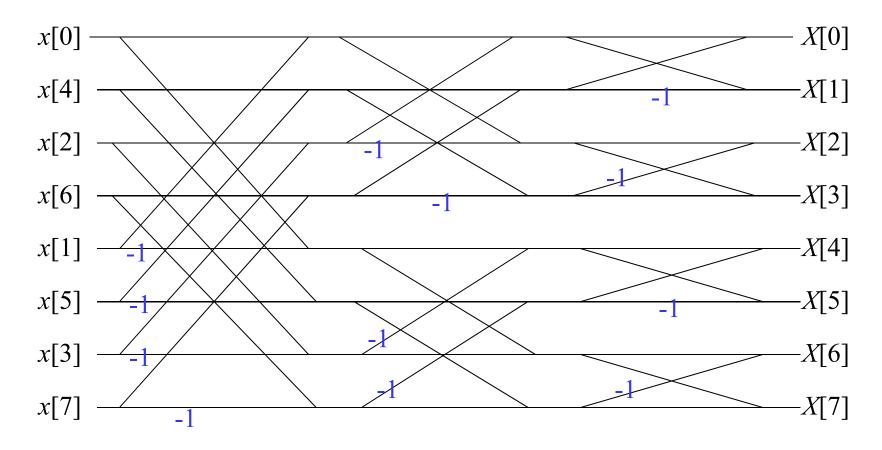


(Method 1) John L. Shark's Algorithm

8點:3個stage 1個 stage:8個加法 3個stage總共24個加法



#### (Method 2) Manz's Sequence Algorithm



There are other fast implementation algorithm for the Walsh transform.

# **O** 14-F Applications

Walsh transform 適合作 spectrum analysis,但未必適合作convolution

may not be better than DFT, DCT

Applications of the Walsh transform

Bandwidth reduction

High resolution

Modulation and Multiplexing

Information coding

Feature extraction

stair-like

ECG signal (in medical signal processing) analysis

Hadamard spectrometer

Avoiding quantization error



• The Walsh transform is suitable for the function that is a combination of Step functions

of the Walsh transform

New Applications: CDMA (code division multiple access)

#### **● 14-G Jacket Transform**

把部分的 1 用  $\pm 2^k$  取代 4-point Jacket transform  $\mathbf{J_4} = \begin{bmatrix} 1 & x & x & 1 \\ 1 & w & -w & -1 \\ 1 & -x & -x & 1 \\ 1 & -w & w & -1 \end{bmatrix} \qquad w = 2^k, \quad x = 2^h,$   $\mathbf{v} = \mathbf{J}$   $\mathbf{v} = \mathbf{J}$  $\mathbf{J}_{2^{k+1}} = \mathbf{P} \begin{bmatrix} \mathbf{J}_{2^k} & \mathbf{J}_{2^k} \\ \mathbf{J}_{2^k} & -\mathbf{J}_{2^k} \end{bmatrix} \qquad \mathbf{P}: \text{ row permutation}$   $\mathbf{J}_{2^{k+1}} = \mathbf{J}_{2^k} \quad \mathbf{J}_{2^k$  $2^{k+1}$ -point Jacket

[Ref] M. H. Lee, "A new reverse Jacket transform and its fast algorithm," *IEEE Trans. Circuits Syst.-II*, vol. 47, pp. 39-46, 2000.

#### **● 14-H Haar Transform**

[Ref] H. F. Harmuth, *Transmission of Information by Orthogonal Functions*, Springer-Verlag, New York, 1972

520

N = 16

$$H[m, n]$$
 的值  $(m = 0, 1, ..., 2^k - 1, n = 0, 1, ..., 2^k - 1)$ :
$$H[0, n] = 1 \text{ for all } n$$
If  $2^h \le m < 2^{h+1}$ 

$$H[m, n] = 1 \text{ for } (m - 2^h)2^{k-h} \le n < (m - 2^h + 1/2)2^{k-h}$$

$$H[m, n] = -1 \text{ for } (m - 2^h + 1/2)2^{k-h} \le n < (m - 2^h + 1)2k^{-h}$$

$$H[m, n] = 0 \text{ otherwise}$$

#### 運算量比 Walsh transforms 更少

Applications: localized spectrum analysis, edge detection

#### AD 1972

Transforms	Running Time	terms required for NRMSE < 10 <sup>-5</sup>
DFT	9.5 sec	43
Walsh Transform	2.2 sec	65
Haar Transform	0.3 sec	128

#### Main Advantage of the Haar Transform

- (1) Fast (but this advantage is no longer important)
- (2) Analysis of the local high frequency component (The wavelet transform is a generalization of the Haar transform)
- (3) Extracting local features (Example: Adaboost face detection)

Haar -> Wavelet transform

# 附錄十六 SCI Papers 查詢方式

我們經常聽到 SCI 論文, impact factor...那麼什麼是 SCI 和 impact factor? 什麼樣的論文是 SCI Papers? Impact factor 號如何查詢?

