1. (30%) Given an LSTM model as shown in Figure 1, point out (i.e., write down the symbols) which is the input gate, output gate, and forget gate, respectively (10%). Then explain the function of each gate (10%). Suppose that we have an application that needs to predict an output y for a sequence of three inputs (x1, x2, x3) (i.e., three time steps); draw an unfolded figure of LSTM for this application. (10%)

給定如圖 1 所示的 LSTM 模型,指出(即記下符號)分別是輸入門、輸出門和忘記門 (10%)。

然後解釋每個門的功能(10%)。

假設我們有一個應用程式需要預測三個輸入序列(x1、x2、x3)(即三個時間步長)的輸出 y;為此應用程式繪製 LSTM 的展開圖。(10%)

## LSTM (長短期記憶)

LSTM 網絡設計用於記住長期依賴,讓模型可以長期的計算每個輸入的影響程度,並由一系列單元組成,每個單元包含三個門:遺忘門、輸入門和輸出門。

- 1. **遺忘門 ft**: 決定從前一個單元狀態中應該丟棄或保留的信息。使用 Sigmoid 函數輸出 0 到 1 之間的值。
- 2. **輸入門 it**: 決定將哪些新信息存儲在單元狀態中。結合輸入數據和之前 的隱藏狀態 hidden state 來更新單元狀態。
- 3. **輸出門 ot**: 控制輸出,決定單元狀態的哪一部分應作為下一時間步的隱藏狀態輸出。
- 4. AT:以前稱為 gate gate,,是一種 tanh 激活函數,用於將輸出入資料控制 在 -1 到 +1 之間。

## 門控循環單元(GRU, Gated Recurrent Unit):

GRU 是 LSTM 的簡化版本,結合**遗忘門 (Forget Gate)**和輸入門 (Input Gate) 成為一個更新門,並將記憶單元和隱藏狀態合併。

GRU 有兩個門:更新門和重置門。

更新門(Update Gate): 決定需要保留多少過去訊息。

重置門(Reset Gate): 決定應該忘記多少過去訊息。

優勢: GRU 的計算效率比 LSTM 更高。

主要差異:LSTM 有三個門(遺忘門、輸入門、輸出門),而 GRU 有兩個(重置門、更新門)。LSTM 更複雜,可以捕捉更多複雜的模式,而 GRU 更簡單,訓練速度更快。

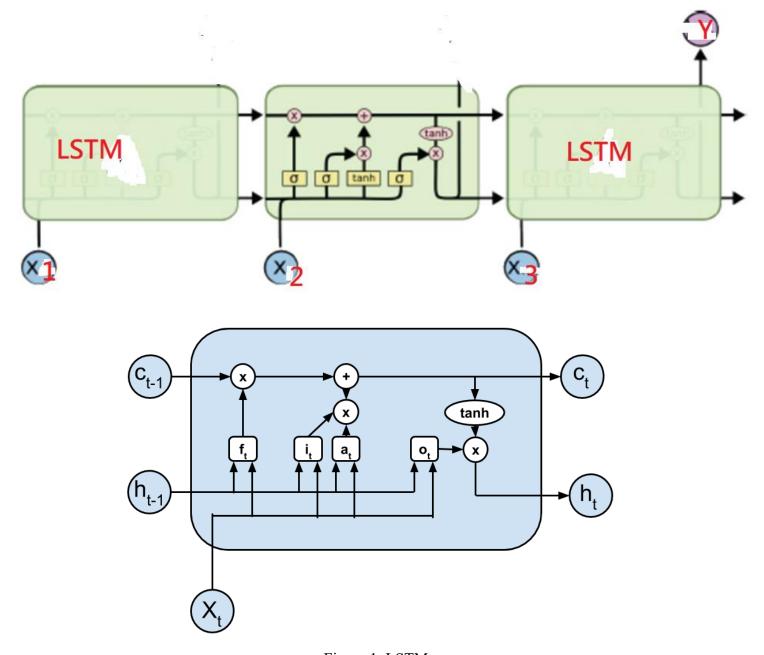


Figure 1. LSTM

2. (10%) What is the problem with a simple (or vanilla) RNN? How to solve it? 可能會導致 gradient vanishing or grading exploding problems 梯度消失或分級爆炸問題。使用「梯度裁剪」求解梯度爆炸問題,使用 LSTM 或 GRU 求解梯度消失問題。

