Dynamic Programming
IEMS469 - 23 Fall
Assignment 3 - Part II

Dinglin Xia

November 26th, 2023

1 Differential Privacy with Laplace mechanism

1.1 Experimental Result

In part 2, we tried injecting noise following Laplace distribution to the training images and applied the FedAvg algorithm. A training/validation plot of FedAvg with Laplace noise ($b = 0.1$) is shown in figure 2. In the experiment part, we tried different scales (i.e., $b = 0, 0.05, 0.1, 0.2, 0.25, 0.5, 1$) for the Laplace noise. During the training process, we save the model which has the highest average validation accuracy in the last 100 episodes. The full experiment record is shown in table 1.

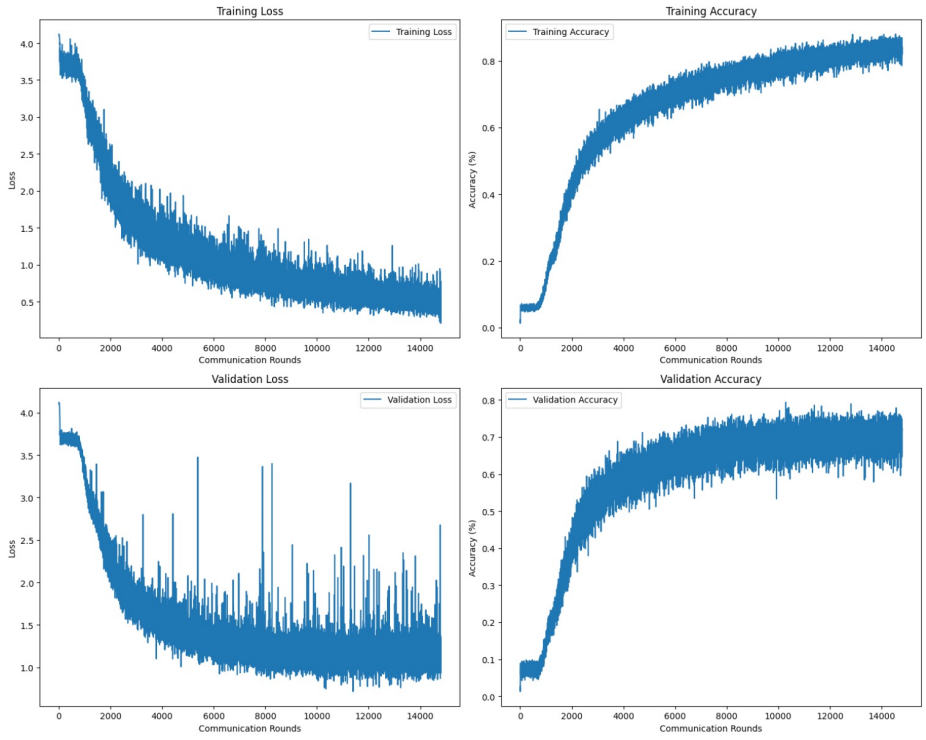


Figure 1: Training/Validation plot of FedAvg with Laplace noise ($b = 0.1$).

Noise Scale	Training Loss	Training Acc.	Validation Loss	Validation Acc.
$b = 0$	0.424	86.9%	0.711	80.4%
$b = 0.05$	0.379	86.5%	1.179	73.8%
$b = 0.1$	0.622	84.4%	1.139	69.7%
$b = 0.2$	0.365	86.1%	1.838	58.6%
$b = 0.5$	2.122	45.0%	2.925	27.6%
$b = 1$	2.620	35.5%	3.506	11.1%

Table 1: Training/Validation Loss/Accuracy of different noise scales.

The full record of training and testing accuracy is shown in fig 3.