SCI 全名: Science Citation Index

(A) SCI 相關網站: ISI Web of Knowledge

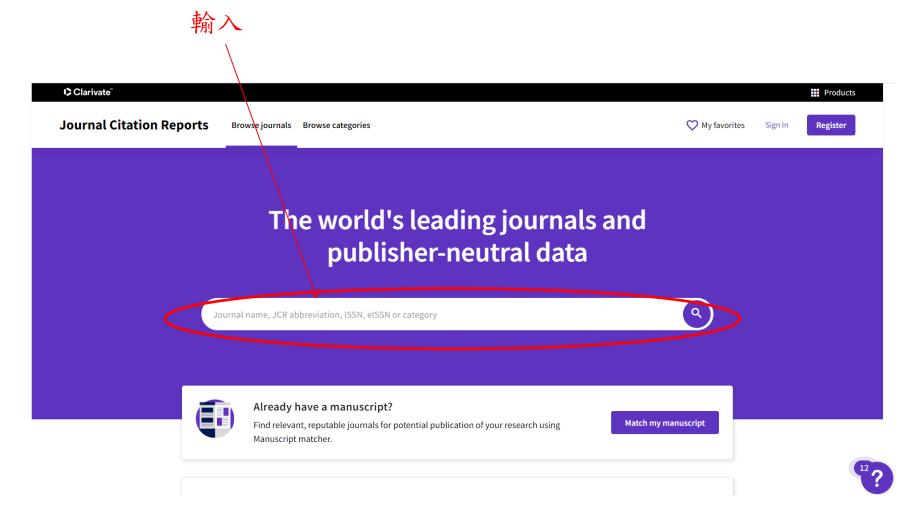
連結至 ISI Web of Knowledge

http://admin-apps.webofknowledge.com/JCR/JCR?RQ=HOME

註:必需要在台大上網,或是在其他有付錢給 ISI 的學術單位上網, 才可以使用 ISI Web of Knowledge

#### (B) 在 Go to Journal Profile

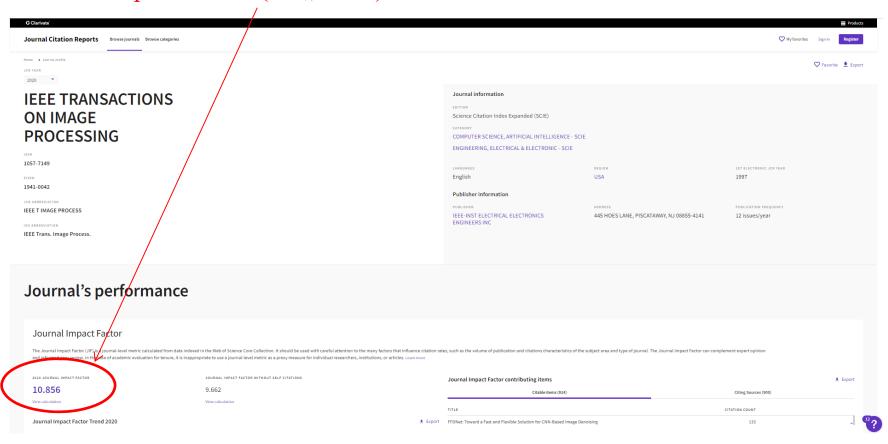
輸入你想查詢的期刊(完整名稱)



#### 若有搜尋到,則代表這個期刊是 SCI 期刊

#### 並且會顯示出這個期刊的 impact factor

#### Impact Factor (影響係數)



#### (C) 關於 impact factor (影響係數):

若一個 journal 裡面的文章,被別人引用的次數越多,則這個 journal 的 impact factor 越高

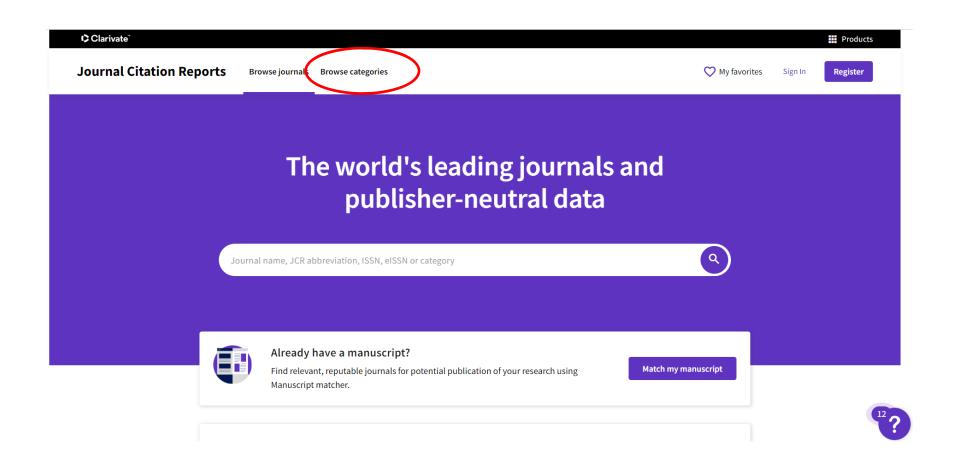
一般而言, impact factor 在 3.5 以上的 journals,已经算是高水準的期刊中等水準的期刊的 impact factors 在 1.5 到 3.5 之間