### 梯度消失和爆炸

- 梯度爆炸問題使 RNN 陷入不穩定狀態 由於 RNN 的長期不收斂被導致資訊量過多的狀態。
- · 當長期梯度以指數速度快速變為零時,就會出現梯度消失問題,且模型暫時無法從遙遠的事件中學習。

#### 總結

基礎 RNN 面臨梯度消失和梯度爆炸問題,這使得模型難以學習長期依賴。LSTM和 GRU 等改進模型通過引入門機制有效地解決了這些問題。此外,梯度截斷 Gradient Clipping、雙向 RNN (Bidirectional RNNs)、注意力機制(Attention Mechanisms)和 transformer 等技術進一步提升了模型捕捉長期依賴的能力和訓練的穩定性。

### 梯度消失問題(Vanishing Gradient Problem):

在基礎 RNN 中,反向傳播過程中會計算損失函數相對於權重的梯度,這些梯度用來更新權重,當梯度通過多個時間步長向後傳播時,梯度會縮小。 這種縮小會導致梯度變得非常小,最終接近於零。這就是所謂的梯度消失問題, 使得模型難以學習長期依賴,因為與較早時間步長相關的權重無法有效更新。

#### 梯度爆炸問題 (Exploding Gradient Problem):

梯度在反向傳播過程中也可能會指數級地增大。這會**導致權重更新過大,從而使網絡不穩定**。雖然梯度爆炸問題相對較少見,但它會使**訓練過程變得困難並** 導致模型無法收斂。

長期依賴問題(Long-term Dependency Problem):

由於梯度消失問題,基礎 RNN 難以捕捉長期依賴關係。這使得它們在處理需要長期上下文的任務時效果不佳。

解決方案

# 梯度截斷(Gradient Clipping):

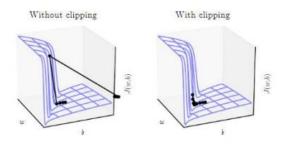
#### 技術:

為了解決梯度爆炸問題,可以使用梯度截斷技術。這種技術涉及設置梯度的閾值,如果梯度超過這個閾值,則將其縮放到閾值範圍內。

# To deal with the gradient exploding problem

 Gradient clipping, where we threshold the maximum value a gradient can get

$$if \|\boldsymbol{g}\| > \beta, \ g \leftarrow \frac{\beta \ \boldsymbol{g}}{\|\boldsymbol{g}\|}$$



## 長短期記憶網絡(LSTM, Long Short-Term Memory):

LSTM 網絡設計用來避免長期依賴問題。

記憶單元和輸入門、遺忘門和輸出門。

記憶單元:能夠長時間存儲訊息,

遺忘門 (Forget Gate): 決定應該丟棄多少訊息。 輸入門 (Input Gate): 決定應該存储多少新訊息。

輸出門(Output Gate): 決定應該輸出多少訊息。

優勢: 這種結構允許 LSTM 有效捕捉長期依賴,並減輕梯度消失問題。

## 門控循環單元 (GRU, Gated Recurrent Unit):

結構:

GRU 是 LSTM 的簡化版本,結合**遺忘門(Forget Gate)**和輸入門(Input Gate) 成為一個更新門,並將記憶單元和隱藏狀態合併。

它包含兩個門:更新門和重置門。

運作:

更新門(Update Gate): 決定需要保留多少過去訊息。

重置門 (Reset Gate): 決定應該忘記多少過去訊息。

優勢: GRU 的計算效率比 LSTM 更高,在許多任務中表現相似。

# 雙向 RNN (Bidirectional RNNs):

這些網絡同時處理前向和後向數據,捕捉來自過去和未來的上下文訊息。

## 注意力機制 (Attention Mechanisms):

注意力機制允許模型在預測每個輸出元素時<mark>關注輸入序列的特定部分</mark>,提高了 長期依賴處理能力。

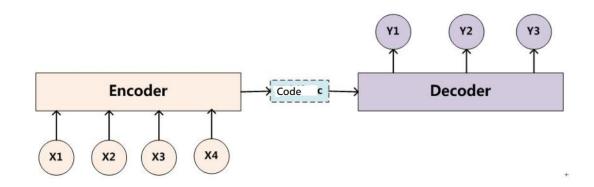
## 變壓器 (Transformers):

