XIII. Number Theoretic Transform (NTT)

◎ 13-A Definition

◆ **Number Theoretic Transform and Its Inverse**

$$F(k) = \sum_{n=0}^{N-1} f(n)\alpha^{nk} \ (\text{mod } M),\ k = 0, 1, 2 \cdots, N-1$$

$$f(n) = N^{-1} \sum_{k=0}^{N-1} F(k)\alpha^{-nk} \ (\text{mod } M) \quad ,n = 0, 1, 2 \cdots, N-1$$

$$f(n) \underset{INTT}{\overset{NTT}{\Longleftrightarrow}} F(k)$$

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) α is a root of unity of order N

$$\alpha^N = 1\,(\text{mod } M)$$

$$\alpha^k \neq 1\,(\text{mod } M)\;, k = 1, 2, \cdots, N-1$$

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

$$\boxed{\begin{array}{l} \alpha^k \neq 1\,(\text{mod } M) \quad \text{for } \; k = 1, 2, \cdots, M-2 \\ \\ \alpha^{M-1} = 1\,(\text{mod } M) \end{array}}$$

α^{-1} 的求法與 N^{-1} 相似

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

[Example 1]:

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

(1) When $N = 4$

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

(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]:

$M = 7$, $N = 6$: α 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： $78 + 123 \pmod{5} = 3 + 3 \pmod{5} = 1$

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

$$a \times b = (a_1 b_1 M + a_1 b_2 + a_2 b_1)M + a_2 b_2$$

在 Number Theory 當中

只有 M^2 個可能的加法，M^2 個可能的乘法

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

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

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

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

$\because \alpha^{k-\ell} \neq 1 \qquad \therefore S_N = 0$

P.2) The NTT and INTT are exact inverse

proof：

$$g(n) = \frac{1}{N}\sum_{k=0}^{N-1} F(k)\,\alpha^{-nk} = \frac{1}{N}\sum_{k=0}^{N-1} \Big(\sum_{\ell=0}^{N-1} f(\ell)\,\alpha^{\ell k}\Big)\,\alpha^{-nk}$$

$$= \frac{1}{N}\sum_{\ell=0}^{N-1} f(\ell) \sum_{k=0}^{N-1} \alpha^{(\ell-n)k} = \frac{1}{N}\sum_{\ell=0}^{N-1} f(\ell)\cdot N\delta_{\ell,n} = f(n)$$

P.3) Symmetry

$$f(n) = f(N-n) \quad \overset{\text{NTT}}{\Leftrightarrow} \quad F(k) = F(N-k)$$

$$f(n) = -f(N-n) \quad \overset{\text{NTT}}{\Leftrightarrow} \quad F(k) = -F(N-k)$$

P.4) INNT from NTT

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

Algorithm for calculating the INNT from the NTT

(1) $F(-k)$: time reverse

$$F_0, F_1, F_2, \ldots, F_{N\text{-}1} \xrightarrow[\text{reverse}]{\text{time}} F_0, F_{N\text{-}1}, \ldots, F_2, F_1$$

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

P.9) 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., $f(n) \otimes g(n) = INTT\left\{NTT\left[f(n)\right]NTT\left[g(n)\right]\right\}$

$$f(n) \cdot g(n) \leftrightarrow \frac{1}{N} F(k) \otimes G(k)$$

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

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

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

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

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

We apply the fact that

$$\sum_{k=0}^{N-1}\alpha^{nk} = \begin{cases} 1 & \text{if } n \text{ is a multiple of } N \\ 0 & \text{otherwise} \end{cases}$$

When $q = \left(\left(n-m\right)\right)_N$

$m+q-n$ 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.

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

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

$$= \begin{cases} G(k) + \alpha^k\ H(k) & ,0 \le k \le \dfrac{N}{2} - 1 \\ G(k - \dfrac{N}{2}) + \alpha^k\ H(k - \dfrac{N}{2}) & ,\dfrac{N}{2} \le k \le N \end{cases}$$

where $G(k) = \sum_{r=0}^{N/2-1} f(2r)\,(\alpha^2)^{rk}$ $\quad H(k) = \sum_{r=0}^{N/2-1} f(2r+1)\,(\alpha^2)^{rk}$