Nature 的 impact factor 為 49.962 Science 的 impact factor 為 47.728

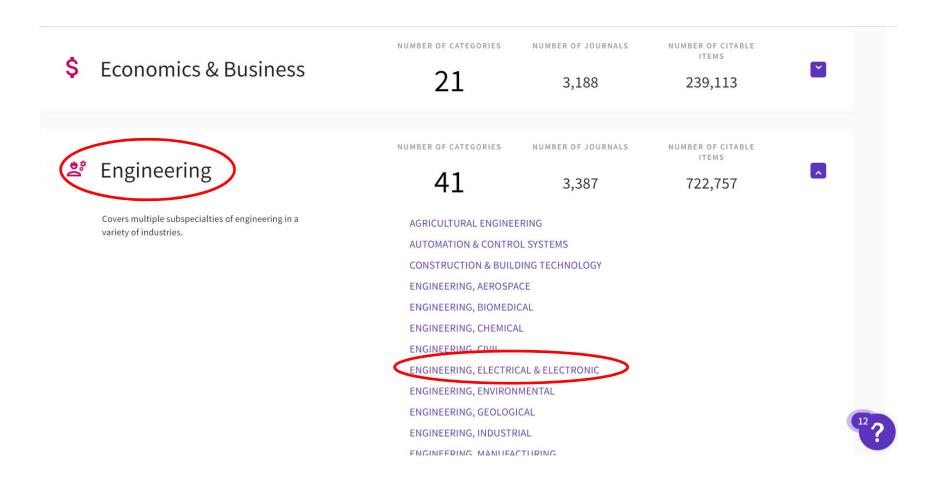
IEEE 系列的期刊的 impact factors 通常在2到13之間

#### (D) 要查詢一個領域有哪些 SCI journals

連結至 ISI Web of Knowledge 之後,點選「Browse Category」



#### 再選擇要查詢的 category,如



#### (E) EI (Engineering Village)

官方網站: www.engineeringvillage.org

http://www.engineeringvillage.com/search/quick.url

查詢期刊或研討會是否為EI

http://tul.blog.ntu.edu.tw/archives/4627

#### (F) SSCI (Social Science Citation Index)

比較偏向於社會科學

http://www.thomsonscientific.com/cgi-bin/jrnlst/jloptions.cgi?PC=J

#### (G) Conference 排名

Microsoft Academic Search 有列出各領域知名的 conferences 並加以排名 (大致上也是被引用越多的排名越前面)

和通訊與信號處理相關的 conferences,大多排名於

http://academic.research.microsoft.com/RankList?entitytype=3&topDomainID=2&subDomainID=0&last=0&start=1&end=100

或

http://academic.research.microsoft.com/RankList?entitytype=3&topDomainID=8&subDomainID=0&last=0&start=1&end=100

#### (H) H Index

論文除了量以外,也要注意 citation 的次數

將發表的論文的 citation 次數從高到低做排序 如果排名第N名的論文 citation 數量大於等於N但是排名第N+1名的論文 citation 數量小於等於N+1

則 H index = N

Example: 假設有一個學者發表了10篇論文, citation 由多到少分別為 33, 24, 18, 13, 9, 7, 4, 3, 1, 1 則這個學者的 H-index 為 6

# 寫論文和投稿的經驗談

研究生經常會寫論文並且投稿。要如何讓論文投稿之後能夠順利的被接受,相信是同學們所期盼的,畢竟每篇論文都是大家花了不少時間的心血結晶,若論文能夠順利的被接受,也代表了自己的成果總算獲得了肯定。然而,影響論文是否被接受的因素很多,一個好的研究成果,還是配合好的編寫技巧,才可以被一流的期刊或研討會所接受。以下是個人關於論文編寫與投稿的經驗談:

(1) 你的論文的「賣點」(優點) 是什麼?人家有沒有辦法一眼看得出來你論文的「賣點」?

寫論文其實就是在推銷商品,而所謂的「商品」,就是你的「研究成果」。要說服人家接受你的商品,首先就是要強調你的商品的「賣點」。

#### (2) 和既有的方法的比較是否足夠?

要證明你所提出的方法是有效的,最好的方式,就是和既有的方法相比較,而且比較的對象越多越好,越新越好。

- (3) 和前人的方法相比,你的方法創新的地方在何處?審稿者是否能看得出來你論文創新的地方?
- (4) 就算你的文章和理論相關,最好也多提出實際應用的例子
- (5) 參考資料越多越好,越新越好 (在研究一個領域時,論文 survey 的量要足夠)
- (6) Previous work (前人已經提出的概念) 精簡介紹即可,多強調自己的貢獻。 Introduction 加上 Previous work 最好不要超過一篇論文的四分之一
- (7) 英文表達能力要有一定的水準

#### (8)可以多用數學式和圖來解釋概念,有時會比文字還清楚

通常東方人英文表達能力有限。審稿者經常會看你們的圖表和數學式(而非文字)來判斷你們論文的品質

- (9) 同樣的道理,可以用「條列式」的方式來取代一大段文字來描述方法的觀念、流程、或優點
- (10) 可以用 Conference 的期限來要求自己多寫研討會論文,之後再陸續改成期刊論文投稿,如此一年的論文量將很可觀
- (11)多注意格式,不同的期刊或研討會,對格式的要求也不同
- (12) 最後,問自己一個問題:

如果你是審稿者,你會滿意你寫的這一篇論文嗎?