變壓器完全依賴於注意力機制,摒棄了循環結構,對於資訊的長期依賴性佳和 處理速度快。

3. (10%) The following diagrams show a sequence-to-sequence translation application of an RNN with or without using attention. Point out which (Fig.2(a) or Fig.2(b) is the RNN with attention model and which is not. Explain what is the difference between them. (10%) 下圖顯示了 RNN 的序列間翻譯應用程式,無論是否使用注意力。指出哪個(圖 2 (a) 或圖 2 (b) 是具有注意力模型的 RNN,哪個不是。 解釋它們之間的區別 Attention-Model.pdf

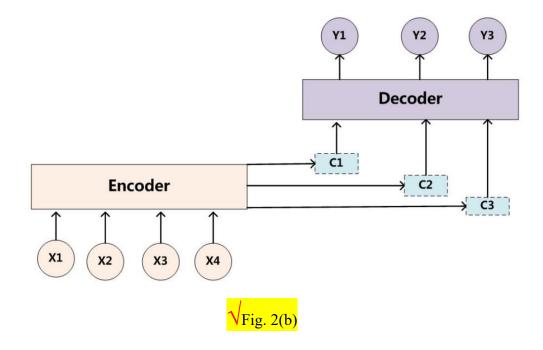
## 注意力機制 (attention model):

注意力機制允許模型<mark>關注輸入序列的特定部分</mark>,讓模型得以對句子(序列)中每個字對個別字的相關性和上下文影響做判斷。



4.

Fig. 2(a)



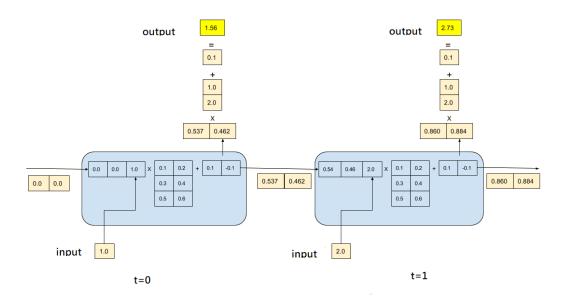
4. (20%) A simple RNN with an initial hidden state of h0=[0.0, 0.0], U=[0.5,0.6], V=[1.0,2.0], Hidden layer bias=[1.0,-1.0], Output bias=[0.1] W = [0.1, 0.2][0.3,0.4] 會在 code forwardrnn

# Given the input vector [2, 3], calculates the corresponding output of y.

For your reference, note that the activation function f is tanh().

$$h_1 = f(U \cdot x_1 + W \cdot h_0)_{\psi}$$
$$y_1 = g(V \cdot h_1)_{\psi}$$

- A. 將 h0 和 input vector(x1)合成一個向量
- B. 乘上W、U權重,做 matrixs 矩陣的乘法計算,横乘直
- C. 加上 hidden layer bias
- D. Tanh,成為下一層 h1 的 hidden layer,並同時繼續運算
- E. 乘上 V 權重
- F. 加上 output bias 得到 outputy1



5. (20%)The following piece of code defines a deep LSTM model for a time series prediction. It uses three time steps of historical time series values to predict the value of the next time step. (20%)

```
# reshape from [samples, timesteps] into [samples, timesteps, features]
   n_features = 1
 3 X = X.reshape((X.shape[0], X.shape[1], n_features))
 4 # define model
 5 print("n_steps", n_steps, "n_features", n_features)
 6 model = Sequential()
   model.add(LSTM(30, activation='relu', return_sequences=True,\
 7
8
                  input_shape=(n_steps, n_features)))
 9
   model.add(LSTM(30, activation='relu'))
10
   model.add(Dense(1))
   model.summary()
11
```

n\_steps 3 n\_features 1

Answer the following questions:

- a How many parameters are there in the first LSTM layer?
- b How many parameters are there in the second LSTM layer?

