

Instructions on running the experiments

As the proposed BulletTrain method is applied to AugMix, TRADES, and MART, this repo heavily depends on the original implementation of AugMix, TRADES, and MART.

AugMix experiments:

1. Please follow the instructions in <https://github.com/google-research/augmix> to install the dependencies and download the datasets
2. Run AugMix baseline:

```
cd augmix/augmix-baseline  
python cifar10.py
```
3. Run AugMix with BulletTrain

```
cd augmix/augmix-speedup  
python cifar10.py
```

TRADES experiments:

1. Please follow the instructions in <https://github.com/yaodongyu/TRADES> to install the dependencies and download the datasets
2. Run TRADES baseline:
 - a. Training

```
cd trades  
python train_trades_cifar10.py --model-dir trades_baseline
```
 - b. Evaluation

```
python pgd_attack_cifar10.py --model-path  
trades_baseline/model-wideres-epoch76.pt
```
3. Run TRADES with BulletTrain:
 - a. Training

```
cd trades  
python train_trades_cifar10_bullet.py --model-dir trades_bullet
```
 - b. Evaluation

```
python pgd_attack_cifar10.py --model-path  
trades_bullet/model-wideres-epoch76.pt
```

MART experiments:

4. Please follow the instructions in <https://github.com/YisenWang/MART> to install the dependencies and download the datasets
5. Run MART baseline:
 - a. Training

```
cd mart  
python train_wideresnet.py --model-dir mart_baseline
```
 - b. Evaluation

```
python eval_wideresnet.py --model mart_baseline --num-steps 20
```

6. Run MART with BulletTrain:

a. Training

```
cd mart
```

```
python train_wideresnet_bullet.py --model-dir mart_bullet
```

b. Evaluation

```
python eval_wideresnet.py --model mart_bullet --num-steps 20
```