若答案是肯定的再投稿

# XV. Orthogonal Transform and Multiplexing

### **15-A** Orthogonal and Dual Orthogonal

Any  $M \times N$  discrete linear transform can be expressed as the matrix form:

$$\begin{bmatrix} y[0] \\ y[1] \\ y[2] \\ \vdots \\ y[M-1] \end{bmatrix} = \begin{bmatrix} \phi_0^*[0] & \phi_0^*[1] & \phi_0^*[2] & \cdots & \phi_0^*[N-1] \\ \phi_1^*[0] & \phi_1^*[1] & \phi_1^*[2] & \cdots & \phi_1^*[N-1] \\ \phi_2^*[0] & \phi_2^*[1] & \phi_2^*[2] & \cdots & \phi_2^*[N-1] \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \phi_{M-1}^*[0] & \phi_{M-1}^*[1] & \phi_{M-1}^*[2] & \cdots & \phi_{M-1}^*[N-1] \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ \vdots \\ x[N-1] \end{bmatrix}$$

$$\mathbf{Y} = \mathbf{A}$$

$$\mathbf{X}$$

$$y[m] = \langle x[n], \phi_m[n] \rangle = \sum_{n=0}^{N-1} x[n] \phi_m^*[n]$$
inner product

Orthogonal: 
$$\langle \phi_k[n], \phi_h[n] \rangle = \sum_{n=0}^{N-1} \phi_k[n] \phi_h^*[n] = 0$$
 when  $k \neq h$ 

orthogonal transforms 的例子:

- discrete Fourier transform
- discrete cosine, sine, Hartley transforms
- Walsh Transform, Haar Transform
- discrete Legendre transform
- discrete orthogonal polynomial transforms
  Hahn, Meixner, Krawtchouk, Charlier

為什麼在信號處理上,我們經常用 orthogonal transform?

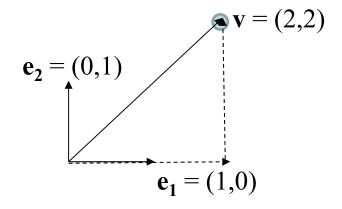
Orthogonal transform 最大的好處何在?

In communication, the basis 
$$\emptyset_{k}[n]$$
 is used to transmit the data in the  $k^{th}$  channel

 $y[n] = x_1 \phi_1[n] + x_2 \phi_2[n] + \cdots + x_N \phi_N[n]$ 

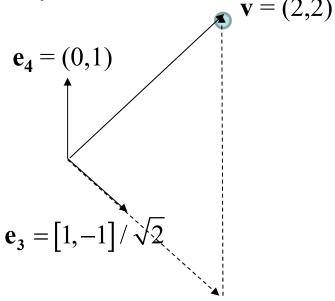
to refrieve  $x_1$ 
 $\langle y[n], \phi_1[n] \rangle = x_1 \langle \phi_1[n], \phi_1[n] \rangle + x_2 \langle \phi_2[n], \phi_1[n] \rangle$ 
 $+\cdots + x_N \langle \phi_N[n], \phi_1[n] \rangle$ 
 $x_1 = \frac{\langle y[n], \phi_1[n] \rangle}{\langle \phi_1[n], \phi_1[n] \rangle}$ 
 $x_2 = \frac{\langle y[n], \phi_1[n] \rangle}{\langle \phi_1[n], \phi_1[n] \rangle}$ 

如果是orthogonal 要還原訊號時, 不同channel 傳送的東西就不會互相 干擾,比較能夠簡單還原 for (DMA  $\chi_k = \frac{\langle y[n], W_k[n] \rangle}{N}$ With] is the kth row of the N-point Walsh matrix



$$\mathbf{v} = 2\mathbf{e_1} + 2\mathbf{e_2}$$

e<sub>3</sub> and e<sub>4</sub> are not orthogonal



$$\mathbf{v} = 2\sqrt{2}\mathbf{e_3} + 4\mathbf{e_4}$$

• If partial terms are used for reconstruction

#### for orthogonal case,

perfect reconstruction: 
$$x[n] = \sum_{m=0}^{N-1} C_m^{-1} y[m] \phi_m[n]$$

partial reconstruction: 
$$x_K[n] = \sum_{m=0}^{K-1} C_m^{-1} y[m] \phi_m[n]$$
  $K < N$ 

reconstruction error of partial reconstruction

$$\begin{aligned} \left\|x[n] - x_{K}[n]\right\|^{2} &= \sum_{n=0}^{N-1} \left\|\sum_{m=K}^{N-1} C_{m}^{-1} y[m] \phi_{m}[n]\right\|^{2} \\ &= \sum_{n=0}^{N-1} \sum_{m=K}^{N-1} C_{m}^{-1} y[m] \phi_{m}[n] \sum_{m_{1}=K}^{N-1} C_{m_{1}}^{-1} y^{*}[m_{1}] \phi_{m_{1}}^{*}[n] \\ &= \sum_{m=K}^{N-1} \sum_{m_{1}=K}^{N-1} C_{m}^{-1} y[m] C_{m_{1}}^{-1} y^{*}[m_{1}] \sum_{n=0}^{N-1} \phi_{m}[n] \phi_{m_{1}}^{*}[n] \\ &= \sum_{m=K}^{N-1} \sum_{m_{1}=K}^{N-1} C_{m}^{-1} y[m] C_{m_{1}}^{-1} y^{*}[m_{1}] C_{m} \delta[m-m_{1}] = \sum_{m=K}^{N-1} C_{m}^{-1} |y[m]|^{2} \end{aligned}$$