Hint: The input of the first layer is just a real number, and the input of the second layer is the hidden vector of the first layer, which has a dimension of 30.

Layer parameters 公式

第一個 LSTM 層 (lstm\_2) parameters

$$4 * [units * (units + n feature + 1))] = 4 * (30 * (30 + 1 + 1)) = 3840$$

第二個 LSTM 層 (lstm\_3) parameters

$$4 *$$
 [units \* (units + iuput\_dim + 1))] =  $4 * (30 * (30 + 30 + 1)) = 7320$ 

全連接層 (dense\_1)公式

Parameter = (input\_dim \* neuron) + neurons

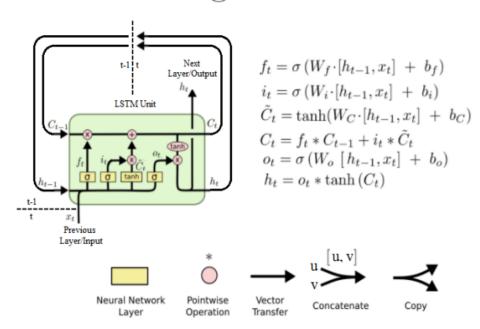
(model.add.dense(A))

## 全連階層參數量受上一層輸出 units 和密集曾自身神經元數影響

Parameter: (30\*1)+1=31

總參數數量 = 3840 + 7320 + 31 = 11191

# Understanding LSTM Networks



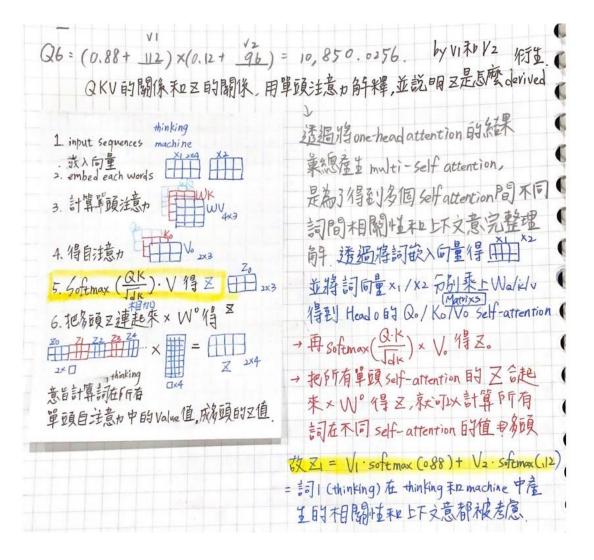
Bf 是 bias

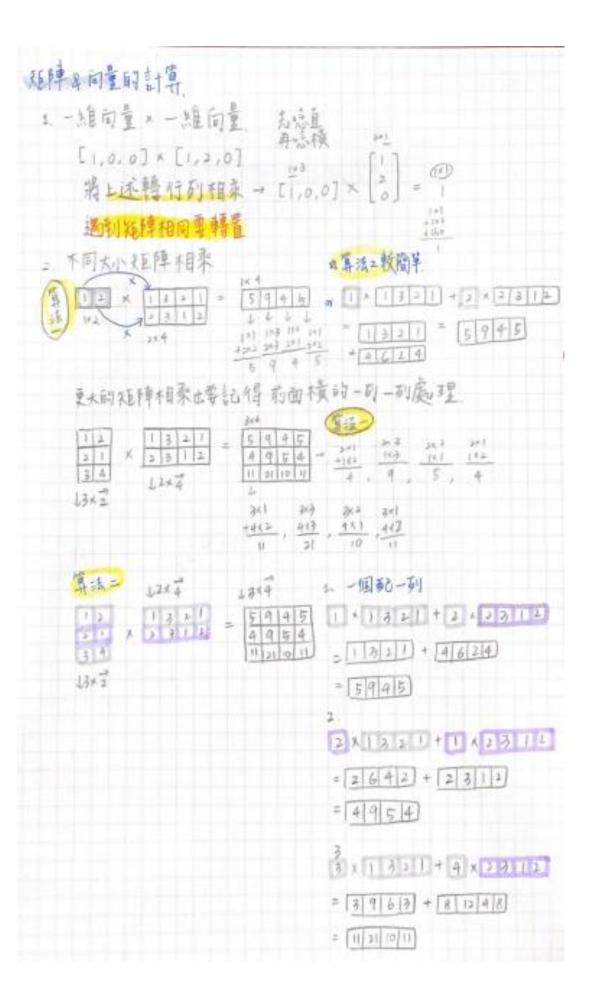
- 5. (10%) Transformer is the foundation of the many recent large pre-trained language models, such as BERT and ChatGPT. The concept of self-attention is the core of the Transformer. Based on the following figure, please explain the relationships among query, key, value and the resulting representation Z. Please answer this question by considering only one-head attention. Specifically, please answer how Z's first row is derived from v1 and v2.
- 在 Transformer 模型中,自注意力機制的核心概念如下:
  - 1. Query (Q):用於搜尋相關訊息的查詢向量矩陣。
  - 2. Key(K):用於配對查詢的鍵向量矩陣。
  - 3. Value (V):包含實際訊息的值向量矩陣。
  - 4. 表示 Z: 自注意力機制的輸出,是基於注意力得分的值的加權和。

Input	Thinking	Machines
Embedding	X <sub>1</sub>	X <sub>2</sub>
Queries	q <sub>1</sub>	q <sub>2</sub>
Keys	k <sub>1</sub>	k <sub>2</sub>
Values	<b>v</b> <sub>1</sub>	V <sub>2</sub>
Score	q <sub>1</sub> • k <sub>1</sub> = 112	q <sub>1</sub> • k <sub>2</sub> = 96
Divide by 8 ( $\sqrt{d_k}$ )	14	12
Softmax	0.88	0.12



