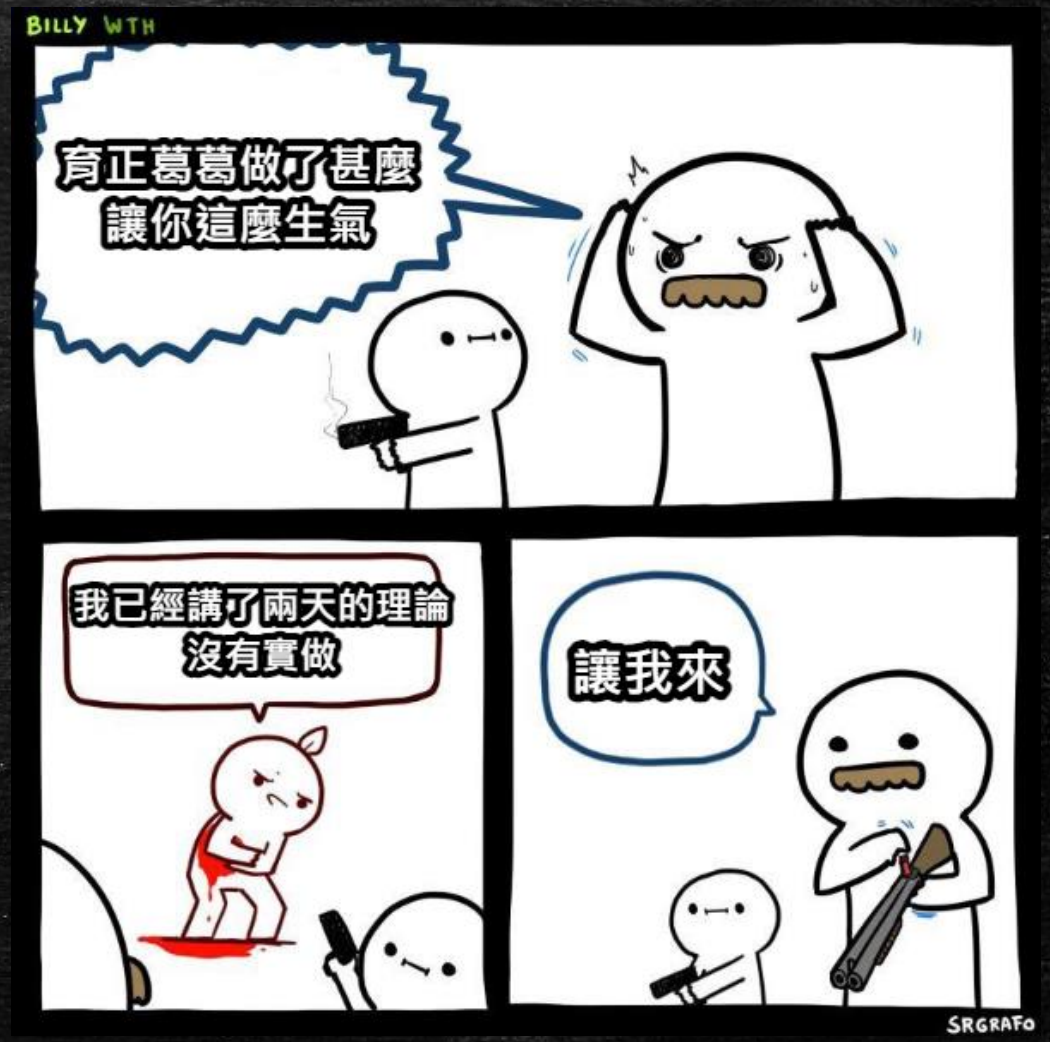
2024 鐵人賽 – 我數學就爛要怎麼來學 DNN 模型安全
Day 03 – 動手安裝篇

大綱

- 開發軟體介紹
- 安裝
  - 版本
  - 安裝步驟
- 結論



軟體介紹 – TensorFlow、PyTorch

- TensorFlow
  - 由Google於2015年推出，它提供了豐富的API，適合從入門到專業級的各種應用

- PyTorch
  - PyTorch是由Facebook的AI研究團隊開發，於2016年推出，在學術界十分流行，許多論文的研究成果都是使用 PyTorch 實現的

安裝軟體 – 更新顯卡驅動程式 (非必要)

```
C:\>nvidia-smi
Tue Jul  9 22:30:37 2024
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 536.67                 Driver Version: 536.67       CUDA Version: 12.2     |
|-------------------------------+----------------------+----------------------+
| GPU  Name                        TCC/WDDM | Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |         Memory-Usage | GPU-Util  Compute M. |
|                                         |                      |               MIG M. |
|===============================+======================+======================|
|   0  NVIDIA GeForce RTX 3070 ...  WDDM  | 00000000:01:00.0 Off |                  N/A |
| N/A   45C    P0              26W / 120W |      0MiB /  8192MiB |      0%      Default |
|                                         |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

安裝軟體

https://medium.com/ching-i/win10-%E5%AE%89%E8%A3%9D-cuda-cudnn-%E6%95%99%E5%AD%B8-c617b3b76deb

- NVIDIA GPU Computing Toolkit : 11.8 (非必要)
- cuDNN : v8.9.3, for CUDA 11.x (非必要)
- Python : 3.12.3
- Miniconda : 24.3.0 (https://docs.anaconda.com/miniconda/)
  - conda create --name py3.9 python=3.9.19
  - conda activate py3.9
- tensorflow : 2.10.0
  - pip install tensorflow==2.10.0
  - pip install numpy==1.26.4

測試 GPU 是否支援

import tensorflow as tf

tf.config.list_physical_devices('GPU')

```
(python3.9) C:\Users\aeifkz>python
Python 3.9.19 (main, May  6 2024, 20:12:36) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import tensorflow as tf
>>>
>>> tf.config.list_physical_devices('GPU')
[PhysicalDevice(name='/physical_device:GPU:0', device_type='GPU')]
>>>
>>>
```

測試向量的乘法

```
import numpy as np
a = np.array([[1, 2, 1]])
b = np.array([[1,2],[3,4],[2,1]])
print(np.dot(a, b))

import tensorflow as tf
tf_a = tf.constant(a)
tf_b = tf.constant(b)
print(tf.matmul(tf_a,tf_b))
```

安裝軟體 - Jupyter Notebook

- 開源的網頁應用程式，它可以讓使用者透過輸入程式碼就得到即時的結果，而且也易於分享給別人
- pip install notebook==6.5.6
- jupyter notebook

結論

- 雖然我是從 tensorflow 起手的，但後續想研究資安的話建議後續還是往 PyTorch 前進

- 畢竟學術論文會用 tensorflow 的真的很少，外加 tensorflow 又自己分裂成 1.0 跟 2.0，會有相容性的問題