由於  $C_m^{-1} |y[m]|^2$  一定是正的,可以保證 K 越大, reconstruction error 越小

#### For non-orthogonal case,

perfect reconstruction: 
$$x[n] = \sum_{m=0}^{N-1} B[n,m]y[m]$$
  $\mathbf{B} = \mathbf{A}^{-1}$ 

partial reconstruction: 
$$x_K[n] = \sum_{m=0}^{K-1} B[n,m] y[m]$$
  $K < N$ 

reconstruction error of partial reconstruction

$$||x[n] - x_K[n]||^2 = \sum_{n=0}^{N-1} ||\sum_{m=K}^{N-1} B[n,m]y[m]||^2$$

$$= \sum_{n=0}^{N-1} \sum_{m=K}^{N-1} B[n,m]y[m] \sum_{m_1=K}^{N-1} B^*[n,m_1]y^*[m_1]$$

$$= \sum_{m=K}^{N-1} \sum_{m_1=K}^{N-1} y[m]y^*[m_1] \sum_{n=0}^{N-1} B[n,m]B^*[n,m_1]$$

由於  $y[m]y^*[m_1]\sum_{n=0}^{N-1}B[n,m]B^*[n,m_1]$  不一定是正的,無法保證 K 越大, reconstruction error 越小

## **15-B** Frequency and Time Division Multiplexing

傳統 Digital Modulation and Multiplexing: 使用 Fourier transform

• Frequency-Division Multiplexing (FDM)

$$z(t) = \sum_{n=0}^{N-1} X_n \exp(j2\pi f_n t)$$
  $X_n = 0 \text{ or } 1$   
$$X_n \text{ can also be set to be } -1 \text{ or } 1$$

When (1) 
$$t \in [0, T]$$
 (2)  $f_n = n/T$ 

$$z(t) = \sum_{n=0}^{N-1} X_n \exp\left(j\frac{2\pi nt}{T}\right)$$

it becomes the <u>orthogonal</u> frequency-division multiplexing (OFDM) in the continuous case.

Furthermore, if the time-axis is also sampled

$$t = mT/N, m = 0, 1, 2, ...., N-1$$

$$z(m\frac{T}{N}) = \sum_{n=0}^{N-1} X_n \exp(j\frac{2\pi nm}{N})$$

(OFDM in the discrete case)

 $t \in [0,T]$ sampling for t-axis

 $z\left(m\frac{T}{N}\right) = \sum_{n=0}^{N-1} X_n \exp\left(j\frac{2\pi nm}{N}\right)$  (i) or thogonal different channels will not interfere with one another (ii) fast algorithm

then the OFDM is equivalent to the transform matrix of the <u>inverse</u> discrete Fourier transform (IDFT), which is one of the discrete orthogonal transform.

如果是orthogonal 要還原訊號時, 不同channel 傳送的東西就不會互相干擾,比較能夠簡單還原

Modulation: 
$$Y_m = \sum_{m=0}^{N-1} A[m, n] X_n$$

Demodulation: 
$$X_n = \frac{1}{N} \sum_{m=0}^{N-1} A^* [m, n] Y_m$$

Example: 
$$N = 8$$

$$X_n = [1, 0, 1, 1, 0, 0, 1, 1]$$
  $(n = 0 \sim 7)$ 

### • Time-Division Multiplexing (TDM)

$$z(0) = X_0, \quad z\left(\frac{T}{N}\right) = X_1, \quad z\left(2\frac{T}{N}\right) = X_2, \quad \cdots, \quad z\left((N-1)\frac{T}{N}\right) = X_{N-1}$$

$$y(m) = z\left(m\frac{T}{N}\right) = \sum_{m=0}^{N-1} A[m, n]X_n$$

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$
 (also a discrete orthogonal transform)

### 思考:

既然 time-division multiplexing 那麼簡單

那為什麼要使用 frequency-division multiplexing 和 orthogonal frequency-division multiplexing (OFDM)?

## **© 15-C Code Division Multiple Access (CDMA)**

除了 frequency-division multiplexing 和 time-division multiplexing,是否 還有其他 multiplexing的方式?