The answer is : Z1 = 0.88 \* v1 + 0.12 \* v2



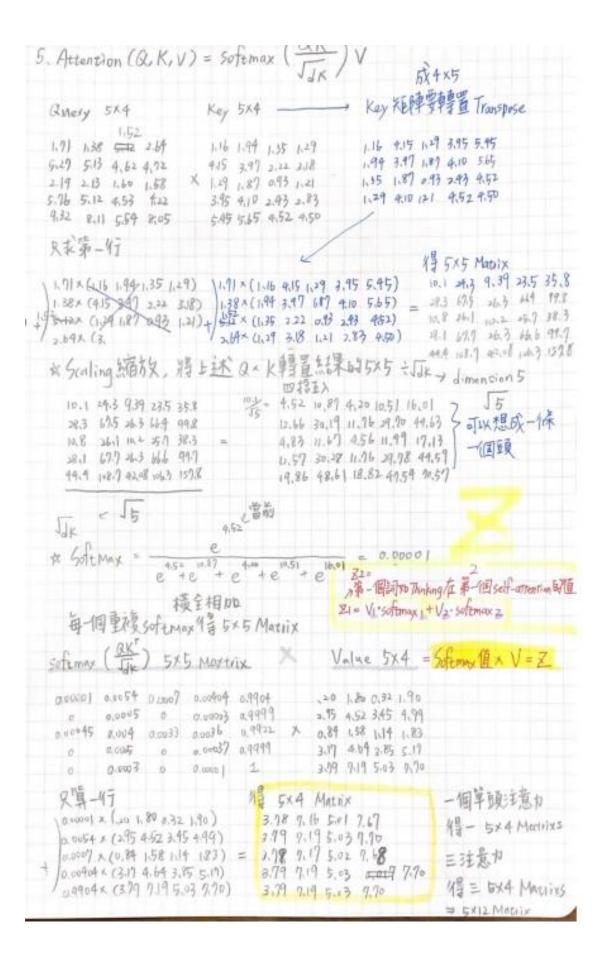


Transformer Gingle Embedding Ell. 前由 input → input embedding → encoding 語版的 1. Input Embedding 嵌入。将草詞轉換高一彩到數列(⑥重),並将后重做為 處理和理解語言的輸入(稱為編稿器), Dimensional 維度是自設的 input Embedding - Cat 75 sleeping on · 預數班/ 5 dim 2. Positional Encoding 位置結晶為三張 Model 知道每個詞的順图, Transformer 是一整可一起理解,並曾考慮詞及詞互相影響,(似上下文) \*PE有2公式 For and position, 不過應該題目會后 相關程度 3. Adding Word Embedding "& Positional Embedding positional embedding input embedding Cat is sleeping on the mat. 0 241 -90 141-95-95 force) Cat is slooping on the mati 59 76 23 -89 1 -67 = Cat is sleeping on the mat 54 160 1.13 1.031 -0.65 -0.28

4. Multi-self attention: Matrix相乘QKV考慮好交、詞間互相影響 計算/考慮可引中來個詞與莫他部份的相關程度

```
4. Multi-self attention
 所有的 Word Embedding + Positional Embedding都相同不同的是QKV的 linear Weights.
                  ·詹梨Weight 冉相加
                                                      Query 5x4 Matrixs
  (at is sleeping on the mat
                                  lineal Weights
               1,031 -0.65 0.28
 54 1.60 1.13
                                  67-14,71.9
                                                       1.71 1.38 1.52 2.64
 13 1917 1.63
               1.33 1.625 0.87
                               X .85 .31 .14 .95
                                                       527 513 462 4,72
  40 566 0.721 0.691 0,202 0.953
                                  129 57 76 43
                                                       219 213 1.60 1.58
 1-72 1.889 1.17 1309 1.509 1.329
                                  39 95 99 38
                                                       5.76 5.12 4.53
                                  64 94 17 51