One N-point NTT $\longrightarrow$ Two (N/2)-point NTTs

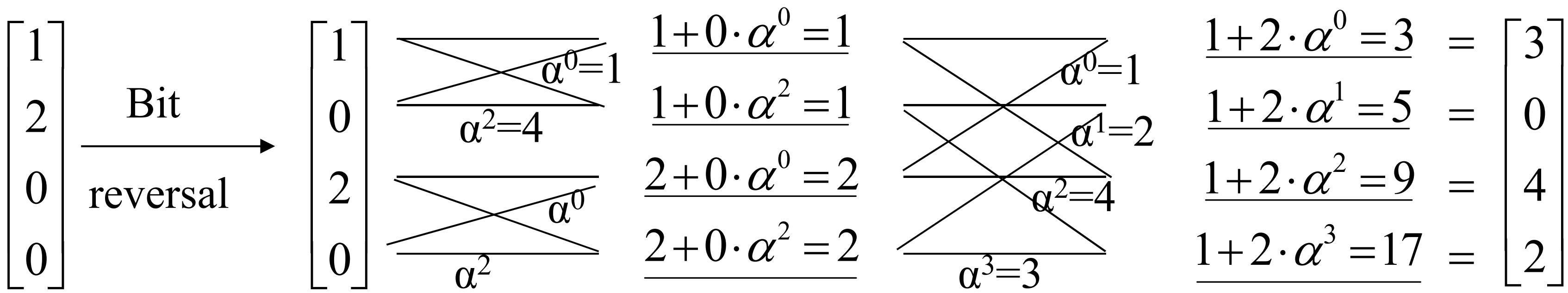
plus twiddle factors

Original sequence $f(n) = (1, 2, 0, 0)$ $N = 4, M = 5$

Permutation $(1, 0, 2, 0)$

After the 1st stage $(1, 1, 2, 2)$

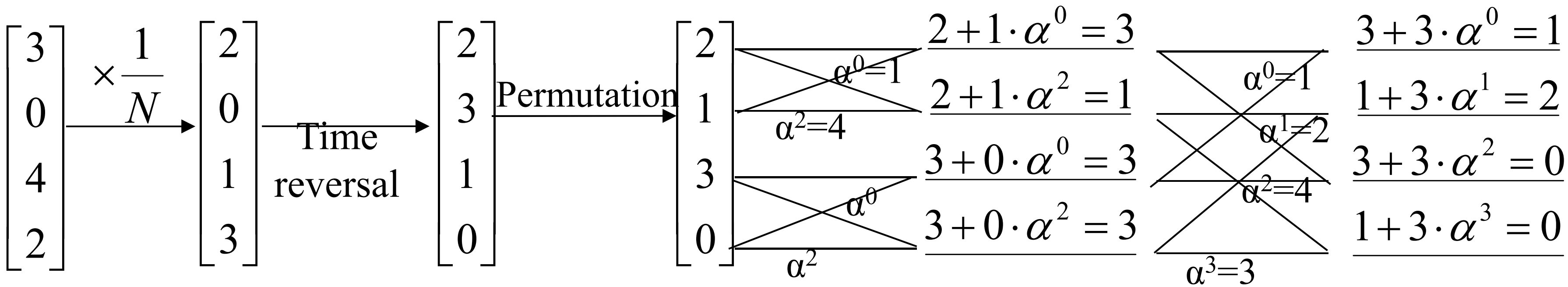
After the 2nd stage $F(k) = (3, 0, 4, 2)$



Inverse NTT by Forward NTT :

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

1) $1/N$
2) Time reversal
3) permutation
4) After first stage
5) After 2nd stage



◉ 13-E Convolution by NTT

假設 $x[n] = 0$ for $n < 0$ and $n \geq K$, $h[n] = 0$ for $n < 0$ and $n \geq H$

要計算 $x[n] * h[n] = z[n]$

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

(1) 選擇 M (the prime number for the modulus operator), 滿足

(a) M is a prime number, (b) $M \geq \max(H+K, A)$

(2) 選擇 N (NTT 的點數), 滿足

(a) N is a factor of $M-1$, (b) $N \geq H+K-1$

(3) 添 0: $x_1[n] = x[n]$ for $n = 0, 1, \ldots\ldots, K-1$,
$x_1[n] = 0$ for $n = K, K+1, \ldots\ldots., N-1$

$h_1[n] = h[n]$ for $n = 0, 1, \ldots\ldots, H-1$,
$h_1[n] = 0$ for $n = H, H+1, \ldots\ldots., N-1$

(4) $X_1[m] = \mathrm{NTT}_{N,M}\{x_1[n]\}$, $H_1[m] = \mathrm{NTT}_{N,M}\{h_1[n]\}$

NTT$_{N,M}$ 指 N-point 的 DFT (mod M)