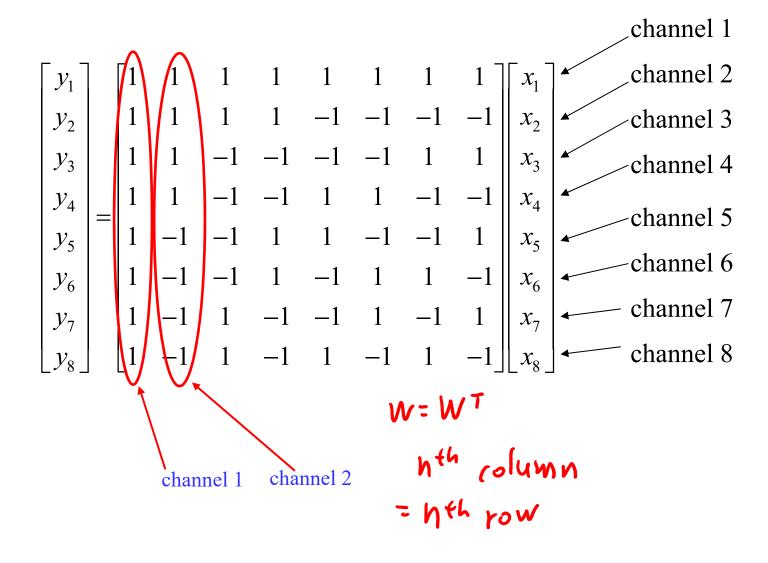
使用其他的 <u>orthogonal transforms</u>
即 code division multiple access (CDMA)

CDMA is an important topic in spread spectrum communication

### 參考資料

- [1] M. A. Abu-Rgheff, *Introduction to CDMA Wireless Communications*, Academic, London, 2007
- [2] 邱國書, 陳立民譯, "CDMA 展頻通訊原理," 五南, 台北, 2002.

#### CDMA 最常使用的 orthogonal transform 為 Walsh transform



當有兩組人在同一個房間裡交談 (A和B交談), (C和D交談), 如何才能夠彼此不互相干擾?

- (1) Different Time
- (2) Different Tone
- (3) Different Language

#### CDMA 分為:

(1) Orthogonal Type (2) Pseudorandom Sequence Type

```
Orthogonal Type 的例子: 兩組資料 [1,0,1] [1,1,0] (1) 將 0 變為 -1 [1,-1,1] [1,1,-1] (2) 1,-1,1 modulated by [1,1,1,1,1,1,1] (channel 1) \rightarrow [1,1,1,1,1,1,1,1,1,1] \rightarrow [1,1,1,1,1,1,1,1,1] \rightarrow [1,1,1,1,1,1,1,1,1] \rightarrow [1,1,1,1,1,1,1,1] \rightarrow [1,1,1,1,1,1,1] \rightarrow [1,1,1,1,1,1] \rightarrow [1,1,1,1,1] \rightarrow [1,1,1,1,1] \rightarrow [1,1,1,1,1] \rightarrow [1,1,1,1] \rightarrow [1,1,1,1] \rightarrow [1,1,1] \rightarrow [1,1,1] \rightarrow [1,1,1] \rightarrow [1,1,1] \rightarrow [1,1,1] \rightarrow [1,1] \rightarrow [1,1]
```

### 注意:

- (1) 使用 N-point Walsh transform 時,總共可以有N 個 channels
- (2) 除了 Walsh transform 以外,其他的 orthogonal transform 也可以使用
- (3) 使用 Walsh transform 的好處

• Orthogonal Transform 共通的問題: 需要同步 synchronization

$$\mathbf{R_1} = [1, 1, 1, 1, 1, 1, 1]$$

$$\mathbf{R_2} = [1, 1, 1, 1, -1, -1, -1, -1]$$

$$\mathbf{R_5} = [1, -1, -1, 1, 1, -1, -1, 1]$$

$$\mathbf{R_8} = [1, -1, 1, -1, 1, -1, 1, -1]$$

但是某些 basis, 就算不同步也近似 orthogonal

$$\langle \mathbf{R}_1[n], \mathbf{R}_1[n] \rangle = 8, \ \langle \mathbf{R}_1[n], \mathbf{R}_k[n] \rangle = 0 \text{ if } k \neq 1$$

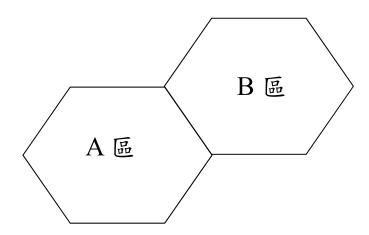
$$<\mathbf{R_1}[n], \mathbf{R_k}[n-1]> = 2 \text{ or } 0 \text{ if } k \neq 1.$$

這裡的shift為circular shift

#### CDMA 的優點:

- (1) 運算量相對於 frequency division multiplexing 減少很多
- (2) 可以減少 noise 及 interference的影響
- (3) 可以應用在保密和安全傳輸上
- (4) 就算只接收部分的信號,也有可能把原來的信號 recover 回來
- (5) 相鄰的區域的干擾問題可以減少