  62 4.85 1.77 1.97 1.932 251
                                                       9.32 8.11 5.54
                                  -94 .73 .17 .02
         5×6 Matrixs
                                       6×4 Matrix
1 Query Sta
                           直向相加
  54x (.67 .14 .71 .03)
                            (362 076 383 016)
+1.601x (85,31,14,95)
                            (1.361 0.50 (224 1.521)
+ 1.13 × ( 24 57 .76 .93)
                           710,271 644 (860 1.051)
+ 1.031 × (.39 .95 .59 .38)
                            (.402 .980 .610 .392)
4-0.65 x (.64.94.77.51)
                           C-0416 -0.611
                                         501-033)
+-0.28 × (.94.73 17.02)
                            (-263 - 204 - 048 - 0.0056)
2 Key計算
  54x (.50 .76 .28.12)
                           (27 41 151 .065)
+ Lbol x (35 .33 .63 .25)
                          (.56.53 1.01 .40)
                          (-90 1.12 0.05 1.07)
 113 x (.09 .99 .04 (95)
                          (.03 ,09 ,24 ,09)
 + 4031 × ( 03,09 ,23 ,097
                         (四55-003-0) -28)
-0.65 * (.85.04.009.43)
                          604 -18 -109-0.06)
 -0.28 × (,14, 67,30 (21)
3. Value計算
                                     老師給的公式錯誤
                           (0.27 .410 ,151 0.065)
  .54 × (.50 .76 .28 .12)
 1.601 4 (.35 .33 . 63 .25)
                           (0560 0.528 1.009 0.400)
                         - (.892 1.119 0.045 1.074)
 1.13 × (.79.99 .04.95)
 1.031 x (03 A .23.09)
                           (0.031 0.093 0.23) 0.093)
 -a.65 x (.85.04.09.43)
                           (-553 -0.026 -0.00585, 280)
                           ( .039 176 -01006 (059)
 7.28 × (.14 .63 .30 .21)
```

