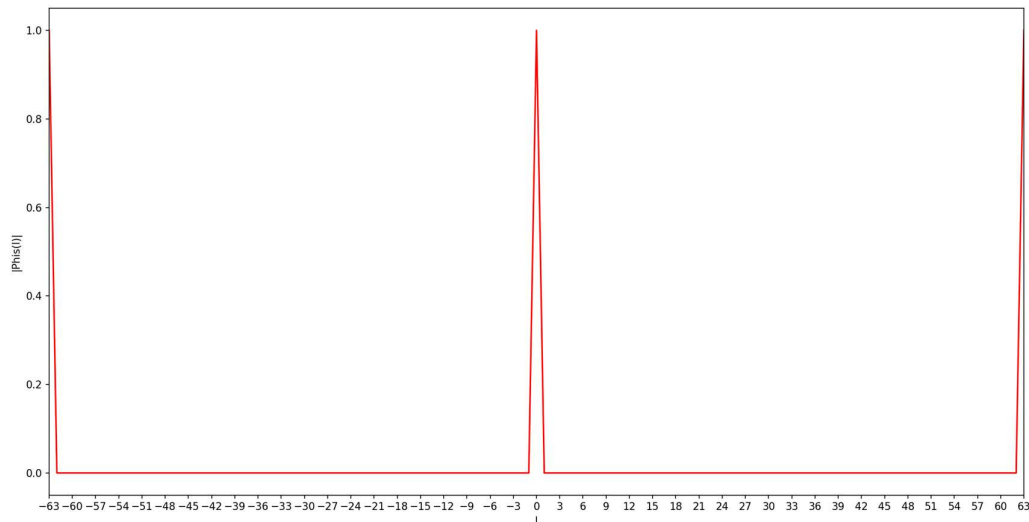


姓名:葉冠宏 學號:r11943113

1

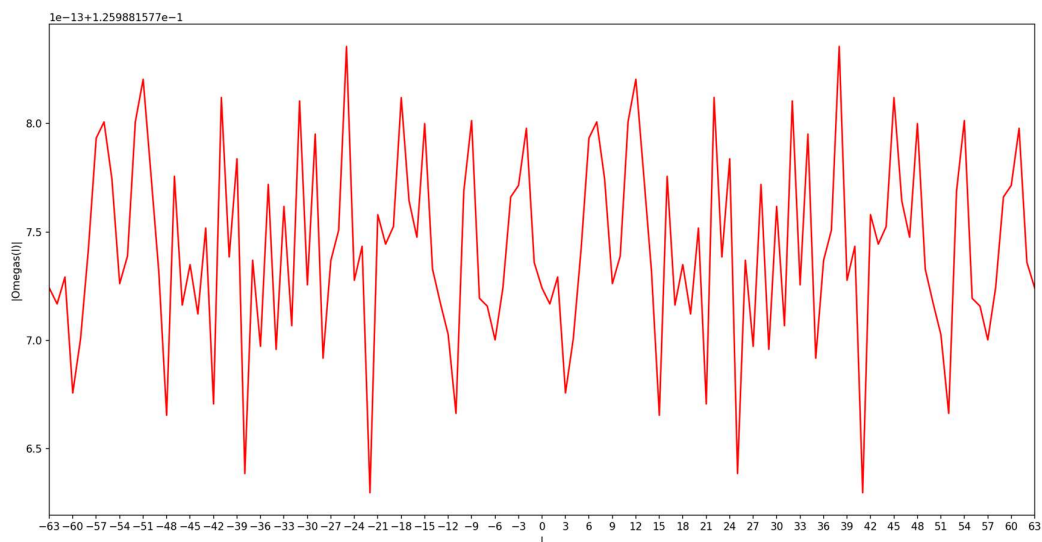
1(a)



我們可以看到在同一個 code 的情況下，autocorrelation 就是當 lag 差為 0 或是差一個 period 的時候，其相關性才為 1，否則為 0。

請執行 python Q1a.py

1(b)