相鄰的區域,使用差距最大的「語言」,則干擾最少



假設 A 區使用的 orthogonal basis 為  $\phi_k[n], k = 0, 1, 2, ..., N-1$ 

B 區使用的 orthogonal basis 為  $\mu_h[n]$ , h = 0, 1, 2, ..., N-1

設法使 
$$\max\left(\left|\frac{\langle \phi_k[n], \mu_h[n] \rangle}{\langle \phi_k[n], \phi_h[n] \rangle}\right|\right)$$
 為最小

$$k = 0, 1, 2, ..., N-1, h = 0, 1, 2, ..., N-1$$

#### (1) Lightening and Darkening

Input YCbCr

RGB to YCbCr

 $Y_o = f(Y)$ 

Chunchanged

Cr unchanged

Output

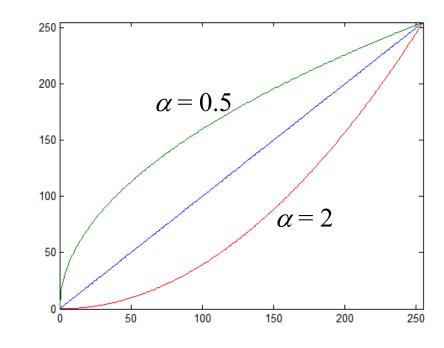
YCbCr to RGB

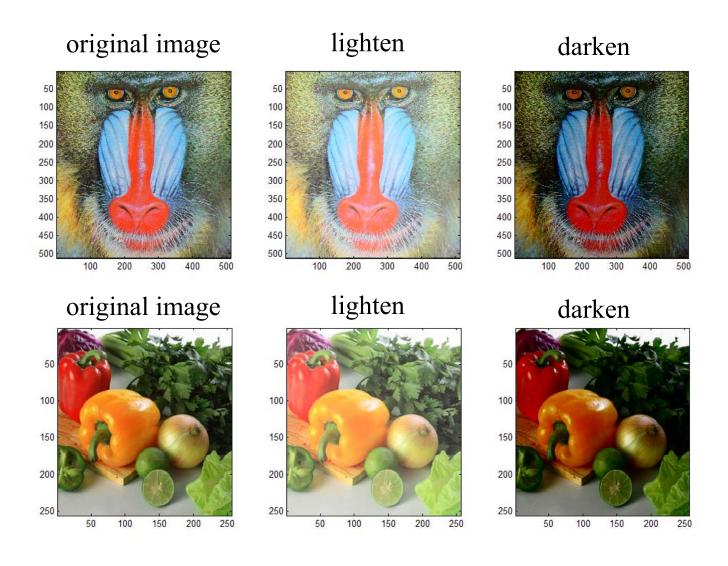
Example:

$$f(Y) = 255 \left(\frac{Y}{255}\right)^{\alpha}$$

 $\alpha$  < 1: lightening

 $\alpha > 1$ : darening





#### (2) Morphology

(2-1) Erosion (去除區域外圍)

$$A[m,n] = A[m,n] & A[m-1,n] & A[m+1,n] & A[m,n-1] & A[m,n+1]$$

*	*	*	*	*	*	*		*	*	*	*	*	*	*	
*	*	*	*	Ø	*	*	-		*	*	*	*	*	*	*
*	*	6	Ø	O	Ø,	*			*	*	*	*	O	*	*
*	Ø,	O	O	O	Ø,	*		*	*	O	O	O	*	*	
*	Ø	O	0	O	Ø,	*		*	*	O	O	O	*	*	
*	Ø	0	O	0		*		*	*	O	O	O	*	*	
*	*	Ø	0	Ø	*	*		*	*	*	O	*	*	*	
*	*	*	Ø	*	*	*		*	*	*	*	*	*	*	
*	*	*	*	*	*	*		*	*	*	*	*	*	*	

Erosion for a Non-binary Image

$$A[m,n] = \min\{A[m,n], A[m-1,n], A[m+1,n], A[m,n-1], A[m,n+1]\}$$

### (2-2) Dilation (擴大區域)

$$A[m,n] = A[m,n] || A[m-1,n] || A[m+1,n] || A[m,n-1] || A[m,n+1]$$

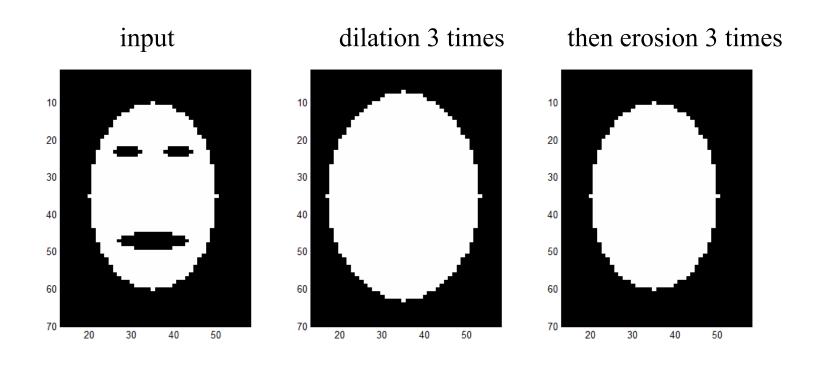
*	•	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*
*		*	*	*	*	*	*	*		*	*	*	*	*	*	*	*
*	:	*	*	*	*	*	*	*		*	*	*	*	0	*	*	*
*	:	*	*	*	O	*	*	*		*	*	*	O	O	0	O	*
*	:	*	*	O	O	0	О	*		*	*	O	O	O	0	О	O
*	:	*	O	O	O	0	*	*		*	O	O	O	O	0	O	*
*	:	*	*	*	O	0	O	*	,	*	*	O	O	O	0	О	O
*	:	*	*	*	*	*	*	*		*	*	*	*	O	0	O	*
*	:	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*
*	:	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*
*	:	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*