反正得出的 Query / Key / Value



Vans firmer: 序列輸入序列輸出模型結構 input + on coder - context: based on RNN,但透過 Self-attention」自注意力機制考慮了句子中所 有甲子相關性和上下之,可以同時理解的可所有的分,對整理語 意史精革方木斤、克服 RNN中長其月依賴和計算效率不佳的限制 \* Transformer 由 alla 表 encoder 未上 肝肠炎 decoder 組成 \*Encoder Shases → 持輸入序列轉為連續形式,以獲得上下文意意 輔出緬军為一般發入向重稱係藏狀態。或「上下又」。 \* Decoder解碼器一 将 Encoder 輔出可應藏狀態反應計算成为ken 可能有三種 Type 副 Transformer A 1. Encoder - only Transformers → 弦在可深入理解和解釋文本 透過 精輔入序到體高名禮數位版本。以 BERT/R。BERTa/DistilBERT 使用雙自注意力→意應前/後,對內卷. 女2. Decoder-only Innshing +2 Moder 经在强大的原出、表述能力透過反 履計算預測下一個PM以時單詞來完成輸出序列,"GPT。 而 Lise Moder 採 Antorograssive attention, 僅多應己輸出的出行上下文。 女子. Encoder-decoder Transformer - 同時擁有動文本、理解語意 輸出回應的能力,如TS/BART,可用於翻譯和產主拍要 #標記以及本 \* Tokenizer,分詞器一使用Tokenizer將望詞轄藏數位,因機器外層數算 而每個問都有自己的編號。 Position Embedding Embedding -- lapat Embedding -> 107001

★ Embedding 嵌入一直支持被標記成數字編號印記轉成面重,一個標記 為一個向重,而這些向量被存在一個「向量嵌入空間」,同時也會 將單詞的位置紅公錄下來(Position Embedding),可使大意理解。

Position Embedding Encoder — F (Feed forward) 前境情

the Encoder Aller And Self-attention 多管在总物。并到Feed Forward,亚斯人同量

\* Multi head Self-attention — 可中参個詞會互相影響,要用 (logits vector 不同角度支充析語意,所以是 THilti head 多頭」

女 Feed-Forward 前後一由面層至連接神經網路組成,單獨處理 嵌入的序列 並由 Transformer 最終輸出層生成 logit,通常 FFD 使用 Gelu 做為沒沒函數 (Gelu 讓數據可在線性和非線性中轉換)

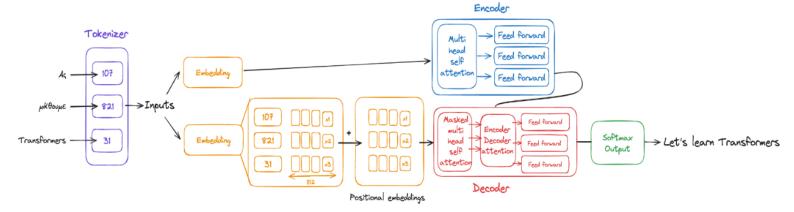
De Coder 解碼器 →和編碼器相同,通常有多個Decodor組成, Decodor 目標的於序列的 input 放到 Multi head self-attention再將 input 得到 FFD, Decodor和 Excodor 主要差别在於, Decodor 解碼器有2個注意力子層。 Masked multi-head self-attention 聚面多項注意力機制:遊光的 看答案,確保生成的力水的僅基於 過去輸出(以產出的內容, 和 管前預測) 的力水的 多頭目樣代表記問因不用影響,並讓Madel 考慮上下文意。

文 Encoder-decoder attention→讓Model要注在原文和譯文之間的轉換, un decoder曾在動出時意思上下文以及目前為止輸入的內落,並輸出此時最相關的Output(Token)

(PMax)