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

(6) $z[n] = z_1[n]$ for $n = 0, 1, \ldots., H+K-1$

(移去 $n = H+K, H+K+1, \ldots\ldots N-1$ 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) $\mathrm{Max}(z[n]) - \min(z[n]) < M$ 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 $x_1 \le x[n] \le x_2$, $\quad z[n] = x[n] * h[n] = \sum_{m=0}^{H-1} h[m]x[n-m]$

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

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

where $h_1[m] = h[m]$ when $h[m] > 0$, $\quad h_1[m] = 0$ otherwise

$h_2[m] = h[m]$ when $h[m] < 0$, $\quad h_2[m] = 0$ otherwise

$$\min\left(z[n]\right) = \sum_{m=0}^{H-1} h_1[m]x_1 + \sum_{m=0}^{H-1} h_2[m]x_2$$

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

$$= (x_2 - x_1)\left\{\sum_{m=0}^{H-1} h_1[m] - \sum_{m=0}^{H-1} h_2[m]\right\} = (x_2 - x_1)\sum_{m=0}^{H-1}\left|h[m]\right|$$

◉ 13-F Special Prime Numbers

Fermat Number : $M = 2^{2^p} + 1$

$P = 0, 1, 2, 3, 4$

$M = 3, 5, 17, 257, 65537$

$P \geq 5$ may not be prime.

Mersenne Number : $M = 2^p - 1$

$P = 1, 2, 3, 5, 7, 13, 17, 19, \ldots..$

$M = 1, 3, 7, 31, 127, 8191, 131071, 524287, \ldots..$

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

$$
\begin{array}{r@{\,}r}
 & 11 \\
\cline{2-2}
100a \big) & 11001 \\
 & 100a \\
\cline{2-2}
 & 1011 \\
 & 100a \\
\cline{2-2}
 & 12 \\
 & \downarrow \\
 & 100
\end{array}
\qquad\qquad a = -1
$$

◉ 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

$$x^2 = -1 \pmod{M} \quad \text{無解}$$

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.

$$(a + i\,b) \pm (c + i\,d) = (a \pm c) + i\,(b \pm d)$$

$$\begin{aligned}(a + i\,b) \cdot (c + i\,d) &= ac + i^2 bd + i\,bc + i\,ad \\ &= (ac - bd) + i\,(bc + ad)\end{aligned}$$