Dilation for a Non-binary Image

$$A[m,n] = Max\{A[m,n], A[m-1,n], A[m+1,n], A[m,n-1], A[m,n+1]\}$$

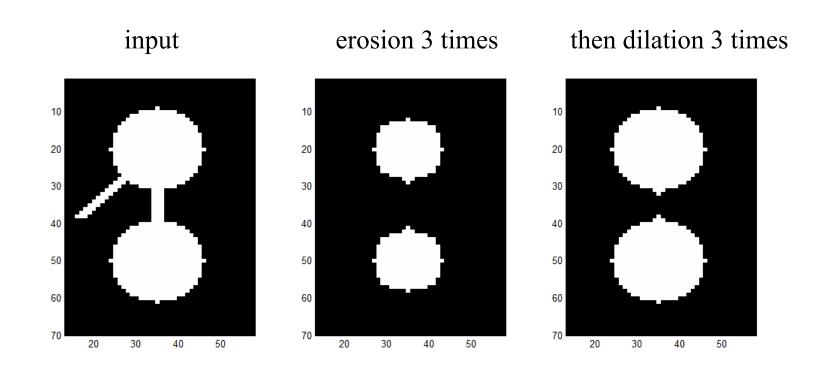
### (2-3) Closing (Hole Filling)

closing = dilation k times + erosion k times



(2-4) Opening

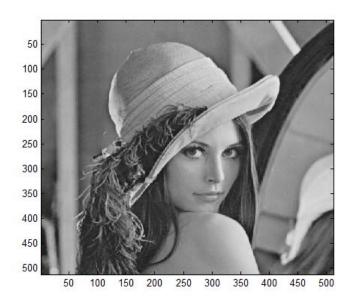
opening = erosion k times + dilation k times



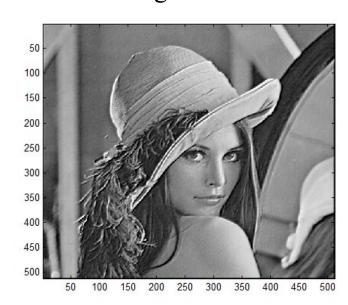
### (3) Edge enhancement

input image +  $\alpha$  | edge detection output|

Original image



With edge enhancement



#### (4) Dehaze (除霧)



He, Kaiming, Jian Sun, and Xiaoou Tang. "Single image haze removal using dark channel prior." *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, pp. 2341-2353, 2011.

Haze Model I(x) = J(x)t(x) + A(1 - t(x))

J(x): scene, I(x): observed image

 $\mathbf{t}(\mathbf{x})$ : transmission, A: intensity for the whole-haze case

A(1-t(x)): airlight

定義 dark channel J<sup>dark</sup>(x)

$$J^{dark}(\mathbf{x}) = \min_{c \in \{r, g, b\}} (\min_{\mathbf{y} \in \Omega(\mathbf{x})} (J^c(\mathbf{y}))),$$

 $\Omega(\mathbf{x})$ : some patch (a small region)

Dark channel 為一個影像在一個小範圍區域當中, RGB 的最小值

- 一個正常影像的 dark channel 大多近於 0
- 一個受 haze 影響的影像, dark channel 常常不為 0

Dehaze 的方法與流程

$$I(\mathbf{x}) = J(\mathbf{x})t(\mathbf{x}) + A(1 - t(\mathbf{x}))$$

$$J^{dark}(\mathbf{x}) = \min_{c} (\min_{\mathbf{y} \in \Omega(\mathbf{x})} (J^{c}(\mathbf{y}))) = 0. \qquad \min_{c} (\min_{\mathbf{y} \in \Omega(\mathbf{x})} (\frac{J^{c}(\mathbf{y})}{A^{c}})) = 0$$

$$\frac{I(\mathbf{x})}{A^{c}} = \frac{J(\mathbf{x})}{A^{c}}t(\mathbf{x}) + 1 - t(\mathbf{x})$$

$$\tilde{t}(\mathbf{x}) = 1 - \min_{c} (\min_{\mathbf{y} \in \Omega(\mathbf{x})} (\frac{I^{c}(\mathbf{y})}{A^{c}}))$$
find the transmission  $t(\mathbf{x})$ 

A: the 95% largest intensity of I(x)

$$\mathbf{J}(\mathbf{x}) = \frac{\mathbf{I}(\mathbf{x})}{t(\mathbf{x})} + \mathbf{A}\left(1 - \frac{1}{t(\mathbf{x})}\right)$$
 recover the original image

He, Kaiming, Jian Sun, and Xiaoou Tang. "Single image haze removal using dark channel prior." *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, pp. 2341-2353, 2011.

# 期末的勉勵

• 人生難免會有挫折,最重要的是,我們面對挫折的態度是什麼

• 長遠的願景要美麗,短期的目標要務實

#### 祝各位同學暑假愉快!

各位同學在研究上或工作上,有任何和 digital signal processing 或 time frequency analysis 方面的問題,歡迎找我來一起討論。