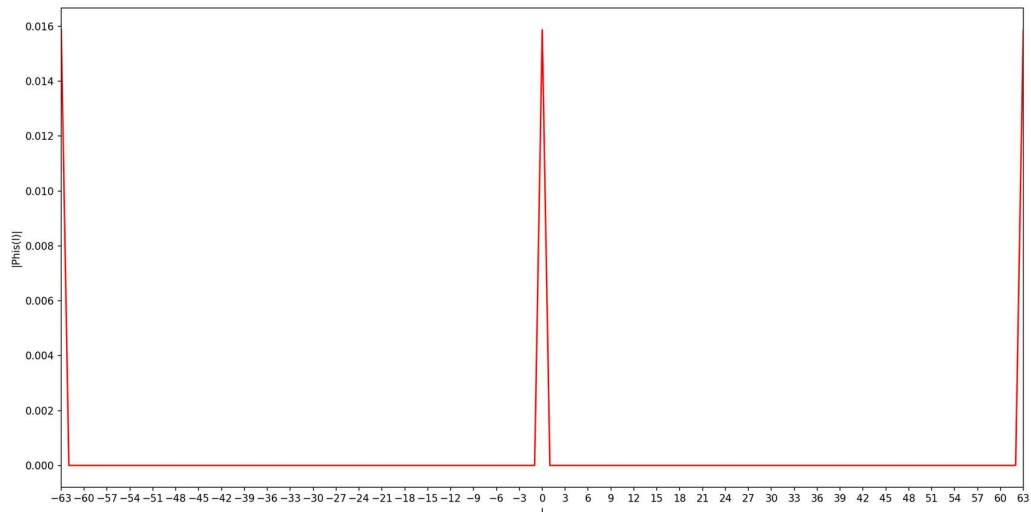


我們可以觀察到針對不同的 code 的 cross correlation 沒有一定的規則。

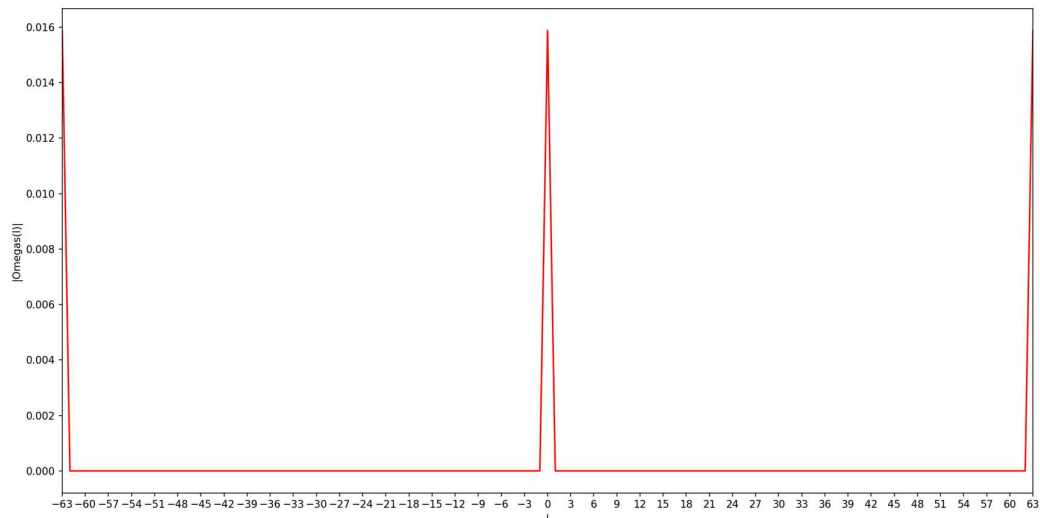
請執行 python Q1b.py

1(c)

$\Phi\{s\}(l)$ :



$\Omega\{s\}(l)$ :