◎ 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。

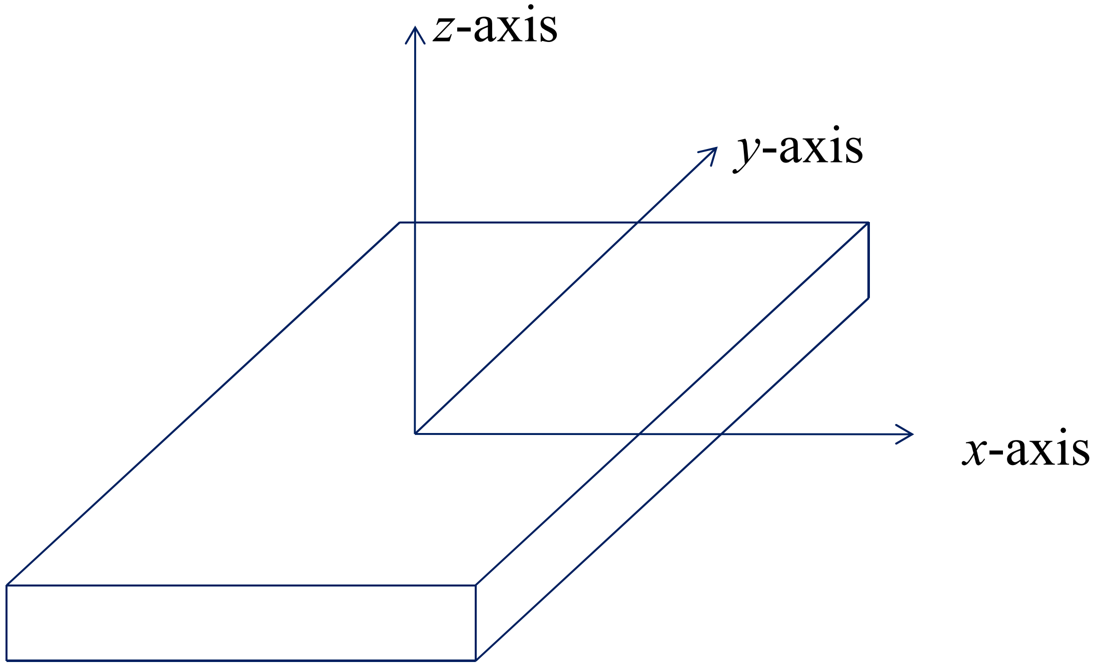
附錄十五 3-D Accelerometer 的簡介

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

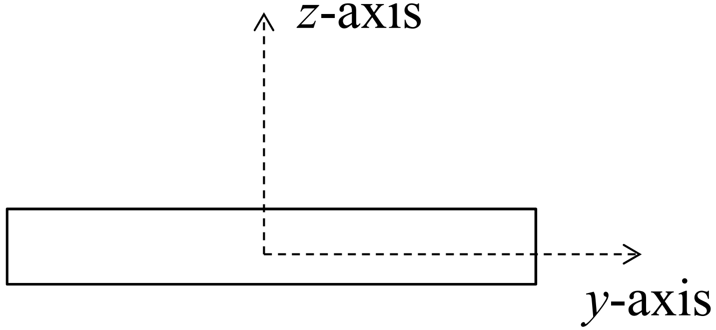
可以用來判別一個人的姿勢和動作

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

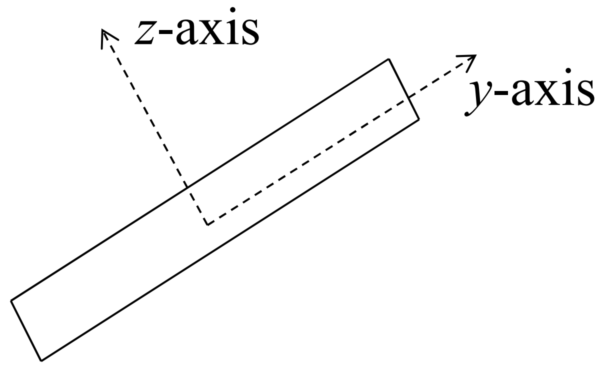
平放且靜止時， z-axis 的加速度為 $-g = -9.8$



y: 0

z: -9.8

tilted by θ



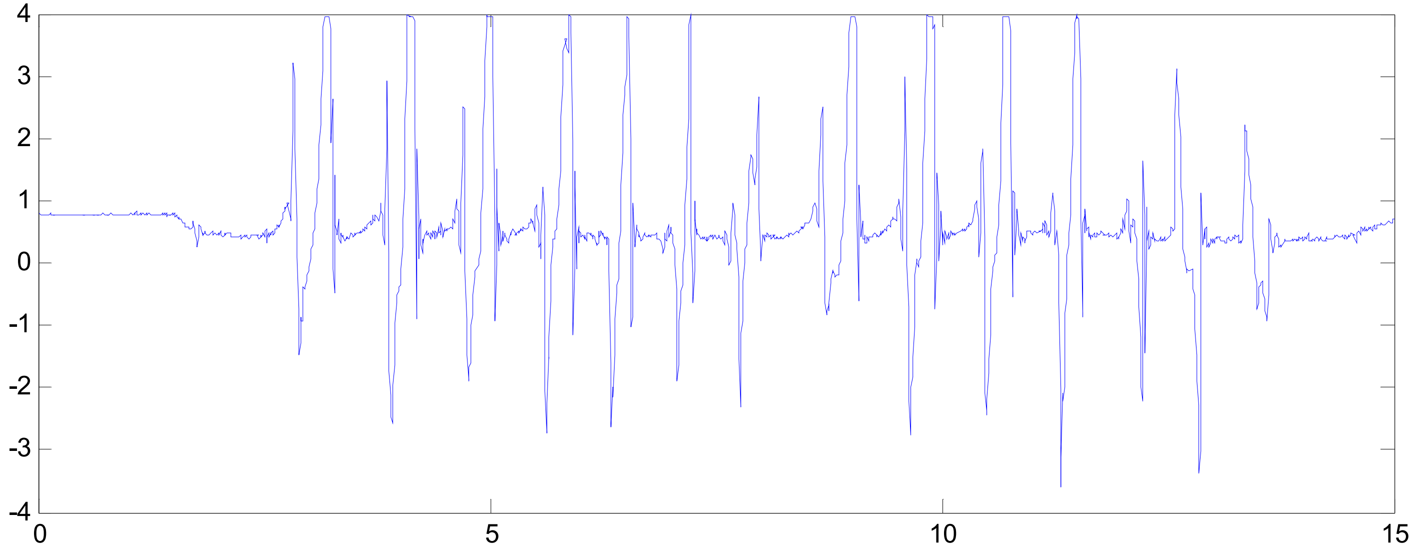
y: $-9.8\sin\theta$

z: $-9.8\cos\theta$

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

其他 (如動物的動作，機器的運轉情形的偵測)

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

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