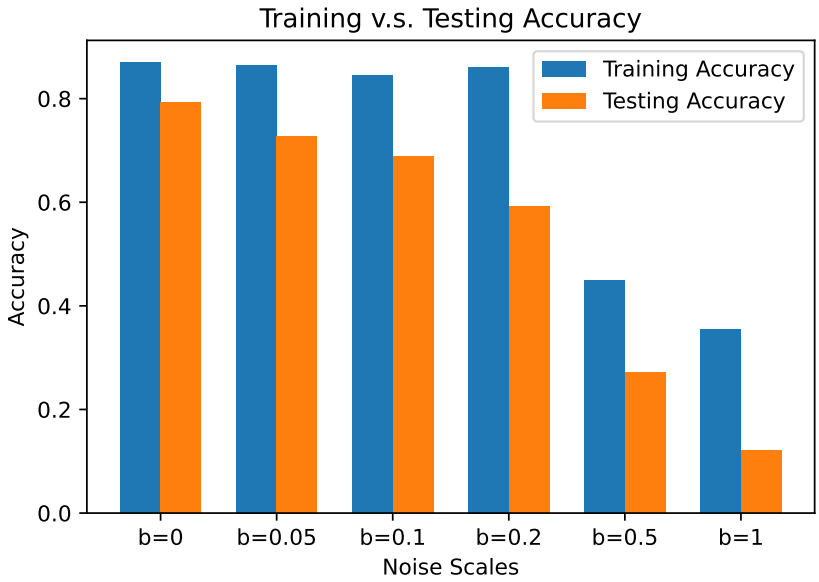


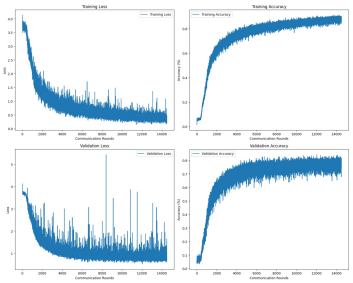
Figure 2: Training and testing accuracy with different noise scales.

From the training plot, we also witness overfitting when b is large. More specifically, the larger the b, the fewer episodes it requires to yield overfitting.

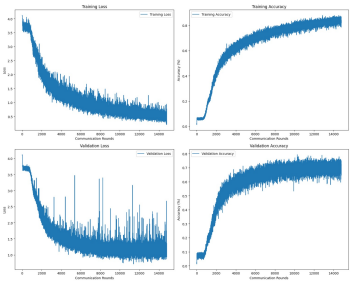
1.2 Observation and Conclusion

From the experimental result of different noise scales b, we witness that the larger b we choose, the bigger the difference between training accuracy and validation/testing accuracy. Thus we see there is a trade-off between privacy and accuracy. I would choose $b = 0.1$ since it offers some extent of privacy while the testing accuracy is about 70%, which is acceptable.

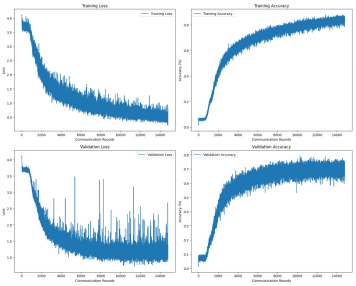
2 Appendix



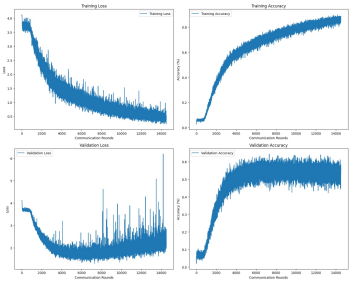
(a) b = 0



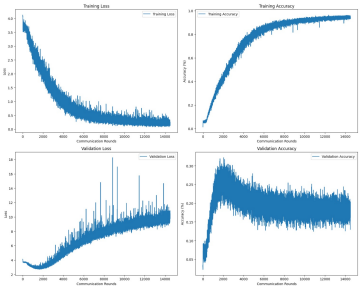
(b) b = 0.05



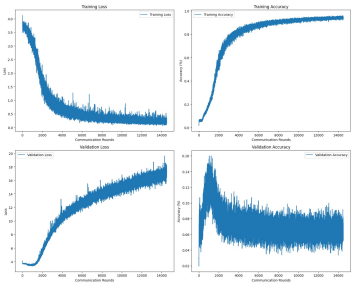
(c) b = 0.1



(d) b = 0.2



(e) b = 0.5



(f) b = 1

Figure 3: Full record of training with different noise scales.