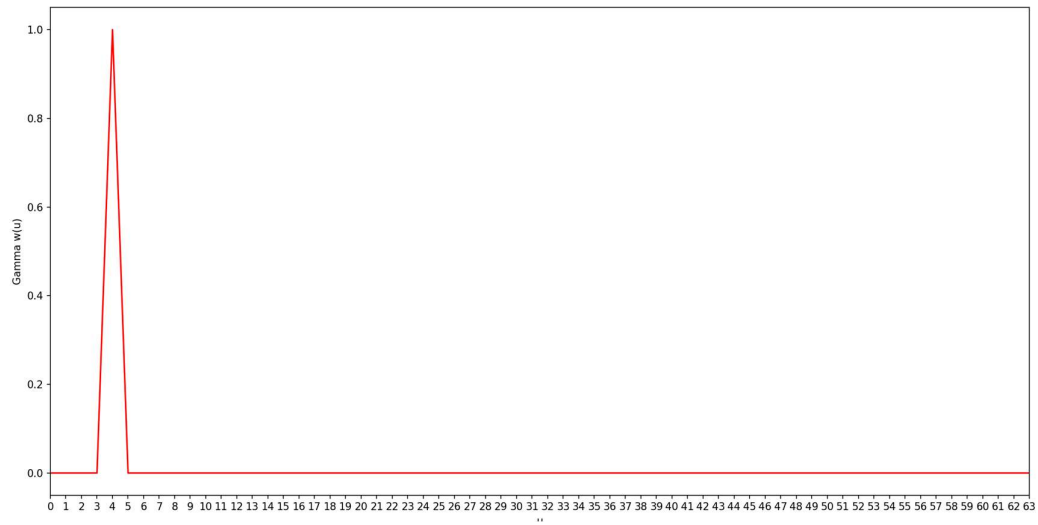
我們可以觀察到，當 Zadoff-Chu sequence 如題目的 1(c)所表示去掉 DC 的時候，其針對相同  $u$  的時候的 autocorrelation 其在 lag 為 0 和 lag 為週期的整數倍的時候，其 autocorrelation 為 1，其餘的值為 0。

然而我們也可以觀察到在針對  $u$  不同的不同 sequence 的時候，其 cross correlation 也是在 lag 為 0 或是週期性的 lag 的時候，其值為 1，其餘 lag 的時候為 0。

請執行 python Q1c.py

2.

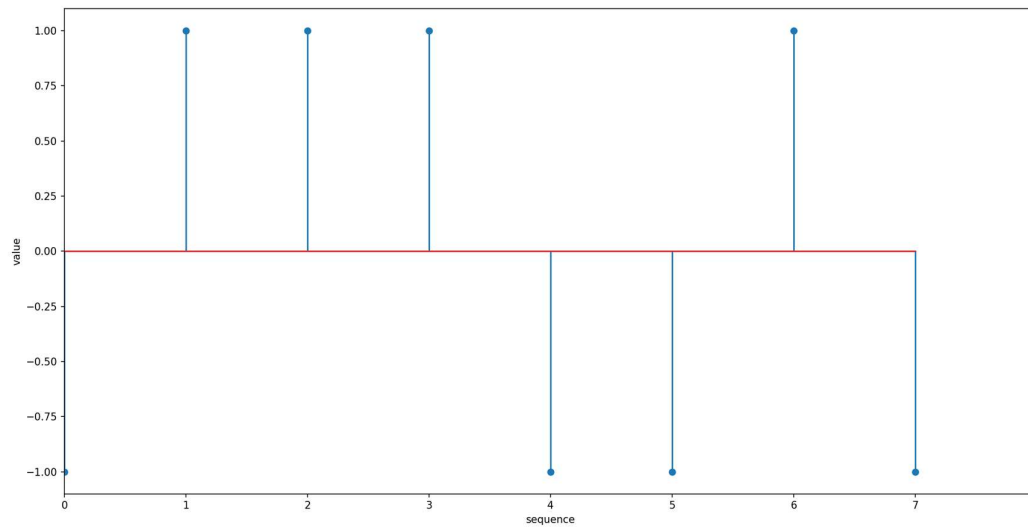
2(a)



