ML2021Spring HW10 Report

<Mechanical Engineering> <陳志臻>
<B07502071>

Public Score	Private Score
0.030	0.000

The methods I used to pass the strong baselines include:
1、FGSM with models ensemble

```
def fgsm(models, x, y, loss_fn, epsilon=epsilon):
    x_adv = x.detach().clone() # initialize x_adv as original benign image x
    x_adv.requires_grad = True # need to obtain gradient of x_adv, thus set required grad
    x_ens = torch.zeros(models[0](x_adv).shape).to(device)
    for model in models:
      x_ens += model(x_adv)
    x_ens = x_ens / len(models)
    loss = loss_fn(x_ens, y) # calculate loss
    loss.backward() # calculate gradient
    # fgsm: use gradient ascent on x_adv to maximize loss
    x_adv = x_adv + epsilon * x_adv.grad.detach().sign()
    return x_adv
```

2、Models choose

```
model1 = ptcv_get_model('resnet110_cifar10', pretrained=True).to(device)
model2 = ptcv_get_model('preresnet56_cifar10', pretrained=True).to(device)
model3 = ptcv_get_model('seresnet56_cifar10', pretrained=True).to(device)
model4 = ptcv_get_model('sepreresnet56_cifar10', pretrained=True).to(device)
model5 = ptcv_get_model('pyramidnet110_a84_cifar10', pretrained=True).to(device)
```

(Your report should be written in English. Do not exceed 100 words describing your methods, but you may add comments to your code to make other students easier to understand.)