a Attention機制:幫助機器提升翻譯質量

\*Transformer = 讓模型訓練並行,提升訓練效率

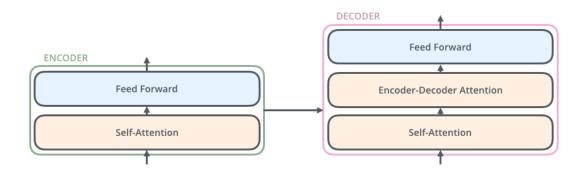


老師可能會給我們三個字,叫我們計算 hidden layer

Transformer——一種利用注意力來提高模型訓練速度的模型

https://zjuturtle.com/2020/01/25/transformer/

其中透過編碼器 encoder 和解碼器 decoder 來進行翻譯的動作,將輸入的句子語言進行編碼,並透過解碼器解碼成另一個語言



編碼器的輸入首先流經自注意力層 self attentions layer,該層幫助編碼器在對特定單字進行編碼時查看輸入句子中的其他單字(看需要注意的前後文)。

**自注意力層的輸出被饋送到前饋神經網路 FFD**。完全相同的前饋網路獨立應用於每個位置。

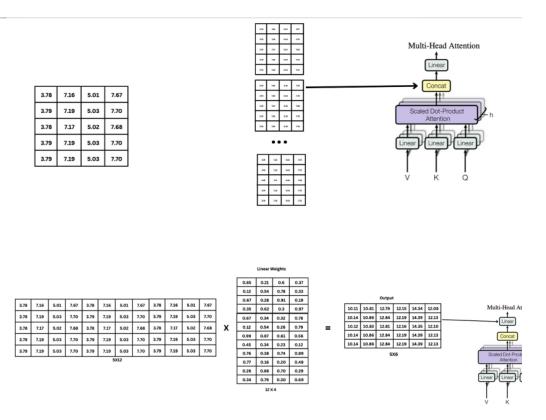
解碼器 decoder 具有這兩個層,但它們之間是一個注意力層,幫助解碼器專注 於輸入句子的相關部分 (類似於 seq2seq 模型中註意力的作用)。

#### 題目也有 GAN

## Information, entropy, cross entropy, KL-Divergence.pdf

https://jianjiesun.medium.com/dl-ml%E7%AD%86%E8%A8%98-%E4%B8%89-kl-divergence-cross-entropy-4b48810e0e90

#### stable disfussion



## **RNN**

# 生成對抗網絡(簡稱 GAN)

深度神經網路架構,包括兩個互相競爭的網絡:生成器(Generator)和判別器(Discriminator),GAN 通過對抗訓練,來讓模型生成與真實數據分佈相似數據的神經網絡架構。它由兩個主要組件構成:

#### 1. 生成器(G):

生成器接受一個<mark>隨機噪聲向量</mark>作為輸入,並生成**很像真實的假數據**。目標是 生成能夠騙過判別器的假數據,使判別器無法區分這些數據是真是假。

## 2. 判別器(D):

判別器接受一個數據樣本(可以是真實數據,也可以是生成數據)作為輸入,並區分輸入數據是真是假。目標是**讓模型判斷真假數據的準確度最大** 化。

#### GAN 的訓練過程是生成器 G 和判別器 D 兩者的對抗過程:

- 1. 初始化權重: 隨機初始化G和D的權重。
- 2. **訓練判別器:** 使用一批真實數據和生成數據來訓練判別器,使其能夠正確區分真實數據和假數據。
- 3. **訓練生成器**: 只更新生成器 G 的權重,使生成器生成的數據<mark>能夠騙過</mark> 判別器。
- 4. **反覆進行:** 重複上述步驟,在多個迭代中交替訓練生成器和判別器,**直 到生成器能夠生成非常逼真的數據**。
- GAN 透過生成器 Generator 和判別器 Discriminator 的對抗訓練,學習 並生成與真實數據分佈相似的數據,並在
- 生成逼真的圖像
- 藝術風格轉換
- 數據增強
- 圖像修復和超分辨率

等多個領域展現了其強大的應用潛力。

## 成本函數和最佳化

• 生成器的損失函數:

$$LG=-log for (D(G(z)))L\_G=-log(D(G(z)))LG=-log(D(G(z)))$$
 其中 DDD 是判別器, $GGG$  是生成器, $zzz$  是隨機噪聲向量。

• 判別器的損失函數:

$$\begin{split} LD &= -(log[fo](D(x)) + log[fo](1 - D(G(z)))) \\ LD &= -( log(D(x)) + log(1 - D(G(z)))) \\ LD &= -(log(D(x)) + log(1 - D(G(z)))) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x))) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x))) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) + log(D(x)) \\ LD &= -(log(D(x)) + log(D(x)) +$$

其中 XXX 是真實數據。