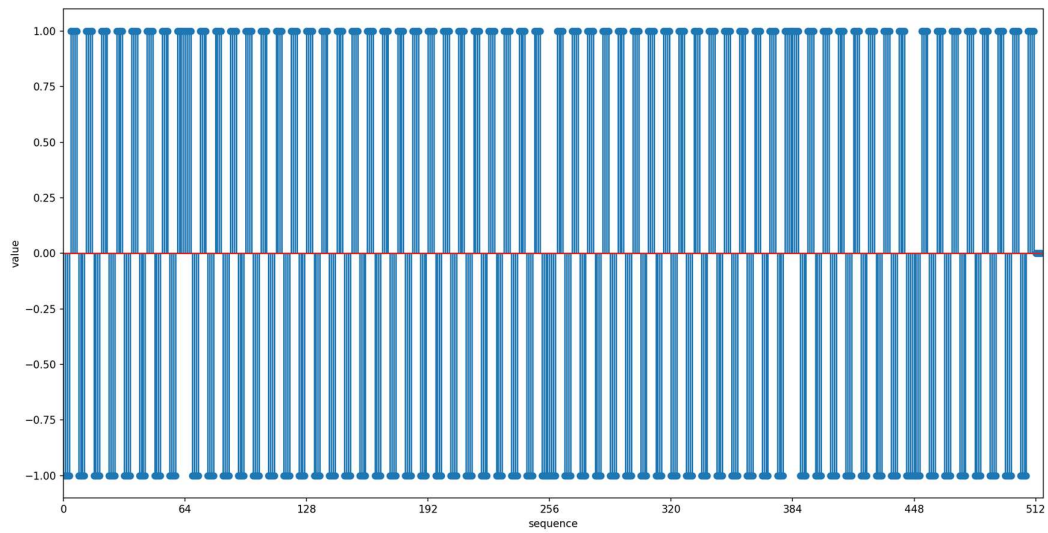
我的  $\alpha$  是 3， $\alpha+1$  是 4。我們可以觀察到只有在同一個 code 的時候的 cross correlation 才為 1。如果是不同 code 的話，cross correlation 為 0。  
請執行 python Q2a.py

2(b)

Before spreading:

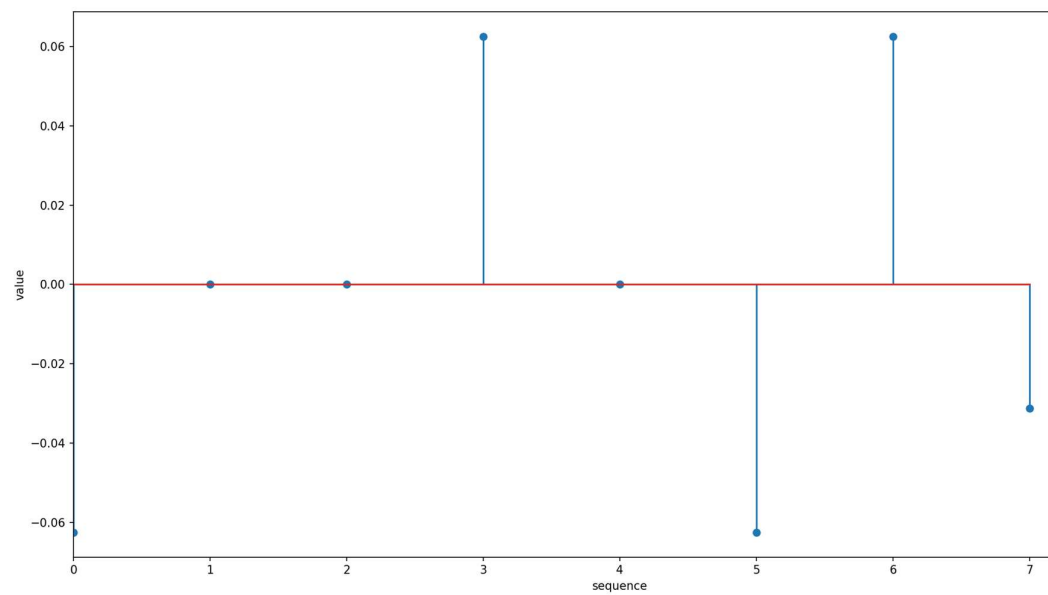


After spreading:



請執行 `python Q2b.py`

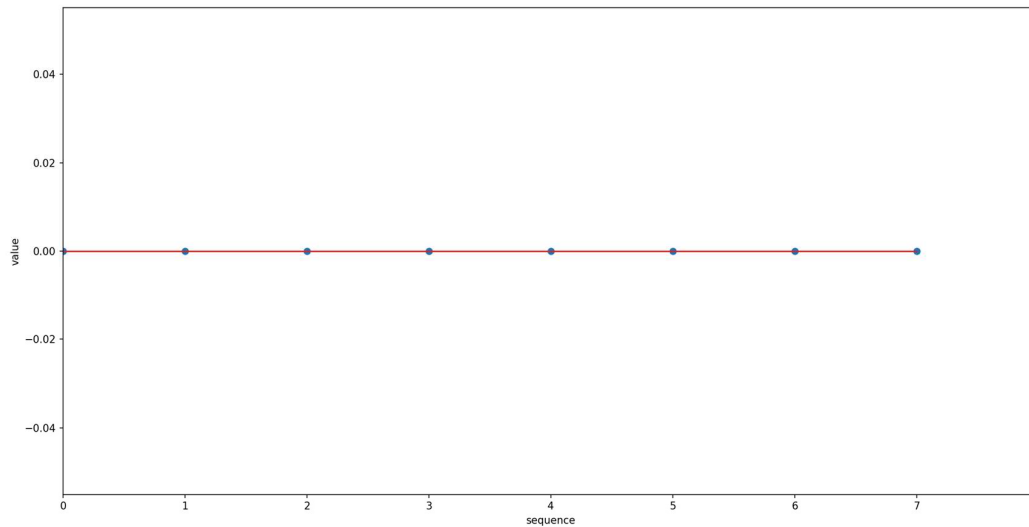
2(c)



我們可以觀察到這樣的 **decode** 方式無法還原出原來的 **code**。

請執行 `python Q2c.py`

2(d)



我們可以觀察到這樣的 **decode** 方式無法還原出原來的 **code**。  
請執行 `python Q2d.py`

2(e)

(1)

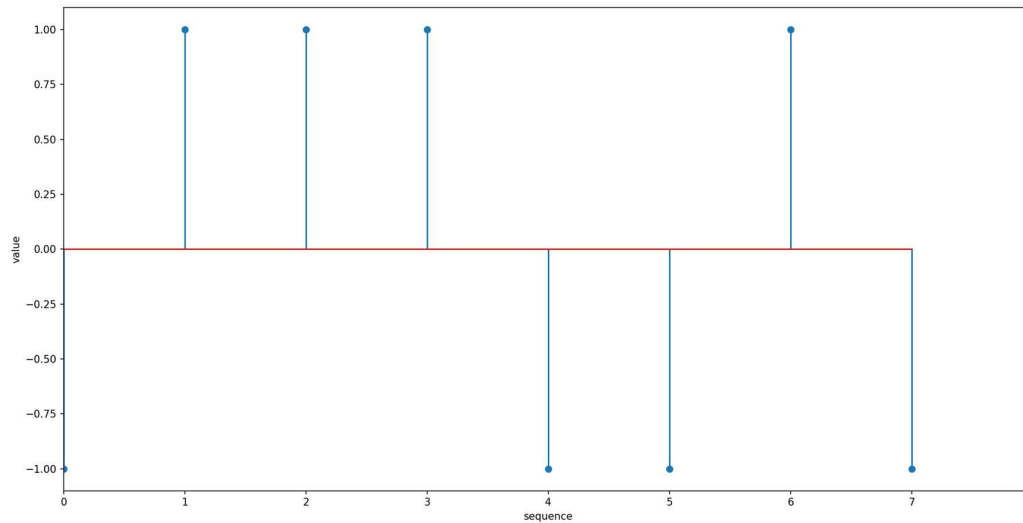
由於我們是用 **code1** 去加密所欲加密的 **data**。因此解密的時候也應該要用 **code1** 去解密才可以還原出原來的 **data**。

在 2(c)的題目中，雖然其要求我們也是用 **code1** 去解密，然而其要求我們解密所配對的序列和原來加密的方式不同，因此仍然無法解密出原來的 **data**。原來加密的方式是針對  $Y\{64i+j\}$  去做加密序列的創造。然而解密的方式卻是針對  $Y\{64i+j+2\}$  的序列來去做解密。

在 2(d)的題目中，雖然解密所針對的序列對了，是用當初加密時所針對的序列  $Y\{64i+j\}$ 。然而，其所解密的方式是用 **code2**，和當初加密所用的 **code1** 並不一樣，因此也還原不出原本的序列。

因此我嘗試用 **code1** 加密，以及用 **code1** 去解密，並用當初加密所創造的序列排序方式  $Y\{64i+j\}$ 。最後的確可以還原出原來的 **data**。如下圖:

請執行 `python Q2e.py`



(2)

在不用實際創造 data，並實際實驗加密、解密的狀況下，我們可以透過檢驗 Walsh Hadamard code 的數學性質來去判斷其是否可以拿來加密、解密。我們可以從 2(a)的結果中看到，因為我的 alpha 是 3， $3+1=4$ ，因此在 2(a)中針對  $W_{64}(j, \alpha + 1)$  這個 code，其和其他 u 不是 4 的不同 code 的 cross correlation 為 0，只有在和自己同樣 code 的 cross correlation，也就是 autocorrelation，才為 1。因此 Walsh Hadamard code 本身符合 random variable 的性質，也就是 autocorrelation 為 1，和其他 code 的 cross correlation 為 0。在實驗前我們就知道 Walsh Hadamard code 是一個好的加密系統。

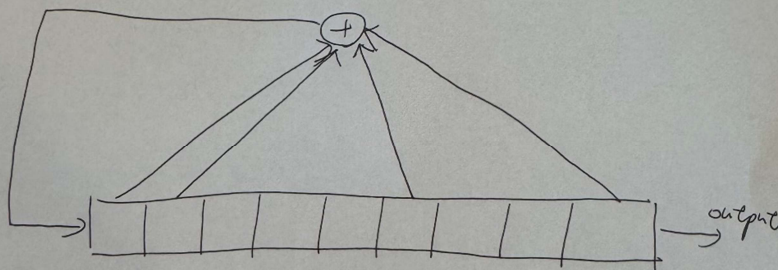
3

3(a)

我的學號是奇數，所以我是用 1423。

<sup>2</sup>  
(a)

$$\begin{aligned} 1423_p &= 1 \times p^3 + 4 \times p^2 + 2 \times p^1 + 3 \times p^0 \\ &= 2^9 + 2^8 + 2^4 + 2^1 + 2^0 \end{aligned}$$



3(b)

我的  $s$  是 3， $s+1$  轉成 binary 是 0000100，也就是 initial state。

請執行 python Q3b.py

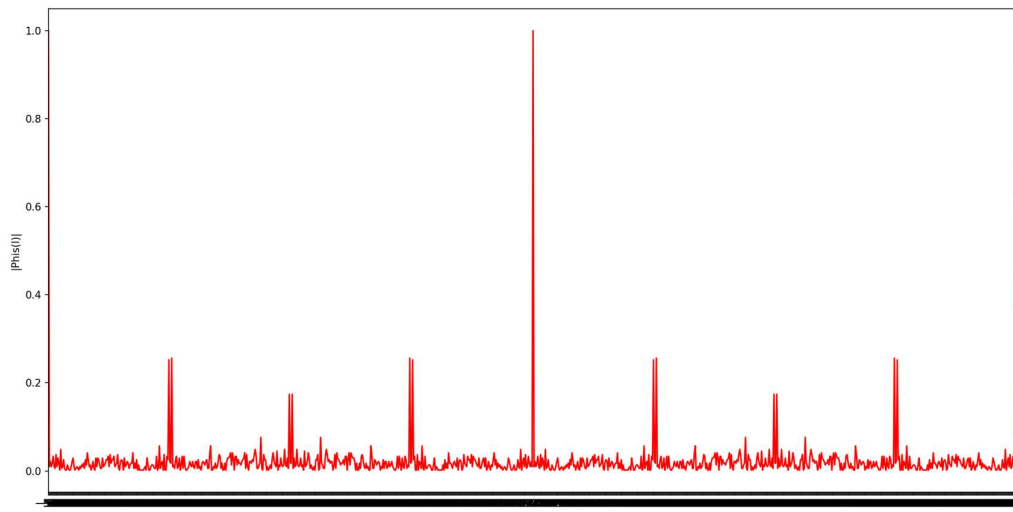
(1)

Print the first 20 binary elements,  $(b_0, b_1, \dots, b_{19})$  of your sequence:

```
[0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0]  
[Finished in 158ms]
```

(2)

periodic autocorrelation function for  $-N \leq l \leq N$ .



因為 degree 是 9 的 primitive polynomial。所以  $N$  是  $2^9-1=511$ ，也就是 complete ML sequence 的週期。我們在 lag 是  $-N \leq l \leq N$  時對序列進行分析。當我們轉換到  $dn$  的時候，我們可以觀察到 autocorrelation 在  $l$  為 0 的時候為 1。然後大約是  $1/4$  週期的整數倍的時候，autocorrelation 也會有比較高的情況。